



Installation and Configuration Guide

Airgo Access Point

Airgo Networks, Inc.
900 Arastradero Road
Palo Alto, CA 94304
P: 650-475-1900
F: 650-475-1708
www.airgonetworks.com

Part Number: 640-00068-00
Published: July 2004

Copyright © 2004 by Airgo, Inc. All Rights Reserved.

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Airgo unless such copying is expressly permitted by U.S. copyright law.

Contents

	Preface	x
1	Overview	1
	Product Overview	1
	Product Suite	1
	Features Overview	2
	Radio Resource Management	3
	Mobility Management	3
	Portal Architecture	4
	Security	5
	VLANs	5
	Quality of Service	6
	IP Routing	6
	Multiple SSIDs	6
	Guest Access	6
	Rogue AP Detection and Classification	6
	Standards and Data Rates	7
	Integration With the Existing Wired Network	7
	Management Interface Options	8
2	Planning Your Installation	9
	Introduction	9
	Example Wireless Network Installation	9
	Assessing Coverage and Capacity Requirements	10
	Site Surveys	11
	Assessing Security Needs and Architecture	11
	Selecting a Network Management Method	12
	Planning Network Features	14
	Example Deployment Scenarios	16
	Example 1: Small office, single AP, possible future growth	16
	Example 2: Small to mid-size business with wireless backhaul	18
	Example 3: Mid-size business, multiple SSIDs, multiple VLANs	19
	Example 4: Large business, guest access, extended network services	21
	Example 5: Large Campus with Branch Offices	23
3	Installing the Access Point	25
	Using the Configuration Interfaces	25
	Hardware Components	25
	System Requirements	25
	Installation Requirements	25

Power and Cabling Requirements	26
Network Information Requirements	26
Installing the Access Point	26
Using Power Over Ethernet	27
Placement and Orientation	27
Verifying the Installation	28
Interpreting the LEDs	28
Connecting the Serial Port	29
Resetting the Access Point	29
Using the Configuration Interfaces	30
Using the Web Browser Interface	30
Using AP Quick Start to Initialize the Access Point	31
Initializing a Normal AP	33
Initializing the Portal AP	36
Navigating the Web Interface	37
The Home Panel	37
Quick Start Panels	39
Other Panels	45
NM Portal Access	45
Configuration Wizards	45
User Security Wizard	45
Guest Access Wizard	50
4 Configuring Radio Settings	55
Introduction	55
Configuring Radio Parameters	56
Global Configuration	57
Admin State Configuration	62
Channel Configuration	64
Performance	66
Admission	68
Setting the Advanced Radio Configuration	69
802.11 Policy	69
MAC Configuration	71
Viewing Radio Statistics	72
Radio State	72
Radio Statistics	75
Viewing Radio Neighbor Details	77
Configuring SSID Parameters	78
SSIDs and Service Profiles	79
SSID Table	80
SSID Details	82
Profile Table	84
Multiple SSIDs	85
Managing Client Stations	86
Stations	87

	Link Statistics	88
	Security Statistics	89
	Configuring Inter Access Point Protocol (IAPP)	90
	IAPP Service	91
	IAPP Topology	91
	IAPP Statistics	92
	Performing Radio Diagnostics	93
	Link Test	94
	Walk Test	97
5	Configuring Networking Settings	99
	Introduction	99
	Interfaces	99
	Configuring Bridging Services	100
	Bridge and STP	100
	Bridge Statistics	102
	ARP Table	102
	Configuring IP Routes	103
	Configuring VLANs	105
	VLAN Table	106
	Interface VLAN	107
	User VLAN	108
	VLAN Statistics	110
	Configuring Quality of Service	111
	Ingress QoS	113
	Egress COS	114
	QoS Stats	115
	Configuring Advanced QoS	115
	Class-Order	116
	IP-DSCP	117
	IP Protocol	118
	IP Precedence	119
	Configuring Packet Filters	119
	Filter Table	119
	Filter Statistics	121
	Configuring Interfaces	121
	Interface Table	122
	Interface Statistics	123
	Configuring SNMP	123
	Ping Test	125
6	Configuring a Wireless Backhaul	127
	Introduction	127
	Use of Radios for Backhaul	128
	Wireless Backhaul Trunks	128
	Wireless Backhaul security	128

Setting Up a Wireless Backhaul	129
Link Criteria	129
Candidate APs	131
Trunk Table	131
Trunk Statistics	132
7 Managing Security	135
Introduction	135
AP Security	136
Administrative Security	136
User Security	136
Data Encryption	137
Configuring Wireless Security	138
Security Mode	138
SSID Authentication	140
Configuring Authentication Zones	143
Authentication Zones	143
Authentication Servers	144
Configuring Administrator Security	144
External RADIUS Server Settings	145
Viewing Security Statistics	146
Authentication Statistics	146
Supplicant Statistics	147
Authentication Diagnostics	149
Configuring Advanced Parameters	150
8 Configuring Guest Access	153
Overview	153
Internal Landing Page	154
External Landing Page	155
Open Subnet	156
Configuring Guest Access	156
Guest Access Services Panel	158
Guest Access Security	160
9 Managing the Network	163
Introduction	163
Using NM Portal	164
Home Panel	164
Menu Tree	164
Using the Network Topology Menu	165
Enrolling APs	165
Viewing Backhaul Topology	168
Viewing IP Topology	169
Displaying Discovered Radios	171
Managing Rogue Access Points	173

IP Rogue AP Management	174
Wireless Rogue AP Management	176
Using the NM Services Menu	179
Working With Policies	179
Configuring Network Discovery	182
Configuring Portals	185
Configuring the DHCP Server	188
Managing Network Faults	192
Viewing Alarms	192
Viewing the Syslog	202
Managing Users	203
Adding Wireless Users	203
Adding Administrative Users	205
Adding MAC-ACL Users	206
10 Maintaining the Access Point	209
Rebooting the AP	209
Managing the System Configuration	209
IP Configuration	210
Syslog Configuration	211
License Management	212
NMS Configuration	212
Hardware Options	213
Managing the AP Configuration	214
Secure Backup	214
Configuration Reports	215
Reset Configuration	217
TFTP Backup	218
Upgrading Software	219
Software Image File	220
Upgrading the AP Software	220
Canceling a Distribution	223
Download Status	223
Image Recovery	224
Common Problems and Solutions	224
A Using the Command Line Interface	227
Using the Command Line Interface	227
Using the Console Port for CLI Access	228
B Regulatory and License Information	231
C Alarms	233
Discovery: Discovered new node	235
Discovery: Node deleted from network	235
Discovery: Managed nodes limit exceeded	236
Enrollment: Node Enrolled	236

Enrollment: Node Un-enrolled	237
Policy: Policy Download Successful	238
Policy: Policy Download Failed	238
Software Download: Image Download Succeeded	239
Software Download: Image Download Failed	239
Software Download: Software Distribution Succeeded	240
Wireless: Radio enabled (BSS Enabled)	241
Wireless: Radio Disabled (BSS disabled)	241
Wireless: BSS Enabling Failed	242
Wireless: Frequency Changed	242
Wireless: STA Association Failed	243
Wireless: STA Associated	244
Wireless: STA Disassociated	245
Wireless: WDS Failed	246
Wireless: WDS Up	246
Wireless: WDS Down	247
Security: Guest Authentication Succeeded	248
Security: Guest Authentication Failed	249
Security: User rejected by RADIUS Server	249
Security: BP rejected by RADIUS Server	250
Security: RADIUS Server timeout	251
Security: Management User login success	252
Security: Management User login failure	253
Security: STA failed EAPOL MIC check	253
Security: STA attempting WPA PSK – no Pre-shared Key is set for SSID	254
Security: Auth Server Improperly configured on this SSID	255
Security: STA failed to send EAPOL-Start	256
Security: RADIUS sent a bad response	256
Security: RADIUS timeout too short	257
Security: STA authentication did not complete in time	258
Security: Upstream AP is using an untrusted auth server	259
Security: Upstream AP is using a non-portal node as its auth server	260
Security: Upstream AP failed MIC check during BP authentication	260
Security: Premature EAP-Success received	261
Security: Profile not configured for user-group	262
Security: STA has failed security enforcement check	263
Security: Guest Authentication Failed	264
Security: AP Detected Bad TKIP MIC	265
Security: BP Detected Bad TKIP MIC on Incoming Unicast	266
Security: BP Detected Bad TKIP MIC on Incoming Multicast/Broadcast	266
Security: STA Detected Bad TKIP MIC on Incoming Unicast	267
Security: STA Detected Bad TKIP MIC on Incoming Multicast/Broadcast	268
Security: TKIP counter-measures lockout period started	268
Security: EAP User-ID timeout	269
Security: EAP response timeout	270

Security: EAPOL Key exchange – message 2 timeout	271
Security: EAPOL Group 2 key exchange timeout	272
Glossary	275
Index	281

Preface

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

The Airgo 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 Airgo 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 Airgo Access Point products.
- **Chapter 2, “Planning Your Installation,”** describes various deployment scenarios and helps determine how many Airgo Access Points will be needed and the appropriate network management scheme.
- **Chapter 3, “Installing the Access Point,”** describes how to install the Airgo Access Point and how to use the Quick Start panels for fast and easy configuration. Also explains how to use the Airgo AP web interface.
- **Chapter 4, “Configuring Radio Settings,”** explains how to configure the Airgo Access Point radios.
- **Chapter 5, “Configuring Networking Settings,”** explains how to configure the advanced networking features of the Airgo 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 Airgo Access Point and explains how to 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 Airgo Access Point to manage multiple APs across your network.
- **Chapter 10, “Maintaining the Access Point,”** describes the tools available to maintain the Airgo Access Point.
- **Appendix A, “Using the Command Line Interface,”** describes how to use the console and command line interface (CLI) to configure the Airgo Access Point, with cross-references to the Airgo Command Line Interface Reference Manual.
- **Appendix B, “Regulatory and License Information,”** provides regulatory specifications for the Airgo Access Point.
- **Appendix C, “Alarms,”** provides a description of the alarms generated by the Airgo Access Point.
- **Glossary**— Provides definitions for acronyms, networking terminology, and Airgo-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.
<i>italic</i>	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 <i>Ctrl</i> . For example, when you read <i>^D</i> or <i>Ctrl-D</i> , 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 Airgo wireless networking product line is available on CD-ROM and also on the Airgo website, <http://www.airgonetworks.com>.

- **Airgo Client Installation and User Guide** — Explains how to install and configure the Airgo Wireless LAN Client Adapter, which provides PC laptop and desktop users with access to the Airgo Access Point products.
- **Airgo NMS Pro Installation and Configuration Guide** — Explains how to use Airgo NMS Pro to manage an enterprise wireless network.
- **Airgo Command Line Interface (CLI) Reference Manual** — Provides a listing of all the commands available for Airgo 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 Airgo Access Point and presents the following topics:

- [Product Overview](#)
- [Features Overview](#)
- [Standards and Data Rates](#)
- [Radio Resource Management](#)
- [Mobility Management](#)
- [Portal Architecture](#)
- [Security](#)
- [Integration With the Existing Wired Network](#)
- [Management Interface Options](#)

Product Overview

The Airgo 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, Airgo products help to promote the mainstream adoption of wireless technology, and help to foster new wireless applications.

Product Suite

The Airgo product suite comprises these wireless networking products:

- Airgo Access Point
- Airgo Wireless LAN Client Adapter
- Airgo Professional Network Management System (NMS Pro)

Airgo Access Points

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

Airgo Wireless LAN Client Adapter

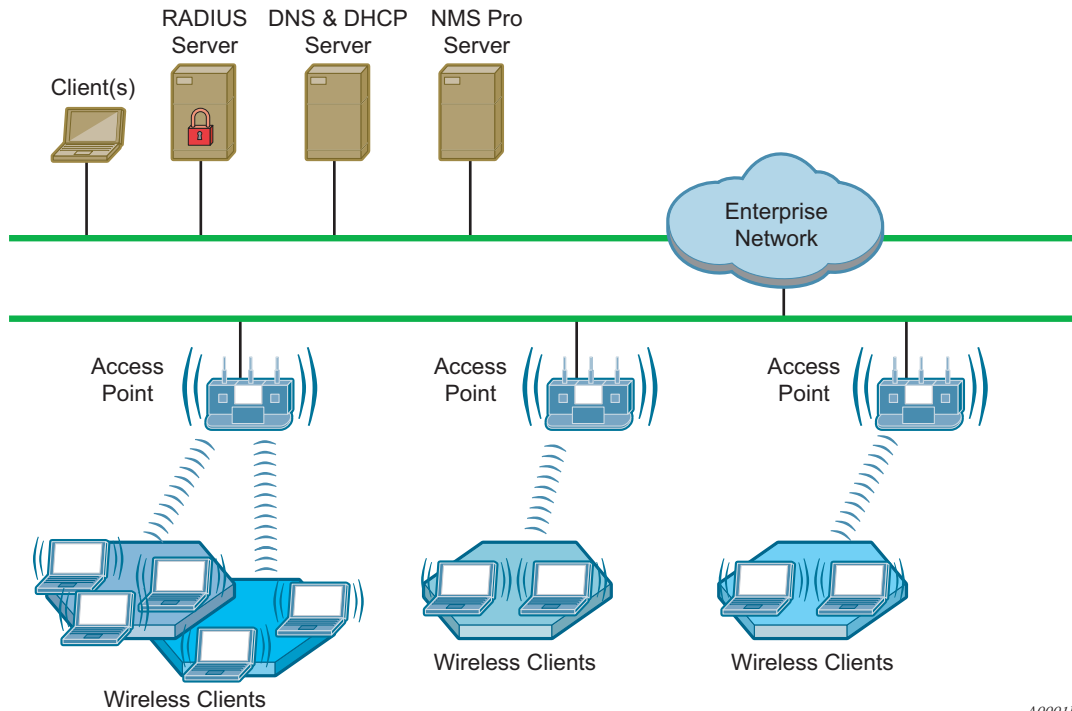
The Airgo Wireless LAN Client Adapter provides the communications link between laptop or desktop PC users and wireless network. Available in PC Card and Mini PCI Card form factors, the Airgo Wireless LAN Client Adapter is designed to take full advantage of the performance, range, security, and management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

Airgo NMS Pro

Airgo's NMS Pro 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 *NMS Pro Installation and Configuration Guide*.

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

Figure 1: Airgo Wireless Network



A0001D

Features Overview

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

- Dual radios, each operating in 802.11b/g or 802.11a mode
- Optional Airgo 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 Airgo 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 Airgo AP also provides support for 802.11f based Inter-Access Point Protocol (IAPP).

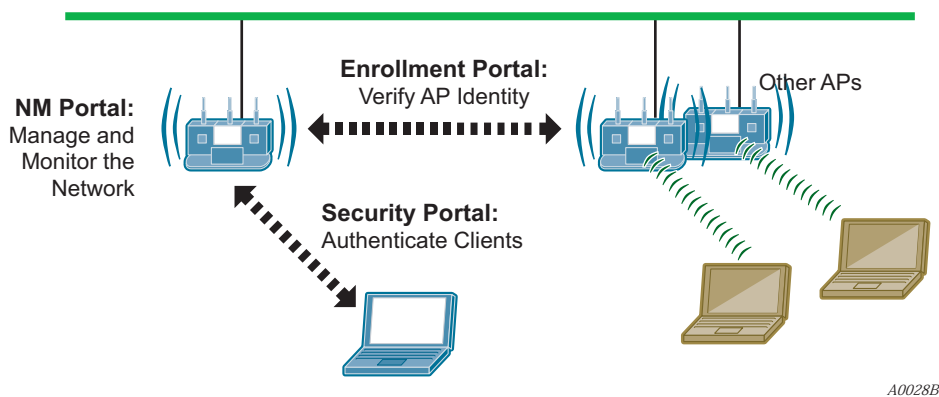
Portal Architecture

To support the range of network sizes and configurations served by Airgo products, Airgo 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 Airgo 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 NMS Pro, the Airgo Professional Network Management System.
Security	Security portal services include support for secure user authentication by way of a RADIUS server internal to the Airgo 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 Airgo wireless network requires an enrollment server to verify the identity of Airgo 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 NMS Pro has been implemented as the enterprise network management solution.

Figure 2 illustrates portal services within the Airgo 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 Airgo 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

Airgo 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, Airgo NMS Pro, Airgo 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 Airgo 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 Airgo 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 Airgo guest access feature (see “Guest Access” on page 6).

Airgo supports interface-based VLANs and user-based VLANs. Interface VLANs separate traffic according to the Ethernet and radio interfaces on the Airgo 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 enterprise work groups and differentiating among categories of users. The Airgo 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.

Airgo 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 Airgo 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 Airgo AP supports flexible, secure managing of guest access at corporate locations. By contrast with most other guest access solutions, the Airgo 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

Airgo 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)

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

Integration With the Existing Wired Network

Airgo wireless networking solutions are standards-compliant to ensure seamless integration with existing wired network infrastructures. The following integration features are included with all Airgo 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 Airgo 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 Airgo 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.”
NMS Pro	The NMS Pro 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 <i>NMS Pro Installation and User Guide</i> .

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](#)
- [Assessing Coverage and Capacity Requirements](#)
- [Assessing Security Needs and Architecture](#)
- [Planning Network Features](#)

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:

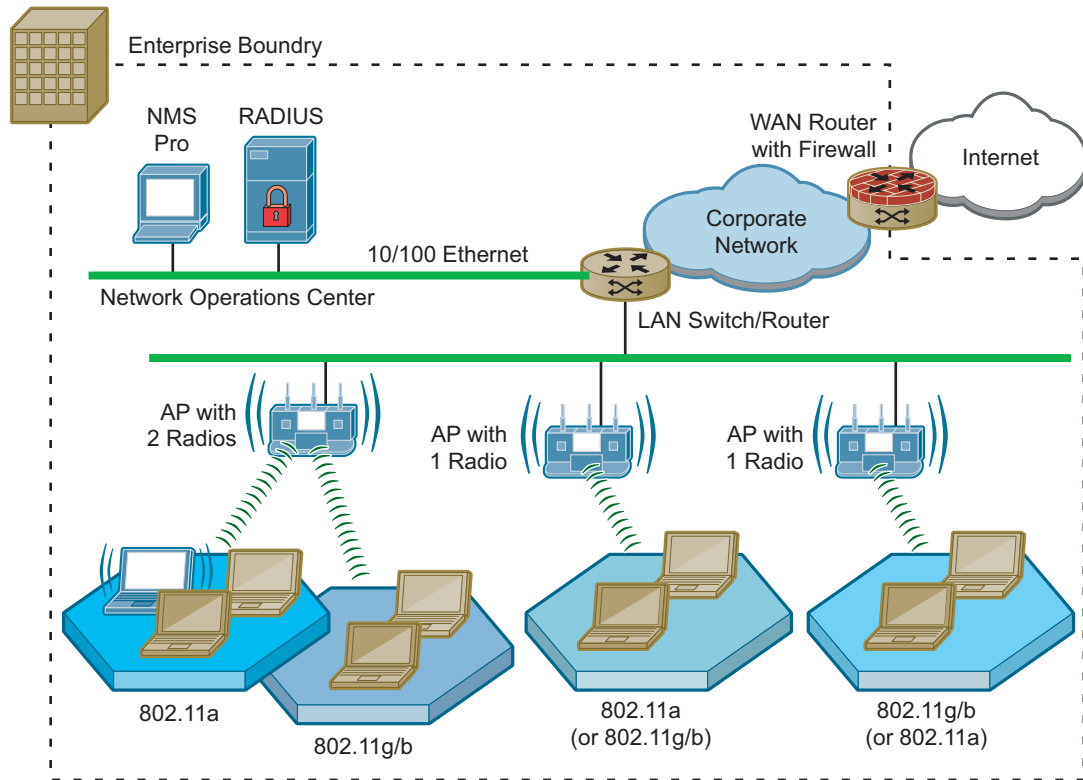
- Coverage and capacity requirements—Identify the numbers and types of access points to install and determine optimal placement.
- Security needs—Choose a security architecture and features.
- Network management—Choose a method to manage the network and monitor its health.
- Network features—Determine 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 Airgo wireless network. Airgo 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 Airgo NMS Pro for enterprise network management.

Figure 3: Typical Wireless Network

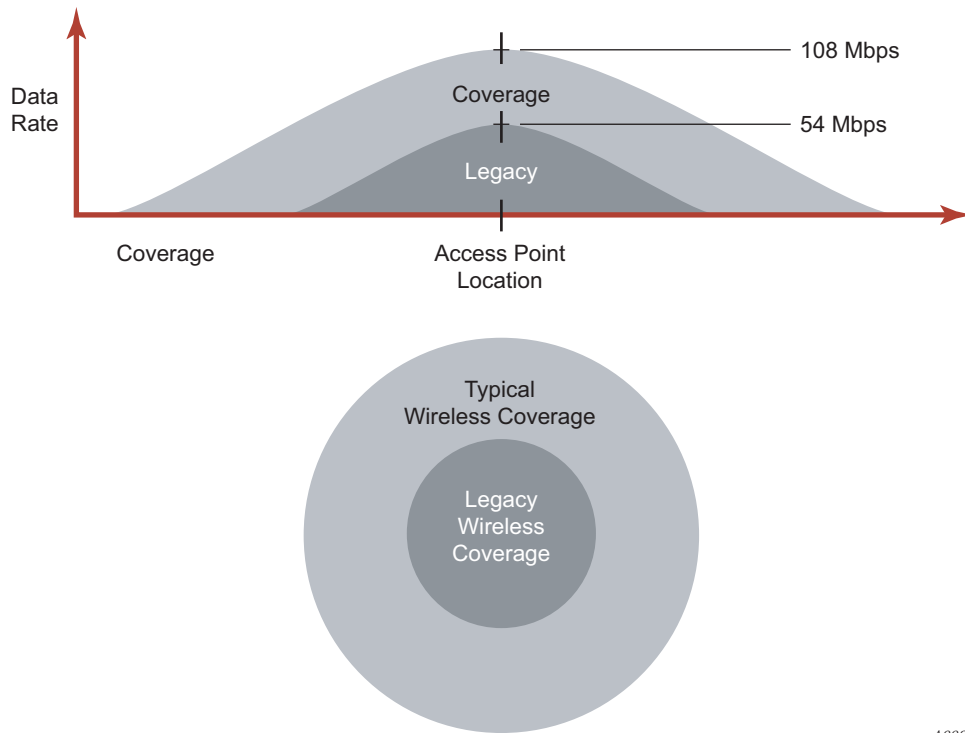


A0008C

Assessing Coverage and Capacity Requirements

Airgo 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 Airgo wireless coverage. Each Airgo 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: Airgo AP Coverage Compared with Other Access Points

A0020A

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 Airgo 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, Airgo offers a selection of features to satisfy all your security needs.

Three aspects of security require planning and decisions:

- Enrollment—Specifying the Airgo AP or NMS Pro 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 12). For large offices and campuses, it is recommended to use the enrollment module within NMS Pro as the enrollment server. The process of enrollment is discussed in “Enrolling APs” on page 165.

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 Airgo 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 Airgo 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 Airgo 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 Airgo NMS Pro network management application, which provides a comprehensive network management solution. Install the NMS Pro server on any suitably configured network computer, and permit network administrators to obtain access from any designated client station. For more information, see the *Airgo NMS Pro Installation and Configuration Guide*.

NMS Pro 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 NMS Pro. 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 Airgo 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	<p>Determine the network management structure.</p> <ul style="list-style-type: none"> • A network management solution such as NM Portal or NMS Pro is strongly recommended for all multiple AP installations. • NM Portal is recommended for small to mid-size networks. • NMS Pro is recommended for large enterprise networks. NMS Pro 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	<p>Determine how to verify the identity of users requesting access to the network. An authentication scheme is required for all except Open access.</p> <ul style="list-style-type: none"> • 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. <p>The Airgo AP can take advantage of the authentication services provided by an external third party RADIUS server, or the internal RADIUS security portal on the Airgo 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.</p> <p>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.</p> <p>The chosen authentication method influences how services can be configured in the network.</p>
Security Modes	<p>Choose WPA, WEP, or open security modes.</p> <ul style="list-style-type: none"> • 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.

Feature	Planning Issues
VLAN	<p>VLANs permit the network to be segmented according to functional needs without the restrictions of the physical topology.</p> <ul style="list-style-type: none"> • If your enterprise uses multiple VLANS, they can be supported in the wireless network. • Multiple VLANs are required for guest access.
SSID	<p>Decide whether one or multiple SSIDs will be supported.</p> <ul style="list-style-type: none"> • 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	<p>Quality of Service (QoS) allows you to set priorities for user traffic, thereby increasing the likelihood that critical data will obtain the needed priority.</p> <p>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.</p> <ul style="list-style-type: none"> • Default and custom mappings are compatible with other feature selections.
Service Profile	<p>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.</p> <p>Once created, a service profile can be bound to an SSID with or without a specified user group.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Decide whether the network will support guest users and if so, how guest access will be managed.</p> <ul style="list-style-type: none"> • 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.

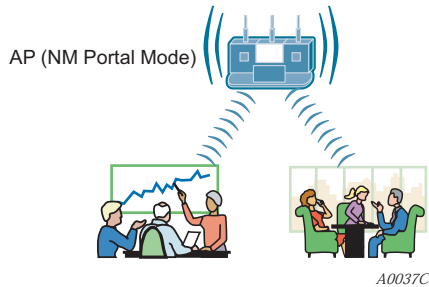
Example Deployment Scenarios

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	<input checked="" type="checkbox"/> One AP	<input type="checkbox"/> Multiple APs	<input type="checkbox"/> Wireless Backhaul
Network Management	<input checked="" type="checkbox"/> NM Portal	<input type="checkbox"/> NMS PRO	
User Authentication	<input type="checkbox"/> Built-In Security Portal	<input type="checkbox"/> External RADIUS Server	
Security Modes	<input checked="" type="checkbox"/> WPA (default)	<input type="checkbox"/> Open	<input type="checkbox"/> WEP
VLAN	<input checked="" type="checkbox"/> Default VLAN	<input type="checkbox"/> Multiple VLANs	
SSID	<input checked="" type="checkbox"/> Single SSID (default)	<input type="checkbox"/> Multiple SSIDs	
Quality of Service (Class of Service - COS)	<input checked="" type="checkbox"/> Default COS Mappings	<input type="checkbox"/> Custom COS Mappings	
Service Profile	<input checked="" type="checkbox"/> Default Service Profile	<input type="checkbox"/> Custom Service Profiles	
Guest Access	<input checked="" type="checkbox"/> Disabled (default)	<input type="checkbox"/> Enabled	

A0036A

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) Airgo AP	<ol style="list-style-type: none"> 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.
Confirm that the network is up	<p>References: “Initializing a Normal AP” on page 33, “Initializing the Portal AP” on page 36</p> <ul style="list-style-type: none"> • 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. <p>References: “Viewing IP Topology” on page 169 and “Managing Client Stations” on page 86.</p>

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

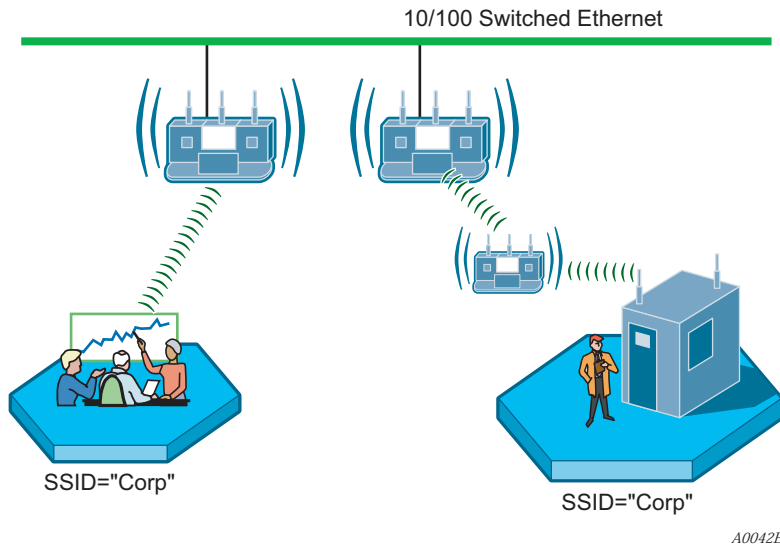


Figure 8 summarizes the feature decisions for this example. The security portal capability within NM Portal provides authentication for the backhaul AP. The security mode is WPA with pre-shared keys (PSK). A single SSID is in place, and the default VLAN, QoS, and service profiles are used.

Figure 8: Example 2 Feature Decisions

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

A0036B

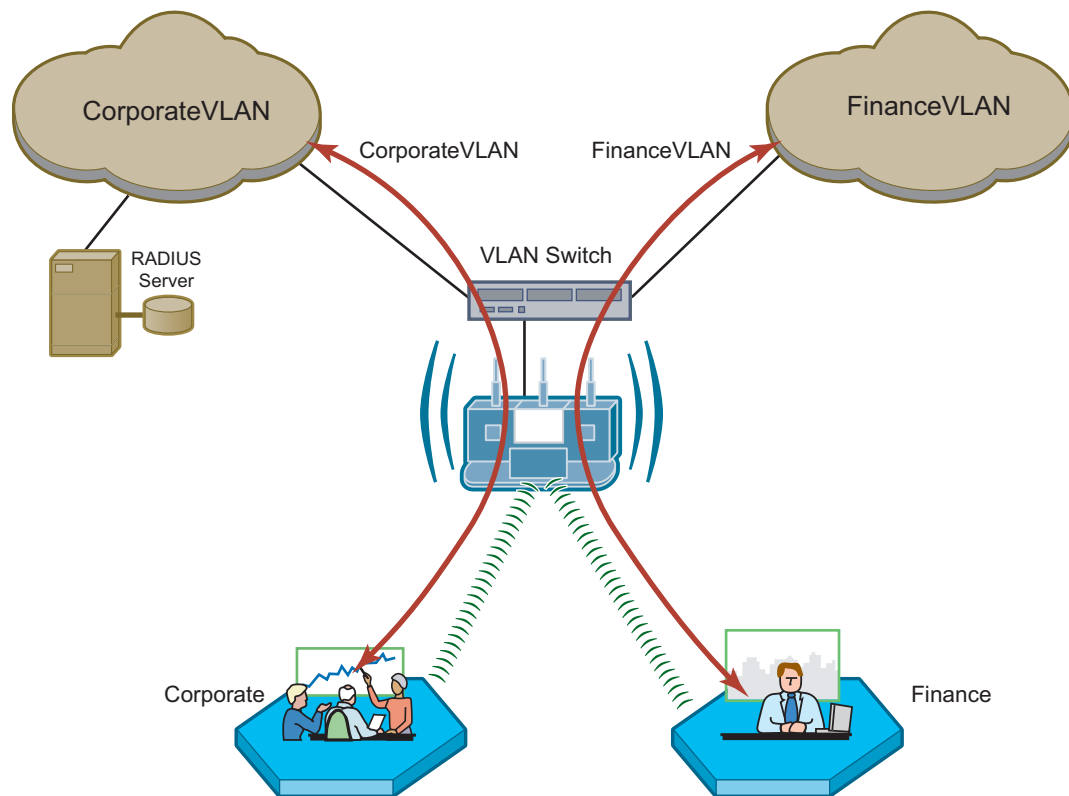
Example 3: Mid-size business, multiple SSIDs, multiple VLANs

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 Airgo 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



A0044B

Figure 10: Example 3 Feature Decisions

Physical Network	<input type="checkbox"/> One AP	<input checked="" type="checkbox"/> Multiple APs	<input checked="" type="checkbox"/> Wireless Backhaul
Network Management	<input checked="" type="checkbox"/> NM Portal	<input type="checkbox"/> NMS PRO	
User Authentication	<input type="checkbox"/> Built-In Security Portal	<input checked="" type="checkbox"/> External RADIUS Server	
Security Modes	<input checked="" type="checkbox"/> WPA (default)	<input type="checkbox"/> Open	<input type="checkbox"/> WEP
VLAN	<input type="checkbox"/> Default VLAN	<input checked="" type="checkbox"/> Multiple VLANs	
SSID	<input type="checkbox"/> Single SSID (default)	<input checked="" type="checkbox"/> Multiple SSIDs	
Quality of Service (Class of Service - COS)	<input type="checkbox"/> Default COS Mappings	<input checked="" type="checkbox"/> Custom COS Mappings	
Service Profile	<input type="checkbox"/> Default Service Profile	<input checked="" type="checkbox"/> Custom Service Profiles	
Guest Access	<input checked="" type="checkbox"/> Disabled (default)	<input type="checkbox"/> 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	<ol style="list-style-type: none"> 1 Identify the RADIUS server for each authentication zone. 2 Select the authentication option for the SSID, with reference to the defined authentication zone. <p>References: “Configuring SSID Parameters” on page 78 and “Configuring Authentication Zones” on page 143</p>
Set up VLANs	<ol style="list-style-type: none"> 1 Choose the VLAN structure for the network. 2 Configure the VLANs. <p>Reference: “Configuring VLANs” on page 105.</p>
Add VLANs to the service profiles	<ol style="list-style-type: none"> 1 Define or modify service profiles to include VLAN selection. 2 Bind each profile to an SSID with an existing or new user group. <p>Reference: “Profile Table” on page 84 and “SSID Details” on page 82.</p>

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

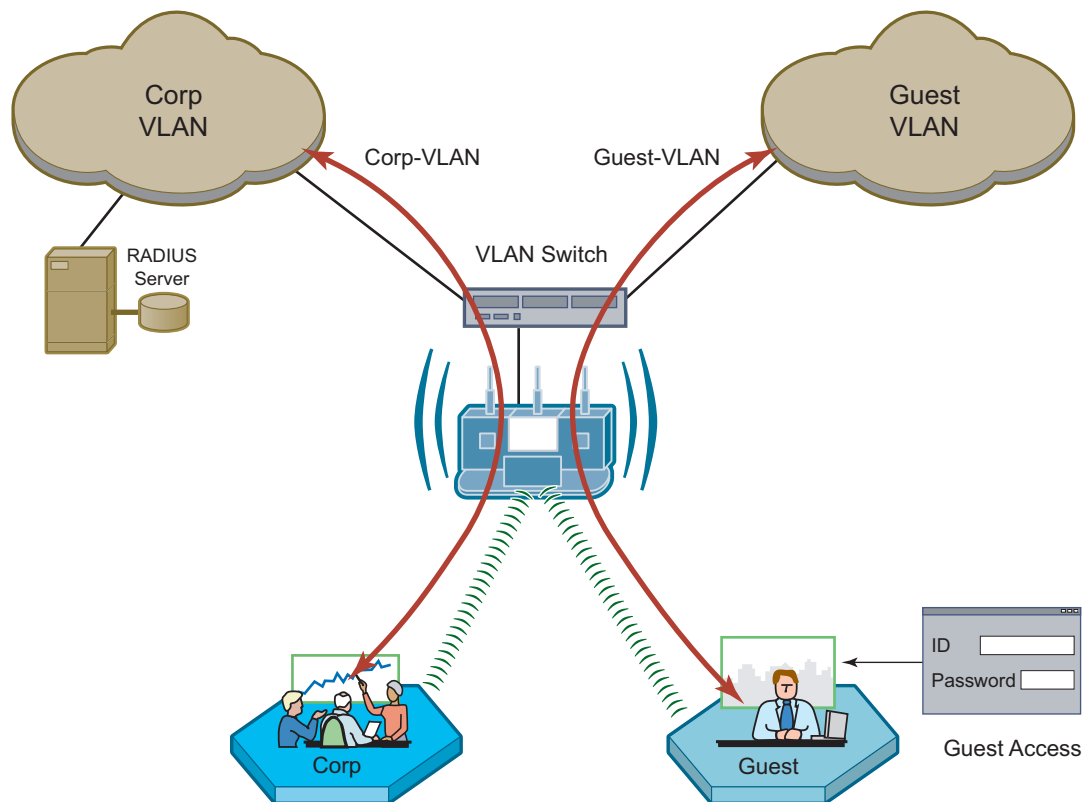
Acme Works is now a widely known and successful enterprise. With an ever increasing number of visitors requiring network access, the network administrator decides to implement a corporate guest access solution.

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



A0045D

Figure 12: Example 4 Feature Decisions

Physical Network	<input type="checkbox"/> One AP	<input checked="" type="checkbox"/> Multiple APs	<input checked="" type="checkbox"/> Wireless Backhaul
Network Management	<input checked="" type="checkbox"/> NM Portal	<input type="checkbox"/> NMS PRO	
User Authentication	<input type="checkbox"/> Built-In Security Portal	<input checked="" type="checkbox"/> External RADIUS Server	
Security Modes	<input checked="" type="checkbox"/> WPA (default)	<input checked="" type="checkbox"/> Open	<input type="checkbox"/> WEP
VLAN	<input type="checkbox"/> Default VLAN	<input checked="" type="checkbox"/> Multiple VLANs	
SSID	<input type="checkbox"/> Single SSID (default)	<input checked="" type="checkbox"/> Multiple SSIDs	
Quality of Service (Class of Service - COS)	<input type="checkbox"/> Default COS Mappings	<input checked="" type="checkbox"/> Custom COS Mappings	
Service Profile	<input type="checkbox"/> Default Service Profile	<input checked="" type="checkbox"/> Custom Service Profiles	
Guest Access	<input type="checkbox"/> Disabled (default)	<input checked="" type="checkbox"/> 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	<ul style="list-style-type: none"> Configure a VLAN for guest access. Reference: “Configuring VLANs” on page 105.
Create guest service profile	<ul style="list-style-type: none"> Add a guest service profile with the guest VLAN and desired COS and open security. Reference: “Profile Table” on page 84 and “SSID Details” on page 82.
Configure landing page	<ol style="list-style-type: none"> Choose an internal or external landing page. Assign guest password. Reference: “Configuring Guest Access” on page 156

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 NMS Pro 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 NMS Pro. 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

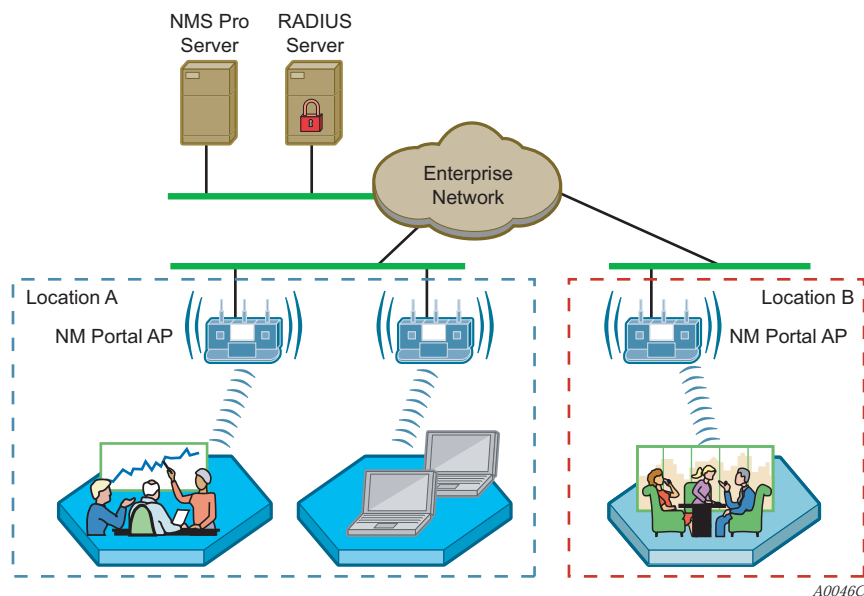


Figure 14: Example 5 Feature Decisions

Physical Network	<input type="checkbox"/> One AP	<input checked="" type="checkbox"/> Multiple APs	<input checked="" type="checkbox"/> Wireless Backhaul
Network Management	<input checked="" type="checkbox"/> NM Portal	<input checked="" type="checkbox"/> NMS PRO	
User Authentication	<input checked="" type="checkbox"/> Built-In Security Portal	<input checked="" type="checkbox"/> External RADIUS Server	
Security Modes	<input checked="" type="checkbox"/> WPA (default)	<input checked="" type="checkbox"/> Open	<input type="checkbox"/> WEP
VLAN	<input type="checkbox"/> Default VLAN	<input checked="" type="checkbox"/> Multiple VLANs	
SSID	<input type="checkbox"/> Single SSID (default)	<input checked="" type="checkbox"/> Multiple SSIDs	
Quality of Service (Class of Service - COS)	<input type="checkbox"/> Default COS Mappings	<input checked="" type="checkbox"/> Custom COS Mappings	
Service Profile	<input type="checkbox"/> Default Service Profile	<input checked="" type="checkbox"/> Custom Service Profiles	
Guest Access	<input type="checkbox"/> Disabled (default)	<input checked="" type="checkbox"/> 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 NMS Pro	Reference: <i>NMS Pro Installation and Configuration Guide</i>
Enroll APs	<ul style="list-style-type: none"> Use the NM Portal in the local building or the campus NMS Pro system to enroll additional APs. Reference: “Enrolling APs” on page 165 or the <i>NMS Pro Installation and Configuration Guide</i>
Create and distribute policies	<ul style="list-style-type: none"> Use NMS Pro to create configuration policies and distribute them to APs across the network. Reference: <i>NMS Pro Installation and Configuration Guide</i>

3 Installing the Access Point Using the Configuration Interfaces

This chapter explains how to install and quickly configure the Airgo 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 Airgo Access Point shipping package contains the following items:

- Airgo Access Point
- Power supply and separate AC cord
- Software and documentation

System Requirements

The following are required to connect to the Airgo 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

Airgo 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 Airgo 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:

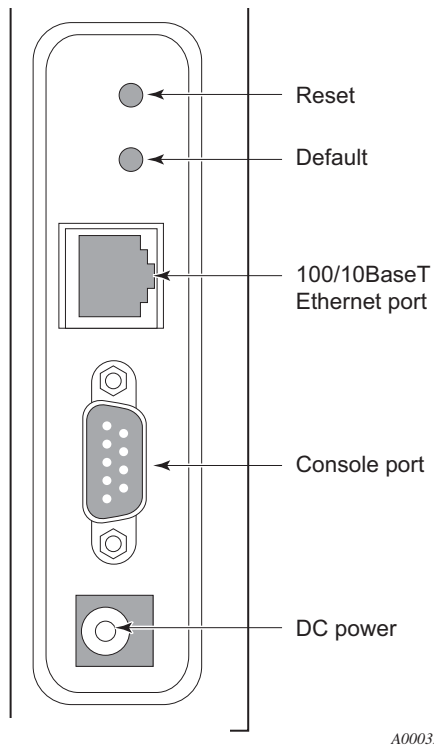
- IP address assigned to the AP (fixed IP address or DHCP-reserved address)
- IP addresses for the default gateway, DNS Server and NTP Server, if DHCP is not used to provide IP addresses
- IP address of the SMTP email server, if the AP is to send alerts to a specified email address
- Email address of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

Installing the Access Point

Follow these steps to install the Airgo 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 Airgo Access Point powers up automatically.

Figure 15: Airgo AP Connections

Using Power Over Ethernet

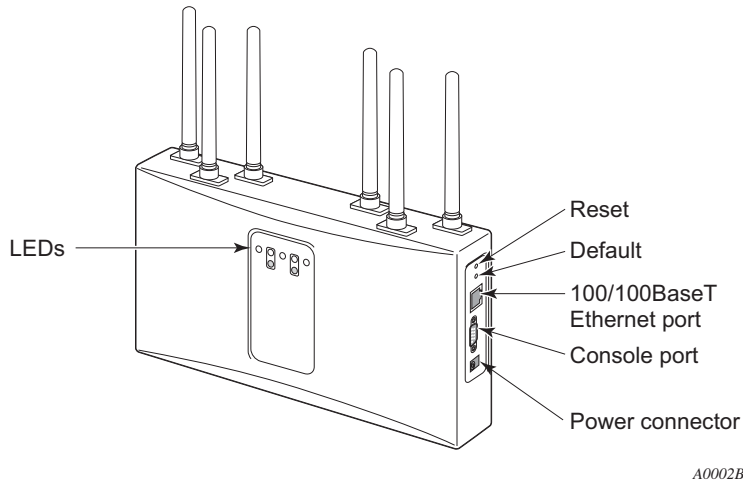
Power-over-Ethernet, based on the 802.3af standard, can be used to supply power to the Airgo AP. If both DC power and power-over-Ethernet are used at the same time, then failover takes place automatically in the event that one of the power sources is lost. For failover, the following rules apply:

- 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 Airgo AP is positioned in an upright position for airflow and antenna placement (Figure 16).

Figure 16: Airgo AP Placement



Verifying the Installation

To verify the Airgo 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: Airgo AP LEDs

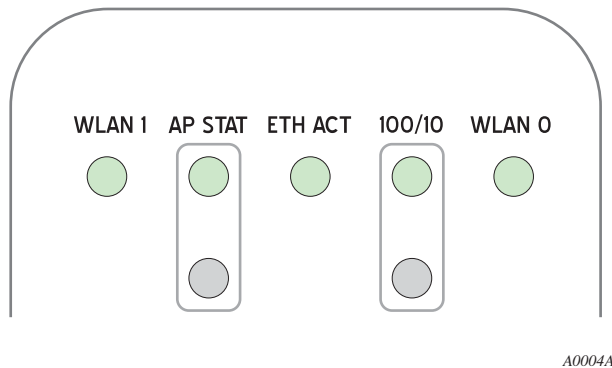


Table 7: LED Definitions

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. <ul style="list-style-type: none"> • 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 217.
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 217.
CLI	Use the command sequence <pre>config system > reset-to-defaults factory-defaults</pre>
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: <ol style="list-style-type: none">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 Airgo 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 Airgo 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:

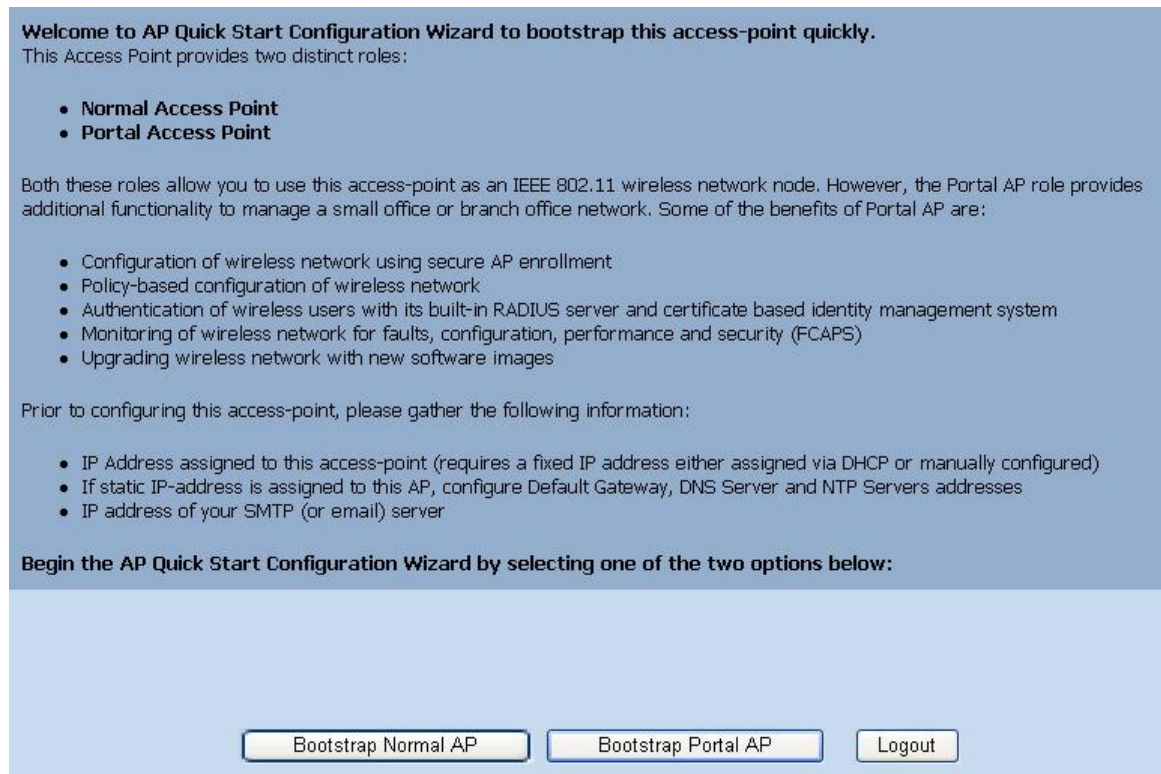
- 1 Launch the web browser.
 - a If your network has a DHCP server, enter the DHCP-assigned address of the AP in the address bar.
 - b If your network does not use a DHCP server, assign the static address 192.168.1.1/24 to your computer, and then enter `https://192.168.1.254` in the browser address bar.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



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 Airgo 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 Airgo network for faults, configuration alerts, performance and security (FCAPS)
- Upgrade of the Airgo 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

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

The screenshot shows a configuration interface for network identity. It includes the following sections and fields:

- SSID:** A text input field for "SSID Name *" containing the value "DeerCreekCo".
- Network Density:** Three radio buttons labeled "Low", "Medium", and "High". The "Low" option is selected.
- Bootstrap Security Mode *:** Three radio buttons labeled "WPA Pre-Shared Key with AES", "WEP", and "Open Access". The "WPA Pre-Shared Key with AES" option is selected.
- WEP:** Two radio buttons labeled "WEP-64" and "WEP-128". Neither is selected.
- WPA-PSK Security Mode:** A text input field for "WPA-PSK" containing the value "password".
- WEP Mode:** A text input field for "WEP Key" which is currently empty.

At the bottom of the panel, there are three buttons: "<< Back", "Next >>", and "Logout".

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 an 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

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: <ul style="list-style-type: none"> 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.

i **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.

- 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

- 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

- 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 Airgo 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



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

The screenshot shows the 'AP Explorer | Home' interface. On the left is a 'Menu Tree' with options like 'AP Explorer - Home', 'AP Quick Start', 'System Services', 'Wireless Services', 'Networking Services', 'Security Services', and 'Guest Access Services'. Below the menu tree are buttons for 'Launch NM Explorer', 'MANAGE WIRELESS NETWORK', and 'Alarm Summary' (showing 92 alarms). The main content area features a welcome message and four summary tables:

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

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

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

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

The screenshot shows the 'IP CONFIG' tab selected in the 'AP Quick Start | Bootstrap Configuration' interface. At the top, there are navigation tabs: IP CONFIG, RADIO CONFIG, CLOCK CONFIG, PORTAL CONFIG, and ADMIN EMAIL, along with HELP and LOGOUT buttons. Below the tabs is a breadcrumb trail: AP Quick Start | Bootstrap Configuration | IP Configuration. A text box explains that the web pages summarize essential configuration parameters for bootstrapping the AP. The 'Management IP Configuration' section has a 'DHCP Assigned IP Address' checkbox checked and labeled 'Enable'. Below it are input fields for 'DNS IP Address *' (192.168.168.1), 'Management IP Address/Maskbits *' (192.168.168.24/24), and 'Gateway IP Address' (192.168.168.254). The 'System Identity Configuration' section has input fields for 'Host Name *' (AP_00-0A-F5-00-01-F2), 'AP Location' (Floor 1 South), and 'Administrator Contact' (admin@DeerCreekCo.com). Both sections have 'APPLY' and 'RESET' buttons.

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.

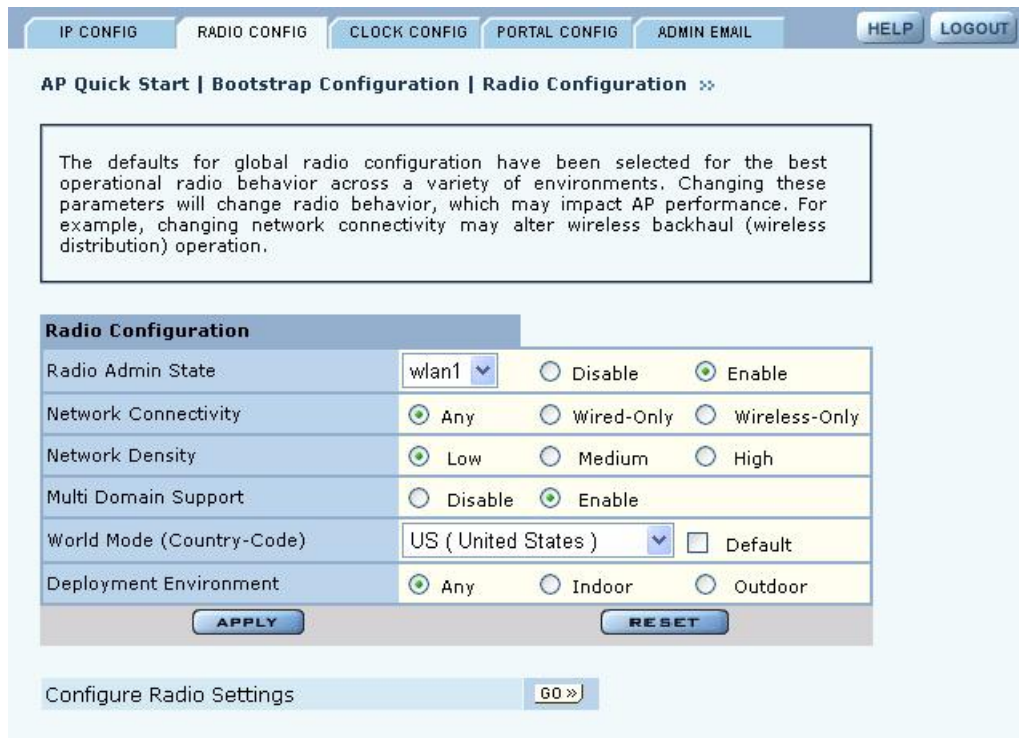
Field	Description
DNS IP Address	<p>Enter the IP address of the server or servers supplying DNS service. This is required if the IP address is not obtained automatically. The default is the DNS server for the existing network.</p> <p>Multiple DNS server addresses may be specified, space-separated. The 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.</p> <p>If you delete DNS servers, only those added manually are deleted. DHCP-assigned DNS servers continue to be available.</p>
Management IP Address/Maskbits	<p>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 .</p>
Gateway IP Address	<p>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.</p>
Host Name	<p>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).</p>
AP Location	<p>Enter the physical location of the AP as a text string.</p>
Administrator Contact	<p>Enter contact information for the person responsible for managing this AP (phone or email address).</p>

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



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.

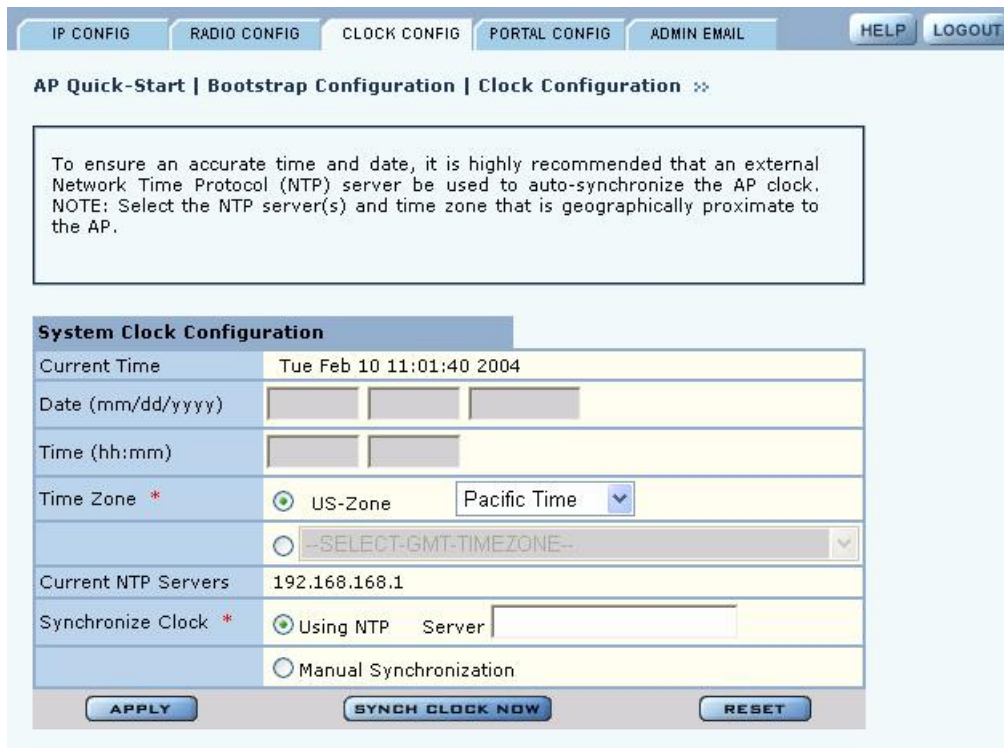
Field	Description
Configure Channel	<p>Select Auto-Select Channel or Assign Fixed Channel options:</p> <ul style="list-style-type: none"> • Auto-Select: Select At Start-up to automatically determine the channel when the AP is booted, or Periodic to auto-select the channel at the specified number of minutes. The default is Periodic and 30 minutes. • Assign Fixed Channel: Select a static channel. <p>In both of these cases, the channel set used for auto-scanning can also be restricted.</p>

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



This tab contains the following settings:

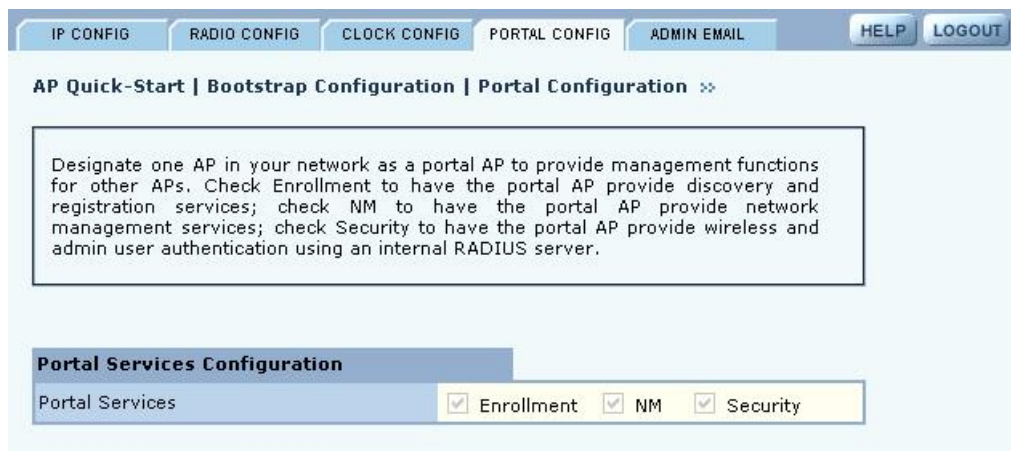
Field	Description
Date	Current date in MM/DD/YYYY format
Time	Current time in HH:MM:SS format (hours 0-23)
Time Zone	US-zone or GMT option. For US zone, click the radio button and select a time zone. For GMT, click the radio button and select an offset in HH:MM format.

Field	Description
Synchronize Clock	<p>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.</p> <p>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.</p> <p>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.</p> <p>If you delete NTP servers, only those added manually are deleted. DHCP-assigned NTP servers continue to be available.</p>

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



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.

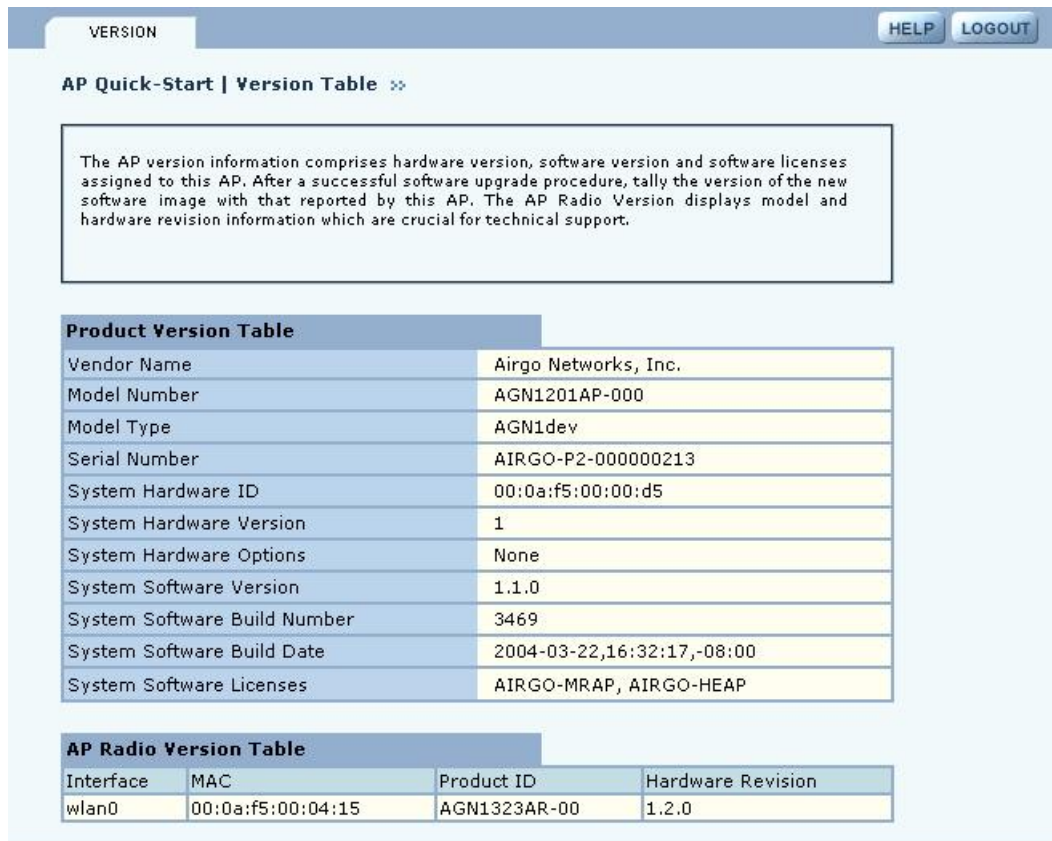
Figure 30: AP Quick Start - Bootstrap Configuration - Admin Email



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



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 Airgo 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



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

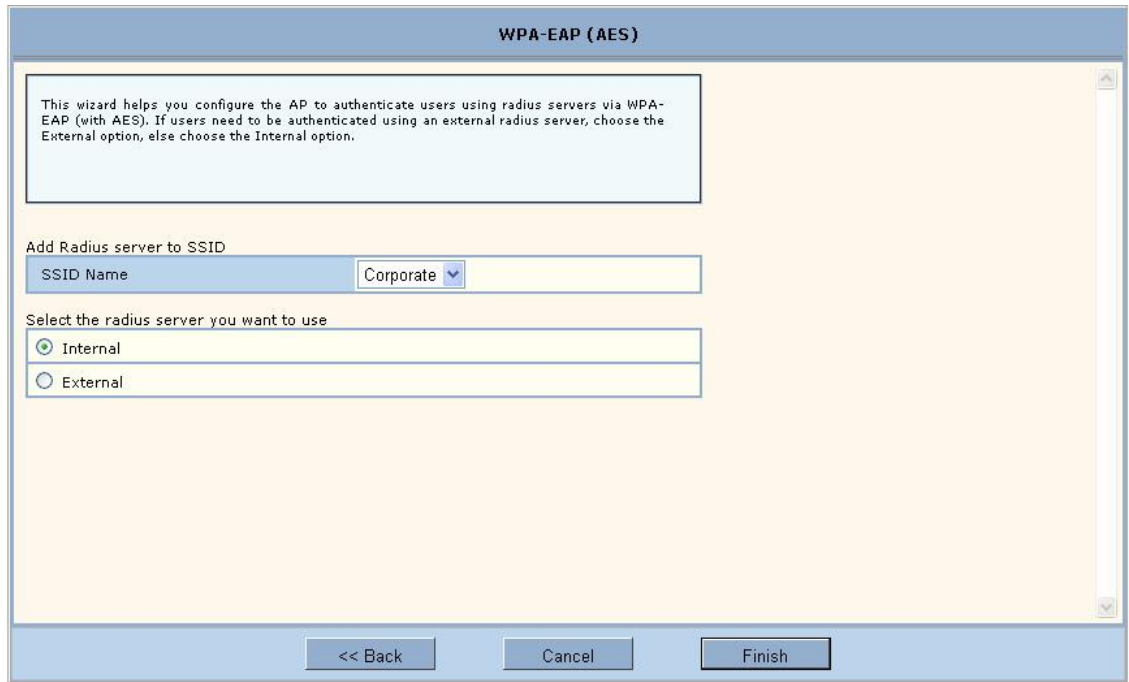
Option	Description
WPA-EAP (with AES encryption)	Configures the AP to work with RADIUS authentication servers. <ul style="list-style-type: none"> The wizard prompts for selection of the internal RADIUS server included in the AP or an external RADIUS server.
WPA-PSK	Configures the AP to work with pre-shared key authentication. <ul style="list-style-type: none"> The wizard prompt for the pre-shared security key.
WEP	Configures the AP to use WEP encryption to support legacy equipment. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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



- 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

The screenshot shows a configuration window titled "User Security: WPA with PSK". It contains a text box with instructions: "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." Below this are three input fields: "SSID Name" with a dropdown menu set to "Corporate", "WPA Pre-Shared-Key" with a masked input field, and "Confirm Key" with another masked input field. At the bottom are three buttons: "<< Back", "Cancel", and "Finish".

- 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	<input type="text"/>	<input checked="" type="radio"/> Default
WEP Key 2	<input type="text"/>	<input type="radio"/> Default
WEP Key 3	<input type="text"/>	<input type="radio"/> Default
WEP Key 4	<input type="text"/>	<input type="radio"/> Default

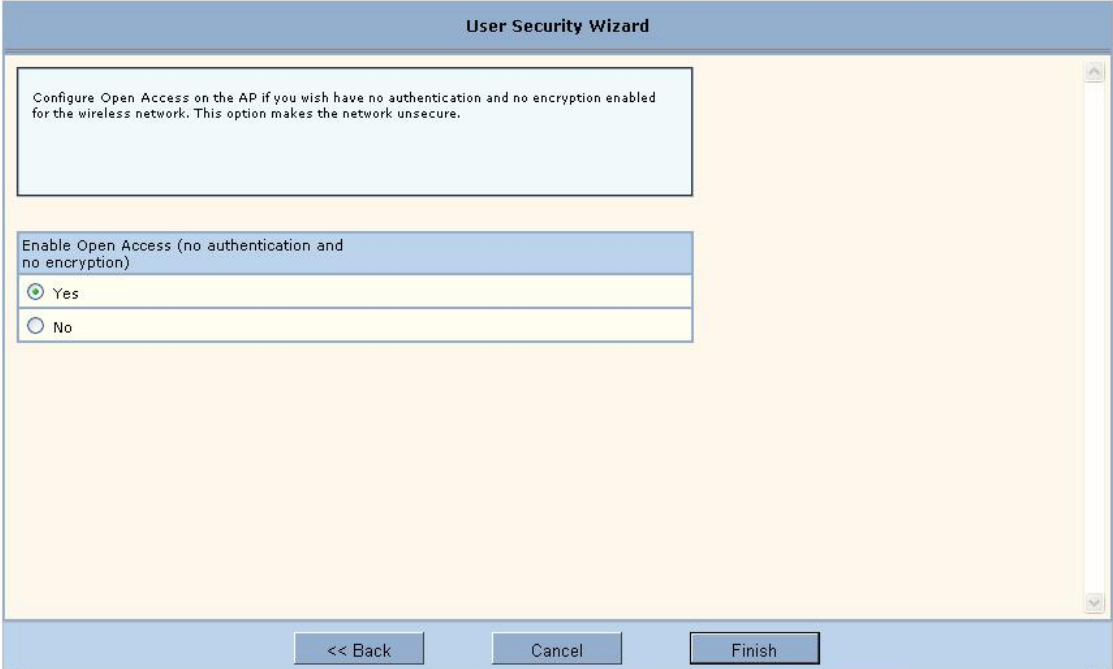
<< Back Cancel Finish

- 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



The screenshot shows a window titled "User Security Wizard". Inside the window, there is a light blue header bar with the title. Below the header, there is a white text box with the following text: "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." Below this text box, there is a section titled "Enable Open Access (no authentication and no encryption)". Under this section, there are two radio button options: "Yes" (which is selected, indicated by a green dot) and "No". At the bottom of the window, there are three buttons: "<< Back", "Cancel", and "Finish".

- 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



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: [Masked]

Confirm Guest Password: [Masked]

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

No

Yes

Allowed Subnet: 192.168.17.1

<< Back Next >>

- 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

The screenshot shows the 'Guest Access Wizard' interface. At the top, a blue header bar contains the text 'Guest Access Wizard'. Below this, a light blue box contains the instruction: '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.' Below the instruction box, the text 'Setup infrastructure for guest access.' is displayed. The main configuration area consists of several fields: 'Allowed Guest VLAN ID' (a dropdown menu), a checked checkbox for 'New VLAN', 'VLAN ID' (a text input field containing '25'), 'VLAN Name' (a text input field containing 'Guest'), and 'Guest QoS' (a dropdown menu containing '2'). At the bottom of the wizard, there are three buttons: '<< Back', 'Close', and 'Finish'.

- 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

- 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 Airgo AP 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 Airgo Access Point radios and explains how to set the configuration using the Airgo 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:

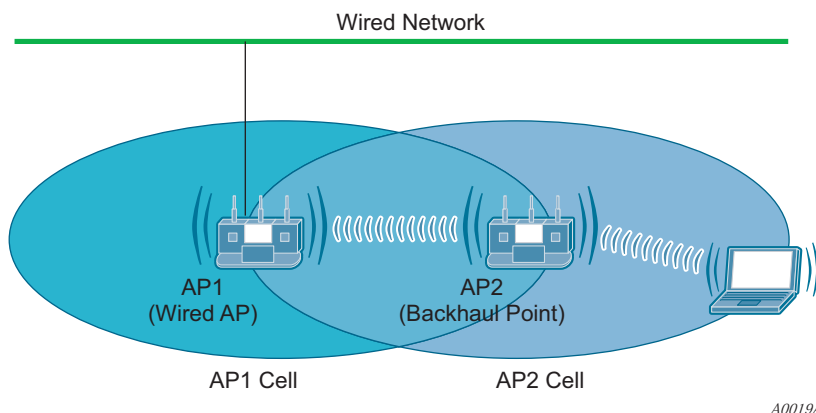
- **Introduction**
- **Configuring Radio Parameters**
- **Setting the Advanced Radio Configuration**
- **Viewing Radio Statistics**
- **Viewing Radio Neighbor Details**
- **Configuring SSID Parameters**
- **Multiple SSIDs**
- **Configuring Inter Access Point Protocol (IAPP)**
- **Performing Radio Diagnostics**

Introduction

The Airgo 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 Airgo 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).

¹Except 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 Airgo 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 Airgo 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 Airgo 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

GLOBAL CONFIG ADMIN STATE CHANNEL CONFIG PERFORMANCE ADMISSION HELP LOGOUT

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	<input checked="" type="radio"/> Any	<input type="radio"/> Wired-Only	<input type="radio"/> Wireless
Network Density	<input checked="" type="radio"/> Low	<input type="radio"/> Medium	<input type="radio"/> High
World Mode			
Multi Domain Support	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
Country Code	<input type="checkbox"/> Default		
	US (United States)		
Deployment Environment	<input checked="" type="radio"/> Any	<input type="radio"/> Indoor	<input type="radio"/> Outdoor
Miscellaneous Configuration			
AP Name in Beacon *	AP-00:0a:f5:00:01:f2		
Background Scanning	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	

APPLY RESET

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	<p>Specify the mode of connectivity to the wired network.</p> <ul style="list-style-type: none"> 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 Airgo AP and whether or not the AP has active Ethernet connectivity. If Any is selected, then the Airgo AP is allowed to change between wireless and wired mode based on a change in Ethernet status. The Wired-Only setting means that the Airgo 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. <p>The default setting of Any is recommended.</p>
Network Density	<p>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 Airgo AP. The default is low; the default setting of “low” is appropriate for maximum coverage.</p>
World Mode - Multi-Domain Support	<p>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.</p>
World Mode - Country Code	<p>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.</p>
World Mode - Deployment Environment	<p>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:</p> <ul style="list-style-type: none"> 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 64). The channel set configuration is set to system determined band configuration. All radios in the AP are reset. <p>For reference, Table 8 provides a list of world modes, including countries, environments, bands, and valid channels.</p>
AP Name in Beacon	<p>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)</p>

Field (continued)	Description
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 64.

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
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

Table 8: World Modes (continued)

Country	Environment	Band	Valid Channel Numbers
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
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

Table 8: World Modes (continued)

Country	Environment	Band	Valid Channel Numbers
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
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

GLOBAL CONFIG ADMIN STATE CHANNEL CONFIG PERFORMANCE ADMISSION HELP LOGOUT

Wireless Services | 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

APPLY RESET

Radio Persona Configuration

Current Radio Persona AP

Persona of Selected Radio Any AP BP

APPLY RESET

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

^aWired 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)

Channel Set Configuration

Channel Set: Band

Channel-list (ex: 1 2...)

Reselect Channel

Current Channel ID: 157

Force Select Best 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	<p>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:</p> <p>Band—Select a specific band, or the system-determined band option (recommended).</p> <ul style="list-style-type: none"> • 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 Airgo 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. <p>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.</p>

 **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

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 Airgo 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	<p>Determines the acknowledgement policy for data packets. The following selections are available:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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 Airgo clients. • Auto-ack – The acknowledgement policy is selected automatically based on current link conditions.
Dot11 QoS	<p>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.</p>

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 69).

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



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-Airgo 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

802.11 POLICY MAC CONFIG HELP LOGOUT

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 11g 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

APPLY RESET

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	<p>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 Airgo enhanced features, which are compatible only with Airgo 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).</p> <ul style="list-style-type: none">• 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	<p>Select to enable 802.11g protection mode, short slot time, and short preamble if the radio is operating in 802.11g mode.</p> <p>If the checkbox is selected, all 3 aspects are enabled; if not, all 3 aspects are disabled. The default setting is disabled.</p>
Select Basic Rate Set	<p>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.</p>

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

The screenshot shows a web interface for configuring the MAC settings of a radio interface. At the top, there are tabs for '802.11 POLICY' and 'MAC CONFIG', along with 'HELP' and 'LOGOUT' buttons. The main heading is 'Wireless Services | Advanced Configuration | MAC Configuration'. A text box contains a note about the default configuration settings. Below this, the 'Radio MAC Configuration' section includes a dropdown for 'Select Radio Interface' set to 'wlan1'. The 'Beacon Configuration' section has input fields for 'Beacon Period (Milliseconds)' (100) and 'DTIM Period (n x Beacon Period)' (1). The 'Threshold Configuration' section has input fields for 'Fragmentation Threshold' (2000), 'RTS Threshold' (2347), 'Short Retry Limit' (100), and 'Long Retry Limit' (100). At the bottom of the configuration area are 'APPLY' and 'RESET' buttons. Below the configuration area, there is a 'Back (Configure Dot11 Policy)' link and a 'GO >>' button.

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

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

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

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.

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:

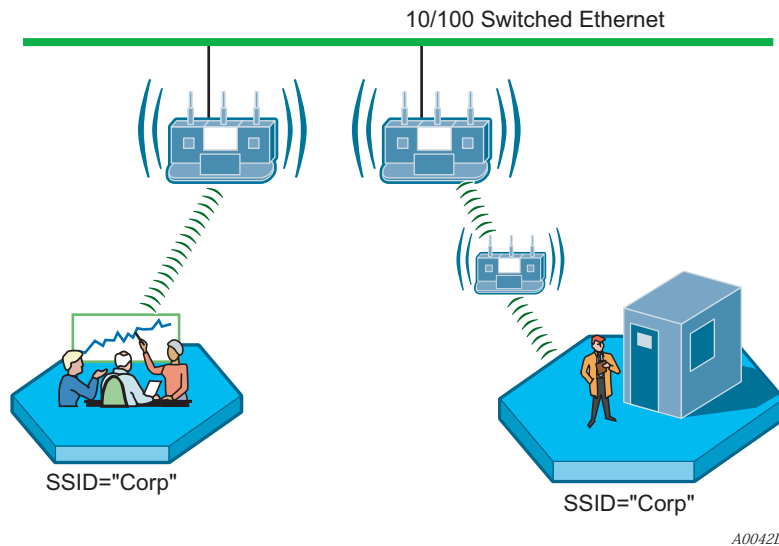
Field	Description
Interface	The AP radio (wlan0 or wlan1)
BSSID	The MAC address of the neighboring AP radio, which determines the BSS
SSID	The name of the network (ESS) in which the AP is operating
BSS Type	Infrastructure or ad-hoc network arrangement
Channel	Current channel of operation for the neighboring 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 Airgo APs, each advertising the same “Corporate” SSID.

Figure 52: Example “Corporate” Network



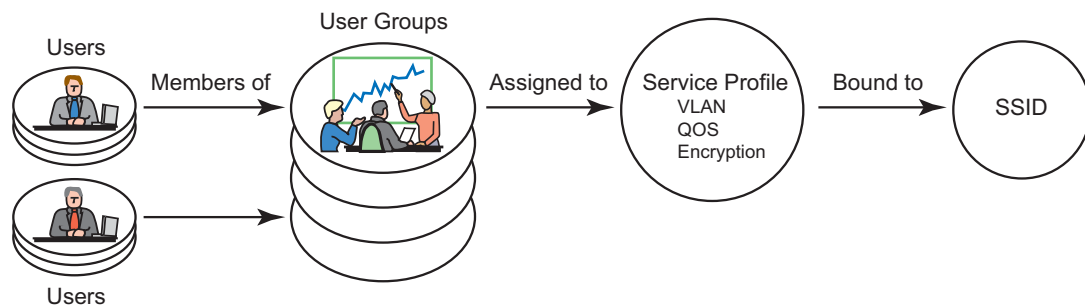
Each Airgo AP is shipped with a default SSID, which must be replaced during the bootstrap process (see “Using AP Quick Start to Initialize the Access Point” on page 31) or from the SSID Configuration panel, as explained in this section. Multiple SSIDs are also supported. “Multiple SSIDs” on page 85 explains 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



A0029

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 127 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.

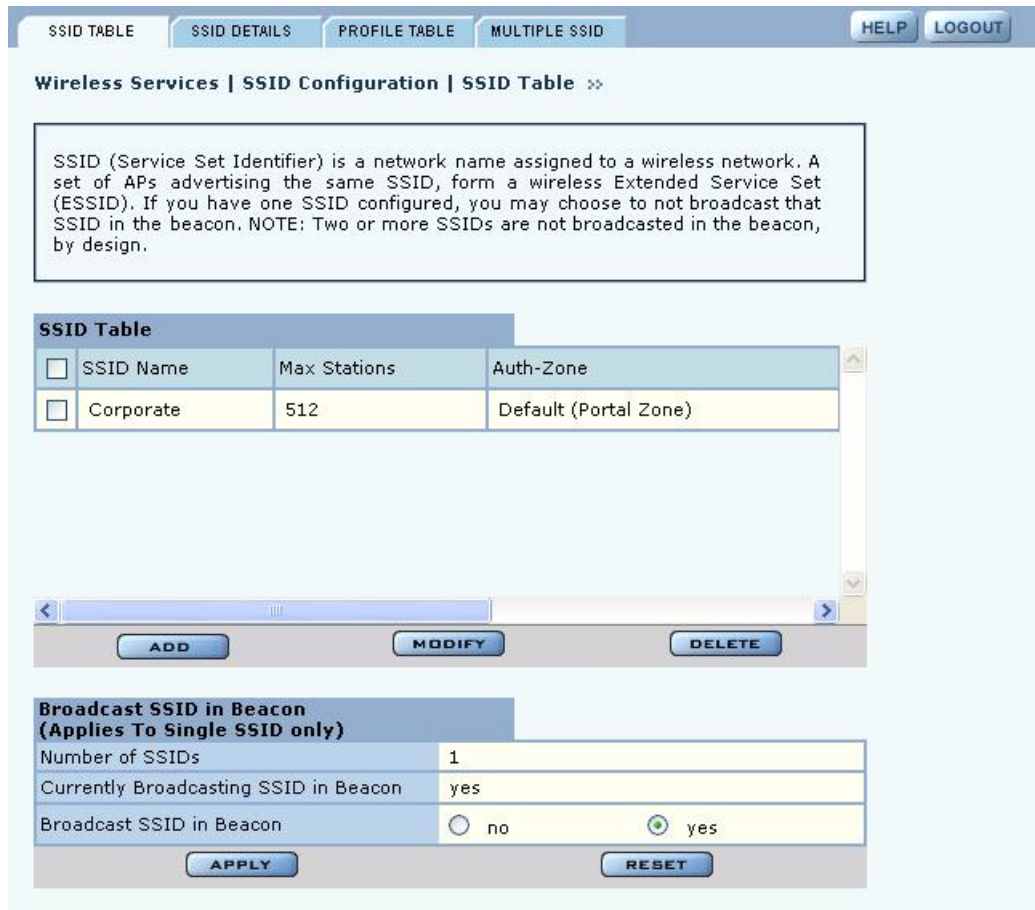
Select **SSID Configuration** from the Wireless Services menu to open the SSID Configuration panel. The panel contains the following tabs:

- **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



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 Airgo AP can be configured to support multiple SSIDs. If this feature is enabled on the Multiple SSID tab (“Multiple SSIDs” on page 85), then it is possible to add new SSIDs from the SSID Table tab, in addition to modifying or deleting an existing SSID.

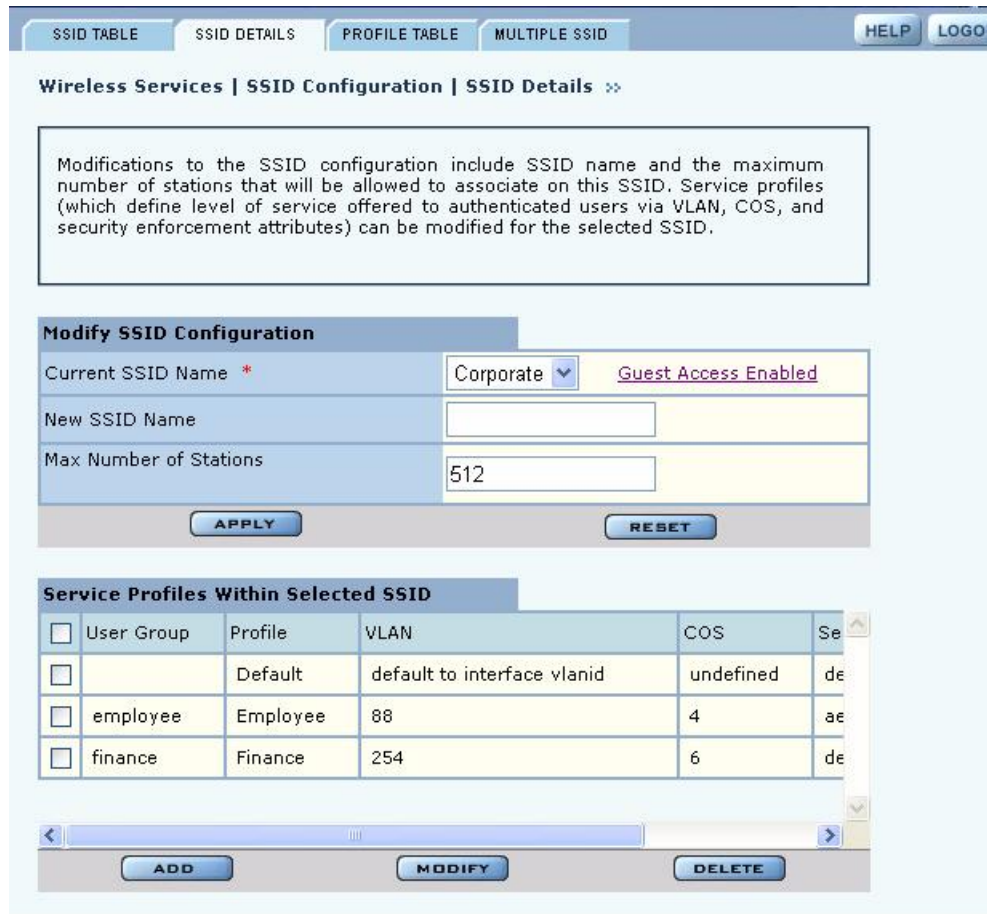
Perform the following functions on the SSID Table tab:

Function	Description
Add new SSID (if multiple SSID is enabled)	<ol style="list-style-type: none"> 1 Click Add and enter the following information: <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> 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)	<p>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.</p> <p>To change the SSID broadcast setting:</p> <ol style="list-style-type: none"> 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



The tab contains two areas. Use the Modify SSID Configuration area to change the current SSID configuration, as described in “SSID Table” on page 80. 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	<ol style="list-style-type: none"> 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 84. 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	<ol style="list-style-type: none"> 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 84. 3 Click Apply.
Delete service profile binding	<ol style="list-style-type: none"> 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 140. 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

The screenshot shows a web-based configuration interface titled "Bind Service Profile to SSID". It contains the following elements:

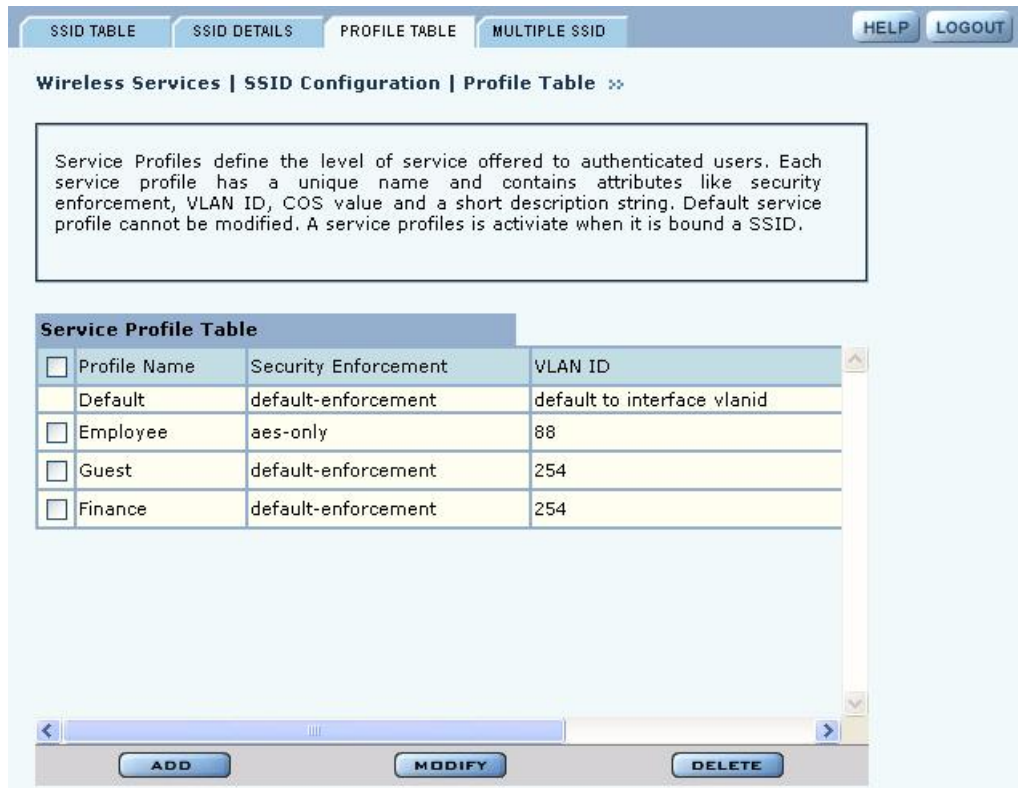
- SSID Name ***: A text input field containing "Corporate".
- User Group Name**: A dropdown menu with a downward arrow, and a checkbox labeled "New Group" to its right.
- Profile**: A dropdown menu showing "Finance" and a link labeled "Add New Profile" to its right.
- Preview Profile Attributes**: A section with three rows:
 - VLAN ID: 254
 - COS Value: 6
 - Security Enforcement: default-enforcement
- Buttons**: Three buttons at the bottom: "APPLY", "CANCEL", and "RESET".

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



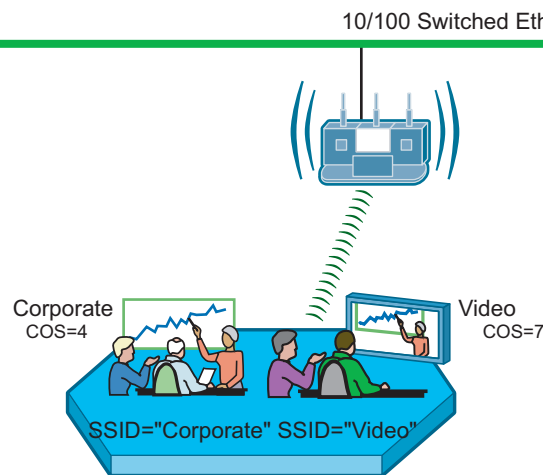
Perform the following functions from this tab:

Function	Steps
Add a new service profile	<ol style="list-style-type: none"> 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 111. 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	<ol style="list-style-type: none"> 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. <p>It is not possible to modify the default profile.</p>
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

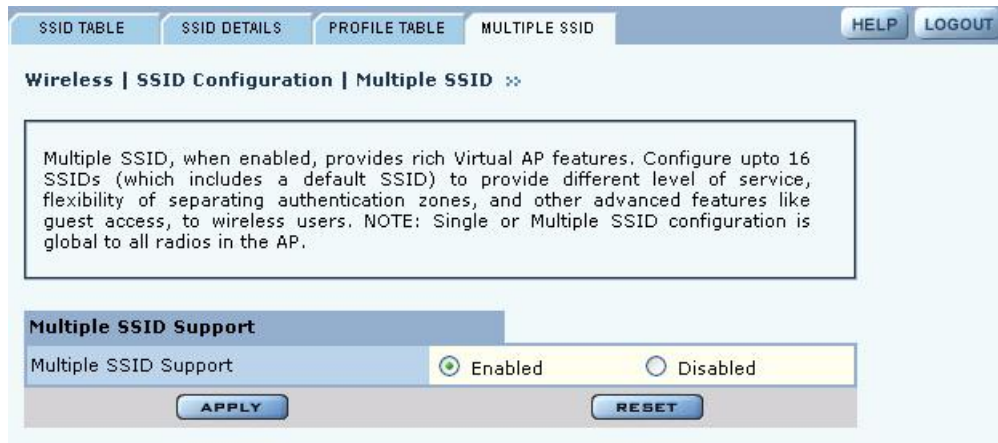


A0043B

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 80).

When multiple SSIDs are enabled on the Airgo AP, that AP no longer broadcasts an SSID in its beacon frame. In order for a client to associate with the Airgo 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 Airgo Client Utility Create function.

Figure 59: SSID Configuration - Multiple SSID



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 Airgo 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



Use this panel to control association to the Airgo 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

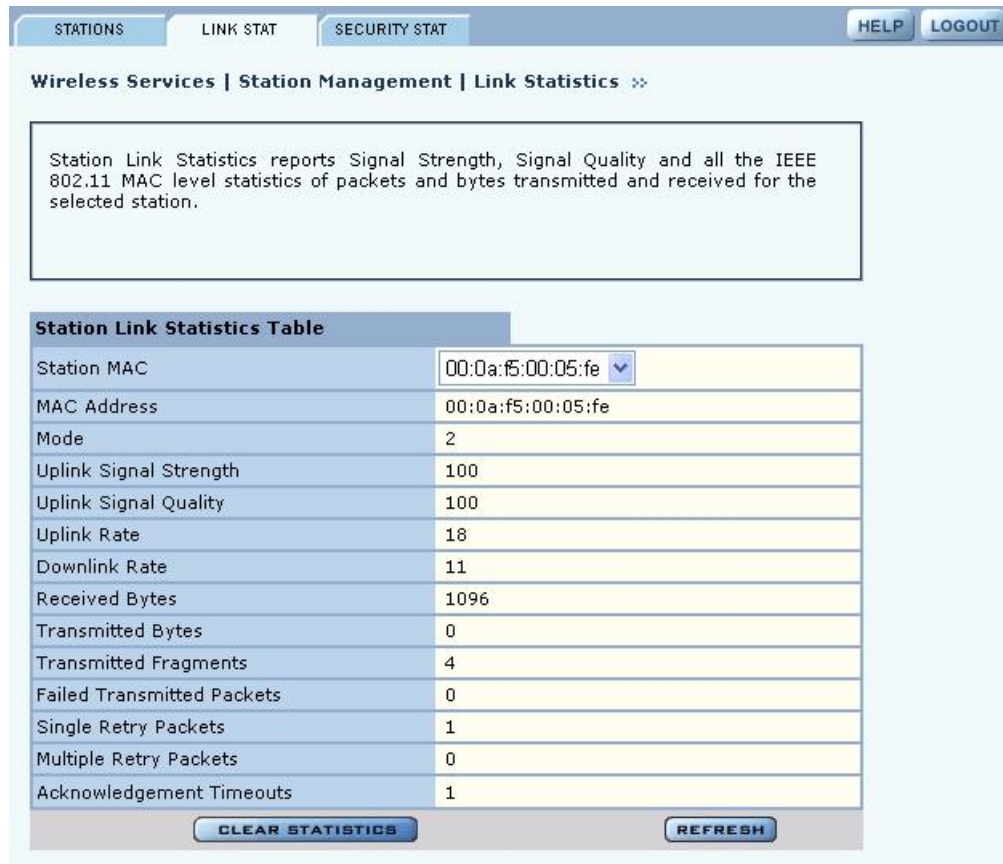
Select a station from the list and click a button at the bottom of the panel to perform any of the following functions:

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



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	

CLEAR STATISTICS REFRESH

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.

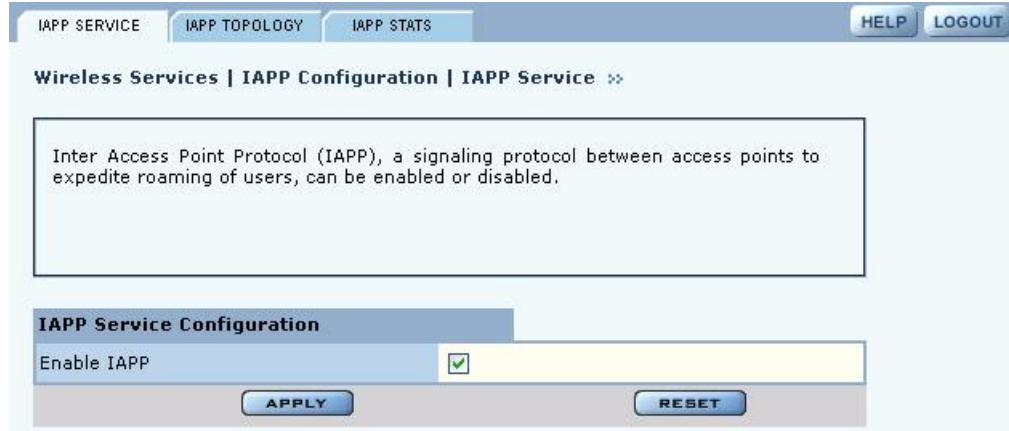
The panel contains the following tabs:

- 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.

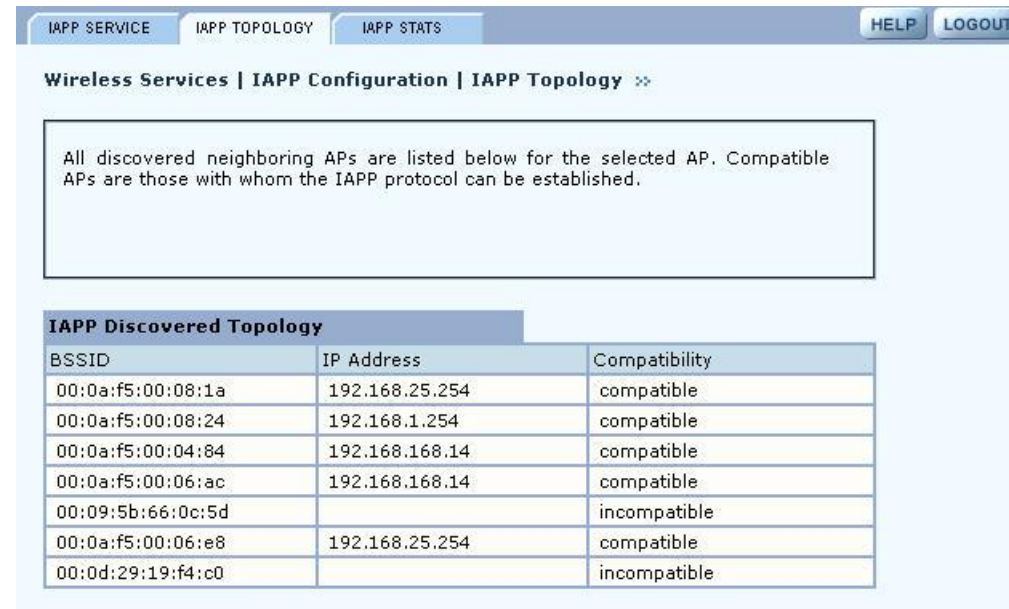
Figure 63: IAPP Configuration - IAPP Service



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).

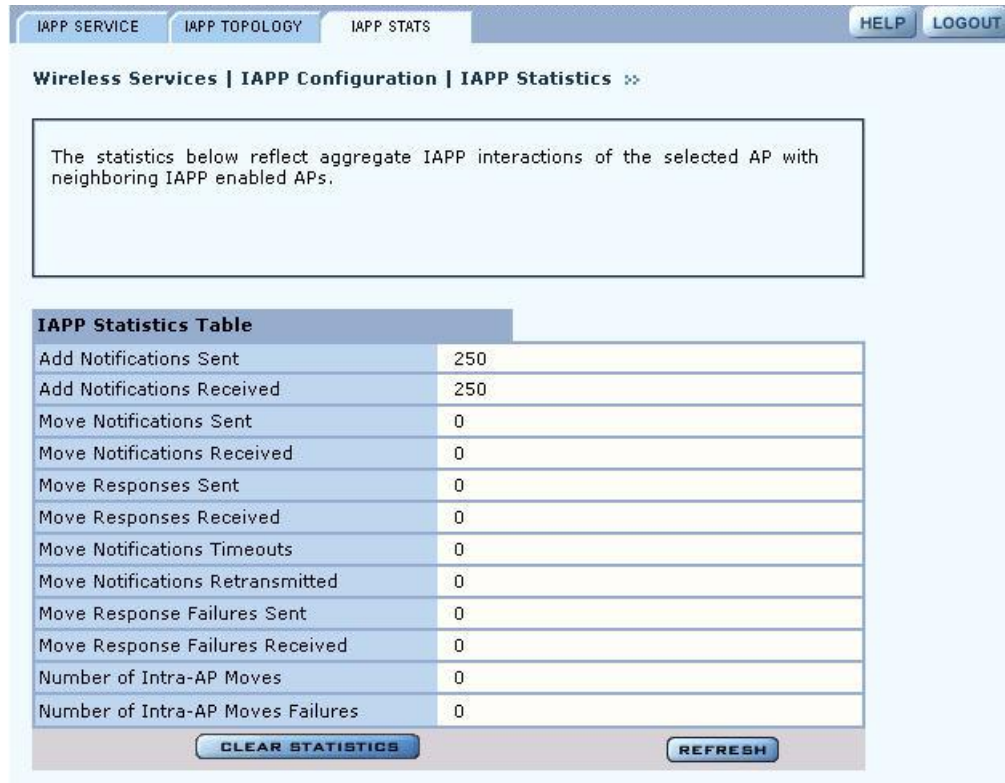
Figure 64: IAPP Configuration - IAPP Topology



IAPP Statistics

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

Figure 65: IAPP Configuration - IAPP Stats



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

The screenshot shows the 'LINK TEST' tab selected. The breadcrumb trail is 'Wireless Services | Radio Diagnostics | Link Test'. There are 'HELP' and 'LOGOUT' buttons in the top right. A text box contains the following description: '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.'

Below the text box is the 'Link Test Table' with the following data:

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

At the bottom of the interface are four buttons: 'ADD', 'DELETE', 'STOP', and 'GRAPH'.

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

- 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.

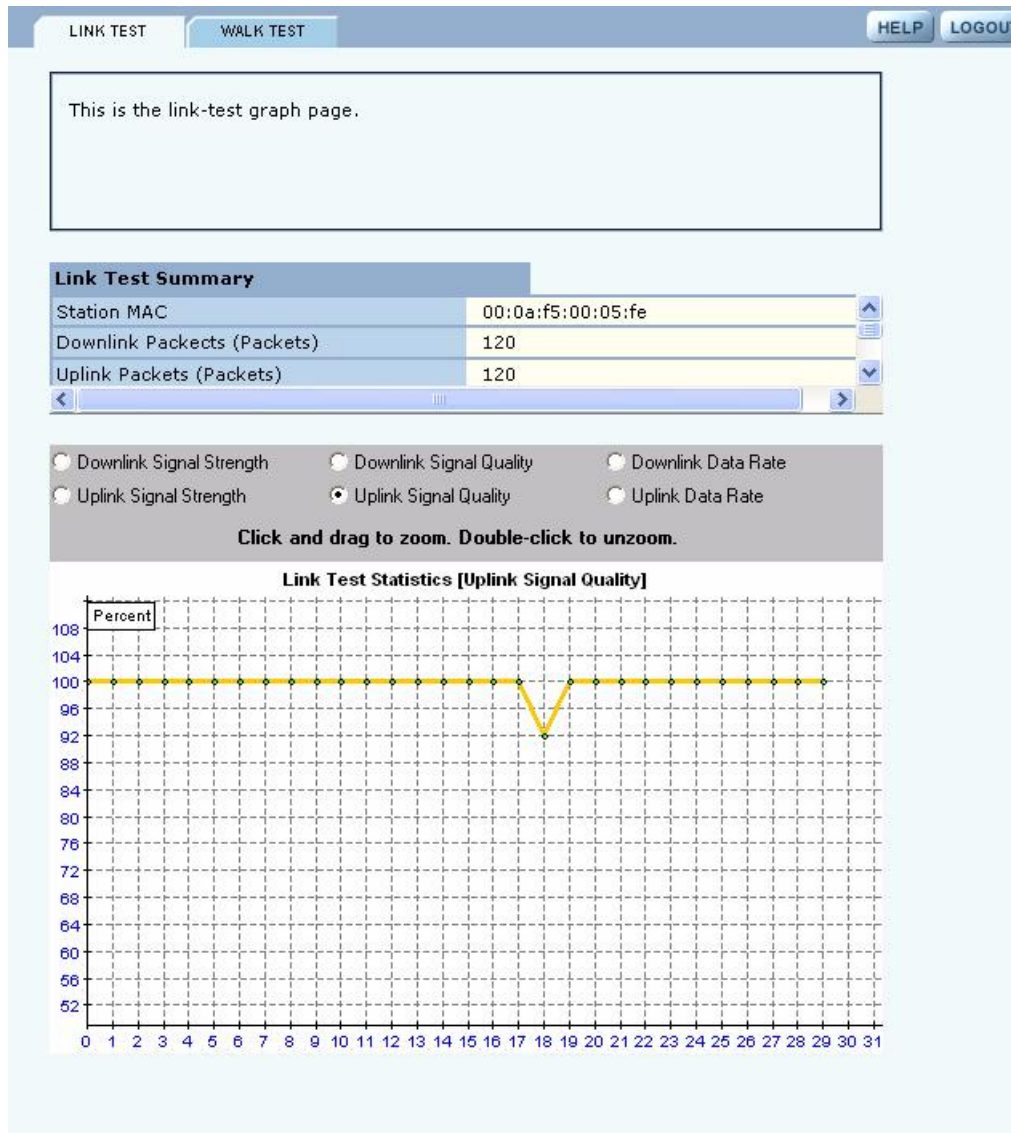
To graph the results of a link test, select the test on the Link Test tab, and click **Graph**. The Graph panel (Figure 68) opens.

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



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

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 Airgo 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

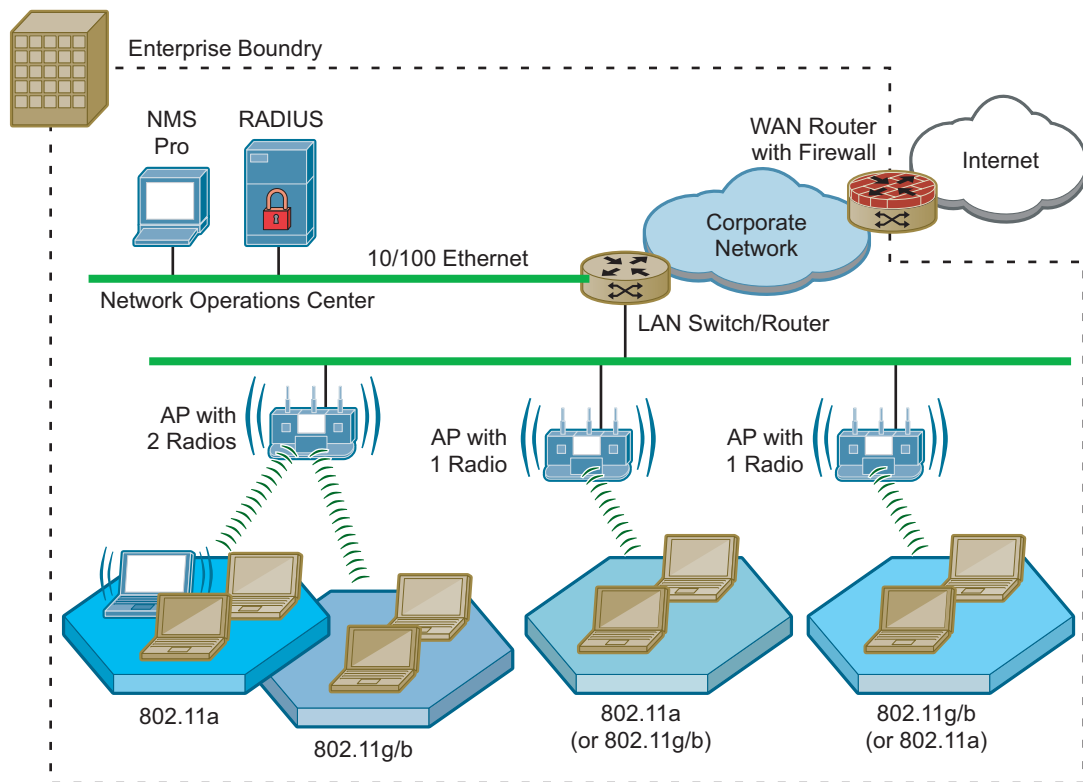
The Airgo Access Point provides advanced features to configure wireless networking services and extend services to network users. From the Networking Services menu, assign interfaces, define quality of service, configure VLANs, and define packet filters. Statistics are also available to monitor network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



A0008C

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

BRIDGE & STP | BRIDGE STATS | ARP TABLE | HELP | LOGOUT

Networking Services | Bridge Configuration | Bridge & STP »

Bridge configuration is automatic and requires no user configuration. Bridge table shows the bridges 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 corresponding 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

ENABLE STP | DISABLE STP

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 101).

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)

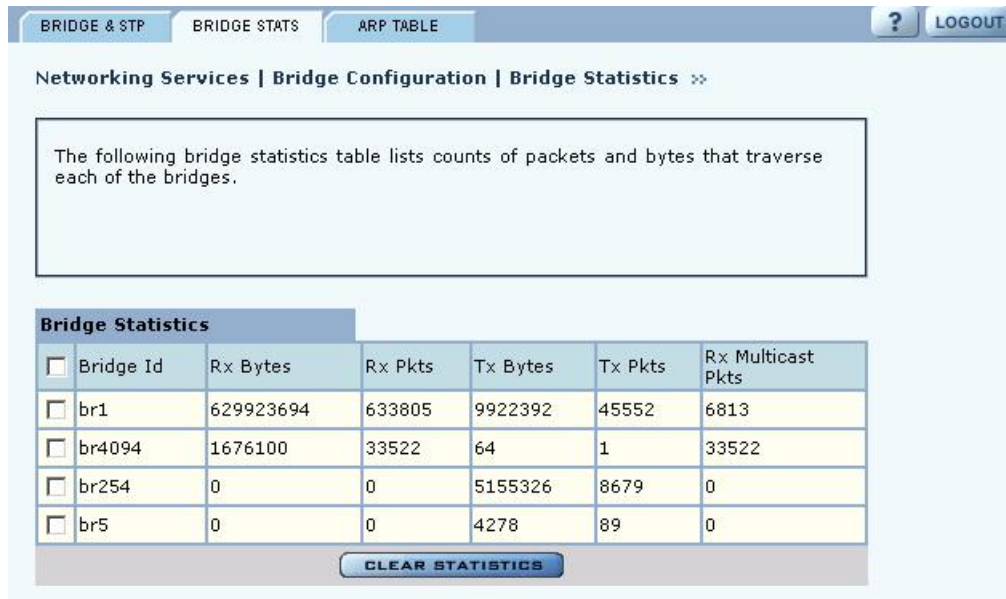
The Summary tab also provides an option for enabling or disabling Spanning Tree Protocol (STP). STP is a protocol that prevents bridging loops from forming due to incorrectly configured networks. STP provides protection against looping, but it does increase network overhead. Before STP allows traffic 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.

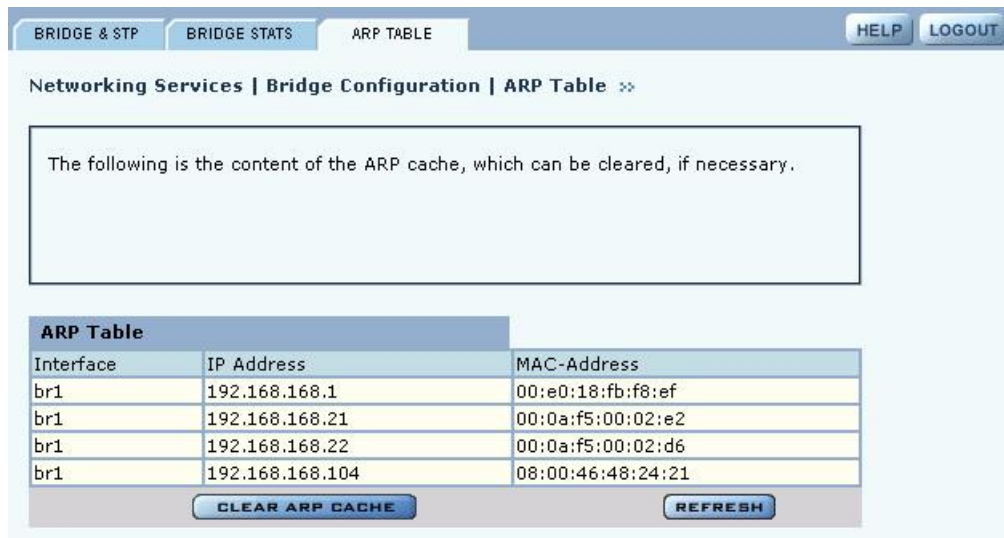
Figure 72: Bridge Configuration - Bridge Stats



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.

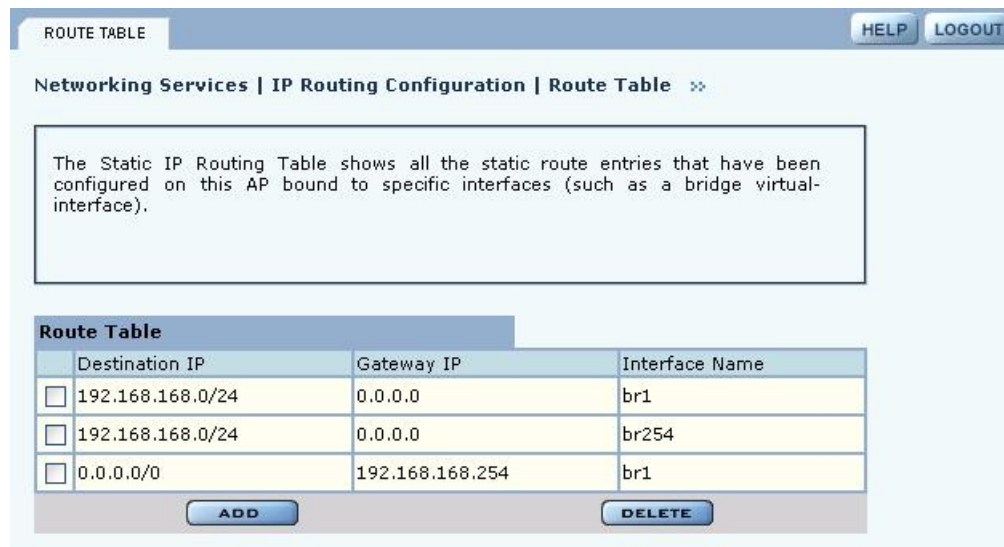
Figure 73: Bridge Configuration - ARP Table



Configuring IP Routes

IP routing expands the addressing capability of the Airgo AP and allows you to manage the AP from outside its local subnet. Use the IP Routing panel (Figure 74) 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



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**.

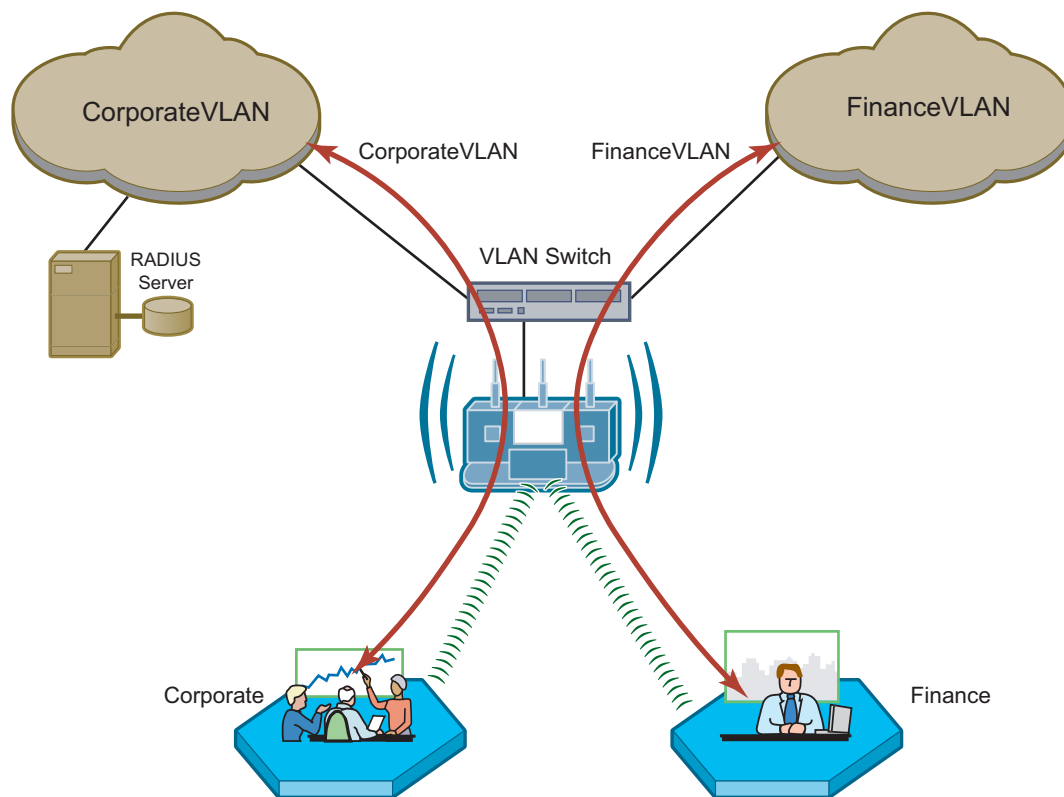
Field	Description
Destination IP	Enter the IP address of the subnet to which packets can be forwarded, along with the subnet prefix for the address.

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 <code>br</code> prefix, as described in “Configuring Bridging Services” on page 100.

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 Airgo 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



A0044B

The Airgo 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 79).

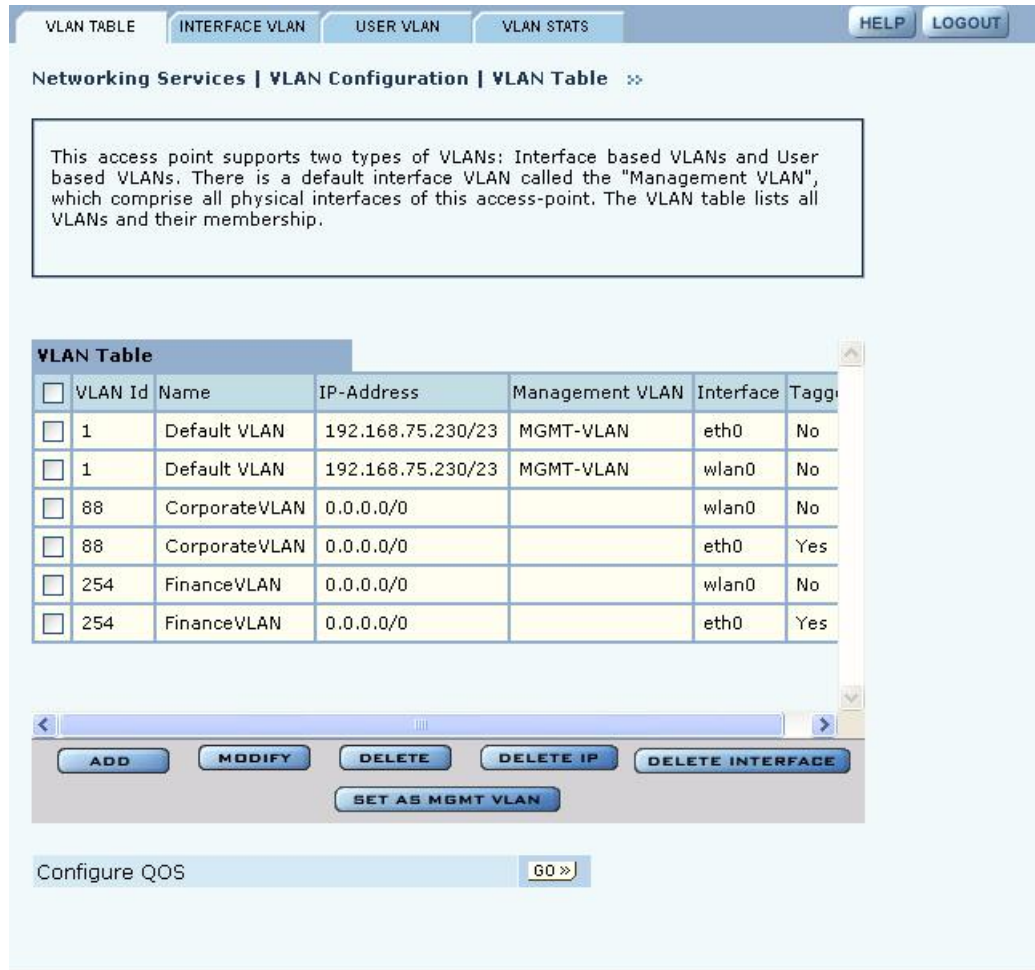
The VLAN Configuration panel contains the following tabs:

- 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



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 <code>br</code> 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 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

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 156
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.

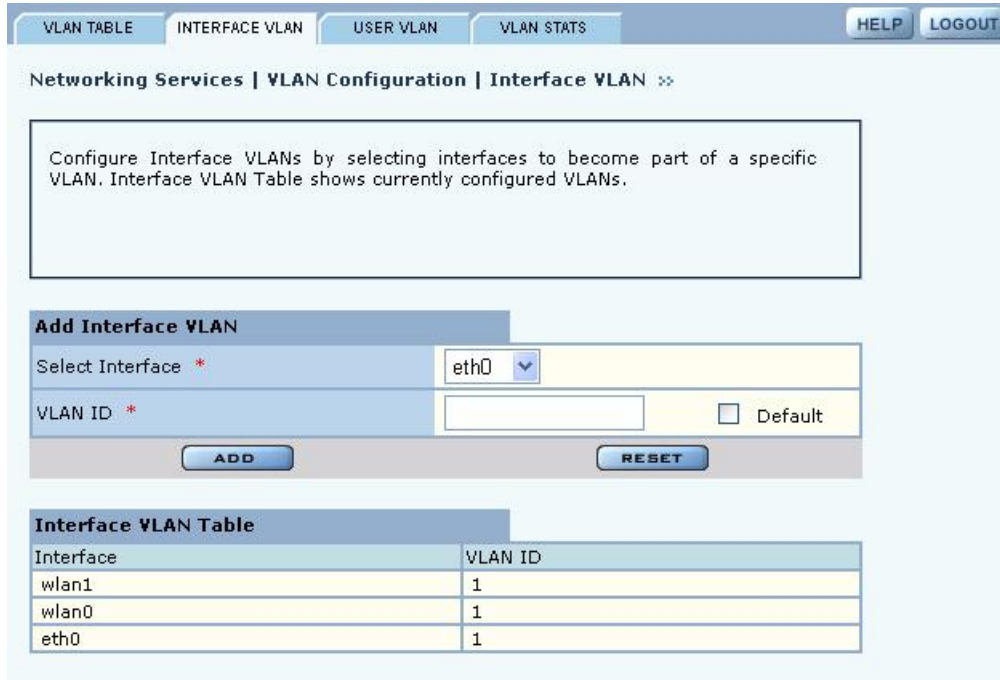
Click **Apply** to create the new VLAN and return to the VLAN table.

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



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 78 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.

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

Networking Services | VLAN Configuration | VLAN Statistics »

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

<input type="checkbox"/>	VLAN ID	Rx Bytes	Rx Pkts	Tx Bytes	Tx Pkts	Rx Multicast Packets
<input type="checkbox"/>	1	358612	3209	1366855	7507	37
<input type="checkbox"/>	88	761702	10322	963435	10325	606
<input type="checkbox"/>	254	683463	4136	1206166	4637	76

CLEAR STATISTICS **REFRESH**

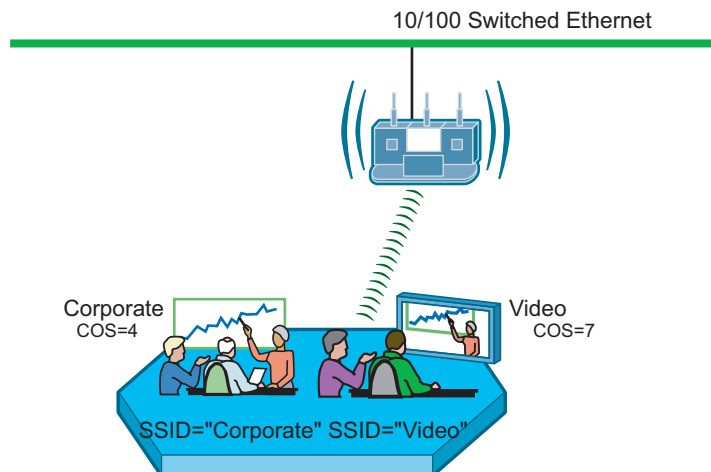
Configuring Quality of Service

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.

Airgo 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



A0043B

The Airgo 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 78).

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 115) 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

INGRESS QoS EGRESS COS QoS STATS [HELP](#) [LOGOUT](#)

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

[APPLY](#) [RESET](#)

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

[ADD](#)

Interface to COS Mapping Table

Ingress Interface Name	COS Value
wlan1	0
wlan0	0
eth0	0

[ADD](#)

[Configure VLAN](#) [GO >>](#)

Perform the following functions on this tab:

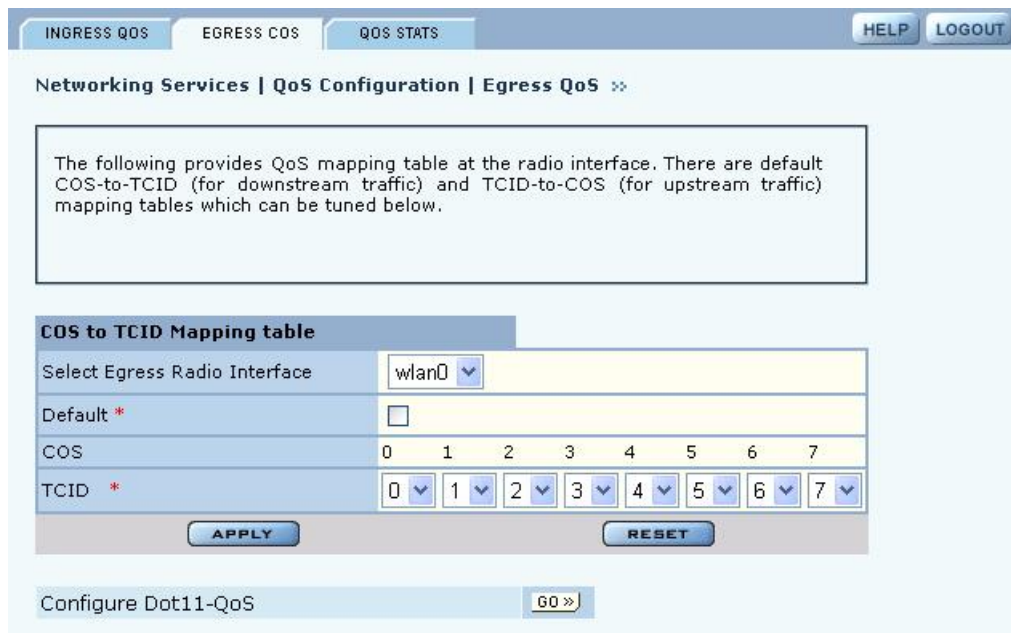
Function	Steps
Define TCID to COS mapping	<ol style="list-style-type: none"> 1 Select the radio interface for the mapping. 2 Select a COS value for each TCID value, or select Default to accept the default mapping. 3 Click Apply.
Define VLAN-to-COS mapping	<ol style="list-style-type: none"> 1 Click Add. 2 Select the AP interface. 3 Select the VLAN ID. (See “Configuring VLANs” on page 105 for information on VLAN IDs.) 4 Select a COS value or select Default to use the default mapping. 5 Click Apply.
Interface-to-COS	<ol style="list-style-type: none"> 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



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

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 interpreted as an array of eight numbers, one for each COS value of 0 through 7.

Interface	In packet Count Index to COS	Out packet Count Index to COS
<input type="checkbox"/> wlan1	1408,0,0,0,0,0,0,0	3650,0,0,0,0,0,0,2760
<input type="checkbox"/> wlan0	73,0,0,0,0,0,0,0	2542,0,0,0,0,0,5,2996
<input type="checkbox"/> 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.

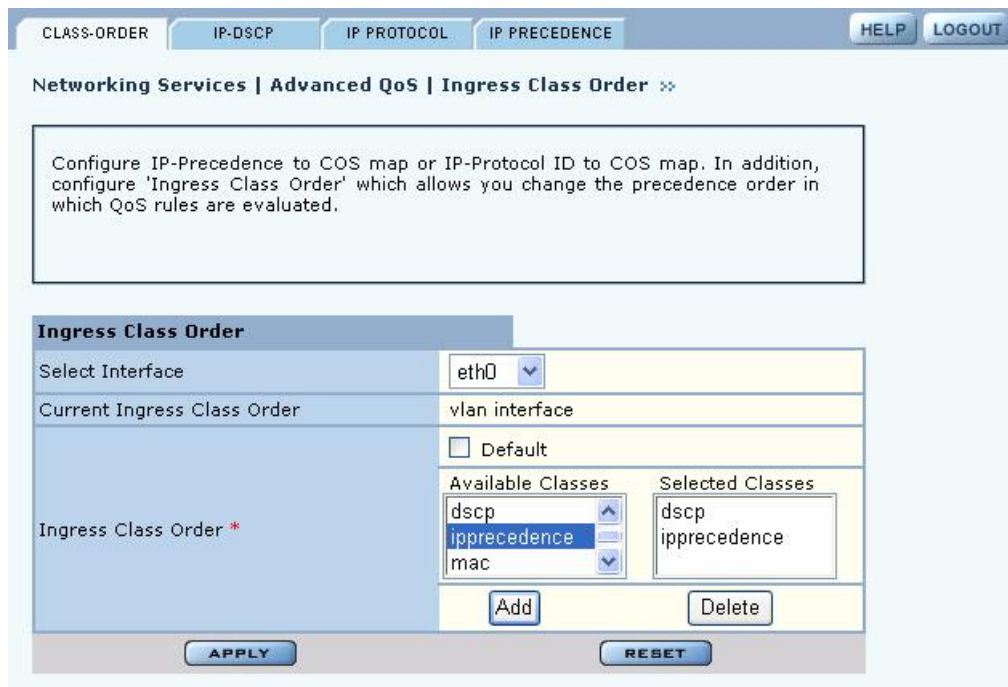
Class-Order

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



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

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

APPLY **RESET**

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:

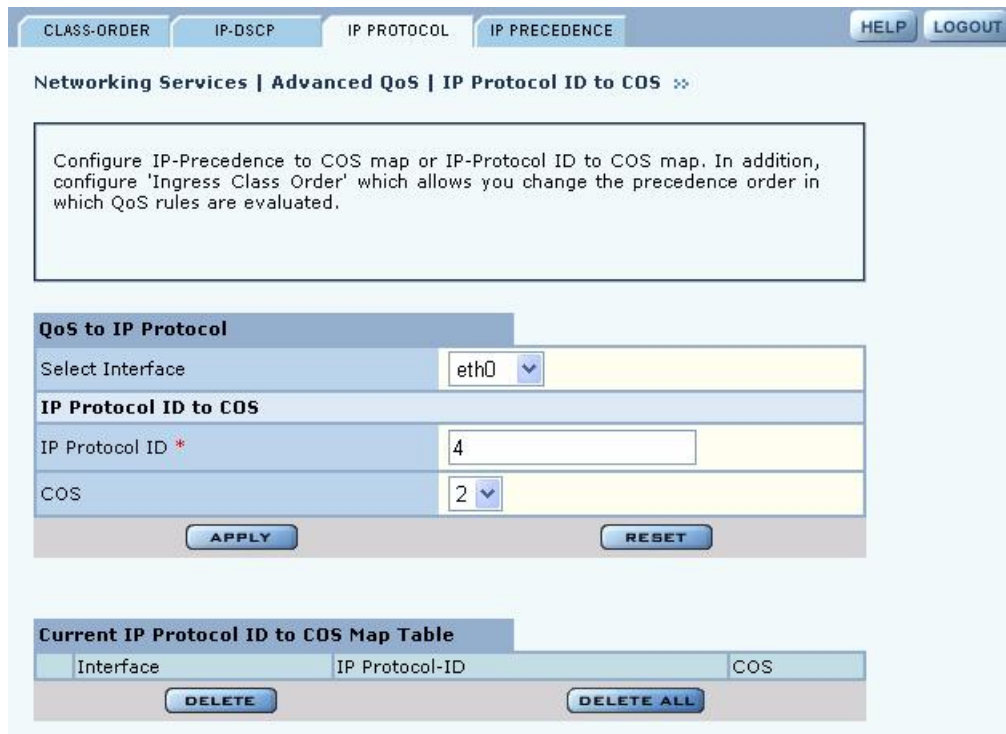
Field	Description
Select Radio Interface	Select the AP interface.
Default	Select to use the default mapping.
DSCP String	If Default is not chosen, enter up to eight DSCP values that you want to map to a specific COS value.
COS	Select the COS value.

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



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

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



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 checked="" type="radio"/> Input <input type="radio"/> Output
Accept/Discard	<input checked="" type="radio"/> Accept <input type="radio"/> Discard
Select Match	<input type="radio"/> Matched <input checked="" type="radio"/> Unmatched <input type="text" value="Ether Type"/>
<input type="button" value="APPLY"/> <input type="button" value="CANCEL"/>	

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

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

<input type="checkbox"/>	Interface Name	Ingress/Egress	Filter	Number of Hits	Action
<input type="checkbox"/>	eth0	input	None	14799	accept
<input type="checkbox"/>	eth0	output	None	7129	accept
<input type="checkbox"/>	wlan0	input	None	216	accept
<input type="checkbox"/>	wlan0	output	None	5577	accept
<input type="checkbox"/>	wlan1	input	None	1612	accept
<input type="checkbox"/>	wlan1	output	None	6410	accept

Configuring Interfaces

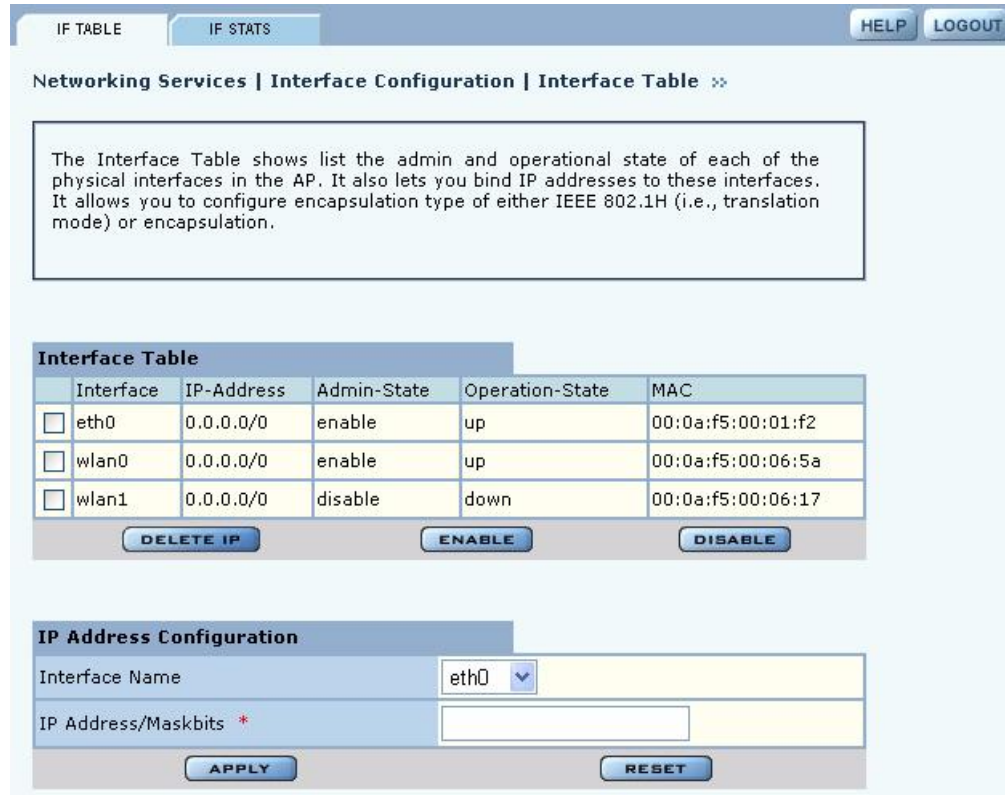
Use the Interface Configuration panel, accessible from the Networking Services menu, to configure the physical AP interfaces (wlan0, wlan1, eth0). The panel contains the following tabs:

- 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



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.

<input type="checkbox"/>	Interface	Rx Bytes	Rx Pkts	Tx Bytes	Tx Pkts	Rx Multicast Pkts	Error Pkts	Drop Pkts
<input type="checkbox"/>	eth0	1831180	14919	2448810	7209	0	0	0
<input type="checkbox"/>	wlan0	36306	294	227334	4164	0	0	60
<input type="checkbox"/>	wlan1	208295	2118	300827	5434	0	0	471

CLEAR STATISTICS **REFRESH**

Configuring SNMP

Simple Network Management Protocol (SNMP) is an industry standard protocol used to manage interactions with the Airgo 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

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)

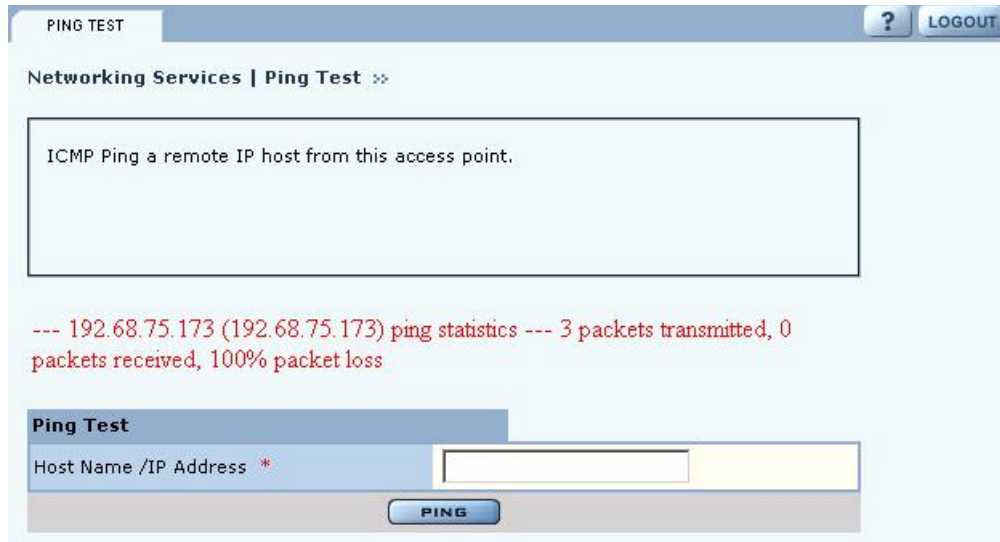
Click **Apply** to save your changes, or **Reset** to return to previously saved values.

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



The screenshot displays a web interface for a Ping Test. At the top, there is a navigation bar with "PING TEST" and a "LOGOUT" button. Below this, the page title is "Networking Services | Ping Test". A large text box contains the instruction: "ICMP Ping a remote IP host from this access point." Below the text box, the test results are displayed in red text: "--- 192.68.75.173 (192.68.75.173) ping statistics --- 3 packets transmitted, 0 packets received, 100% packet loss". At the bottom, there is a "Ping Test" section with a label "Host Name /IP Address *" and an input field. A "PING" button is located below the input field.

6 Configuring a Wireless Backhaul

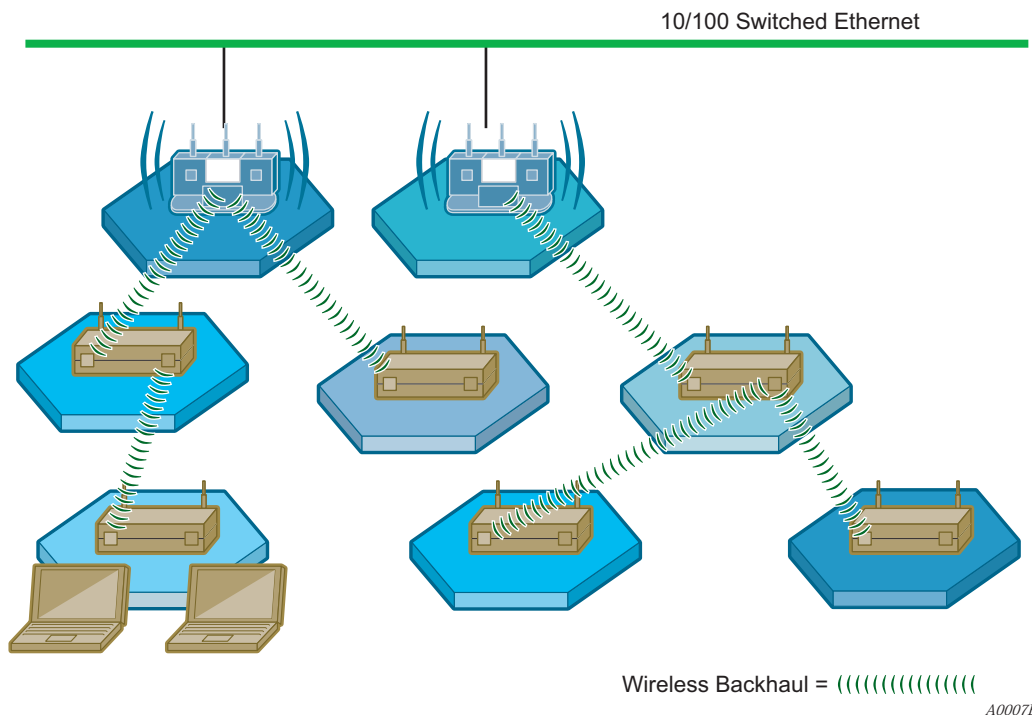
This chapter explains how to set up a wireless distribution system to cover a large area with limited wired network connectivity. It covers the following topics:

- [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 Airgo 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. Airgo 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 165). 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

The screenshot displays the 'LINK CRITERIA' configuration page. At the top, there are tabs for 'LINK CRITERIA', 'CANDIDATE APs', 'TRUNK TABLE', and 'TRUNK STATS', along with 'HELP' and 'LOGOUT' buttons. The main content area is titled 'Uplink Criteria Configuration' and contains a section 'Uplink Criteria (Based on SSID, IP Subnet, Path Selection or BSSIDs)'. This section has several rows of configuration options:

- SSID Criteria:** 'New SSID' is set to 'DeerCreekCo' (selected with a radio button), and 'Detected SSID' is 'DeerCreekCo' (shown in a dropdown menu).
- IP Subnet Criteria:** 'IP-Address/Maskbits' is an empty text field.
- Path Selection Criteria:** 'Lowest Weighted Cost' is selected (radio button), with other options being 'Smallest Hop Count' and 'Highest Node Priority'.
- Uplink BSSID Criteria:** 'Accept from BSSIDs' is selected (radio button), with the other option being 'Discard from BSSIDs'.

Below these options are 'APPLY' and 'RESET' buttons. The lower section is titled 'BSSIDs For Uplink Criteria' and includes an 'Available BSSID list' (empty), an 'Add BSSID' section with a dropdown menu (showing '--select--'), and a 'Selected BSSID List' (empty). 'Add' and 'Delete' buttons are present. At the bottom of this section are 'APPLY', 'RETRUNK NOW', and 'RESET' buttons.

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: <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• 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.

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.

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:

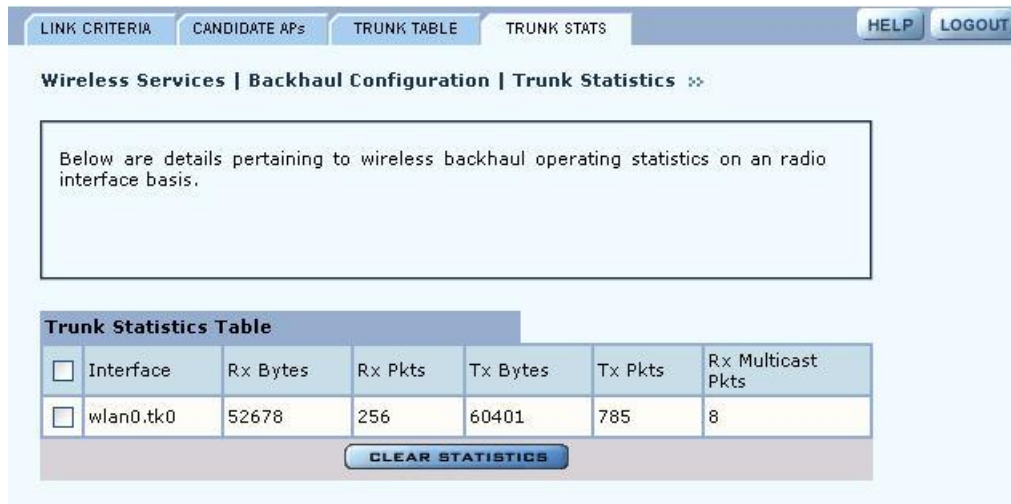
Feature	Description
Interface Name	Radio interface of the BP radio (uplink) or AP radio to which downlink trunks are connected. Applies to uplink and downlink trunks.
Band (2.4 GHz or 5 GHz, or both)	Operating band of the uplink or downlink trunks. Applies to uplink and downlink trunks. For the uplink 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



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 Airgo Access Point and explains how to set the security configuration. The chapter includes the following topics:

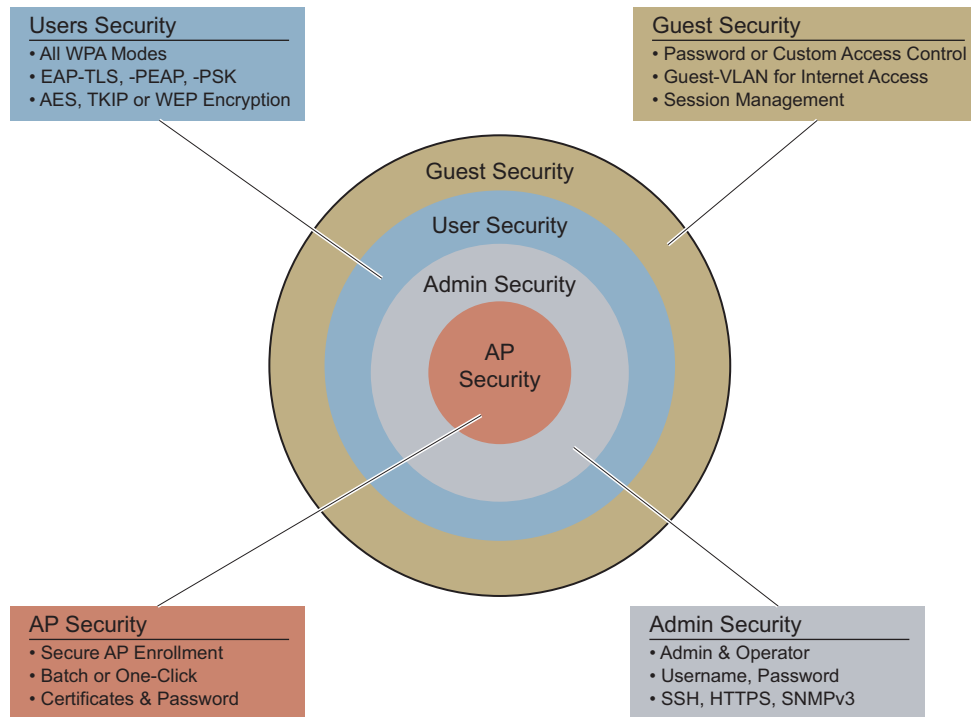
- [Introduction](#)
- [Configuring Wireless Security](#)
- [Configuring Authentication Zones](#)
- [Configuring Administrator Security](#)
- [Viewing Security Statistics](#)
- [Configuring Advanced Parameters](#)

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

Introduction

Airgo 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 Airgo Security

A0047

AP Security

Airgo 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.”
- **NMS Pro**—The NMS Pro network management system, offered as a separate product, operates as a complete enrollment solution for the enterprise. In addition to supporting manual AP enrollment, NMS Pro includes automatic AP pre-enrollment by way of a bar code reader interface. For information on using NMS Pro, see the *NMS Pro 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 Airgo AP can meet all the user authentication needs for the full range of wireless networks. (See Chapter 2, “Planning Your Installation.”) Airgo 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 Airgo AP provide EAP-TLS for user authentication. Airgo also supports integration with RADIUS servers that support EAP-TLS or EAP-PEAP.

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

Table 11: Authentication Options

Type	Description
EAP-TLS	Certificate-based authentication, used by the Airgo 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 Airgo Wireless LAN Client Adapter 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