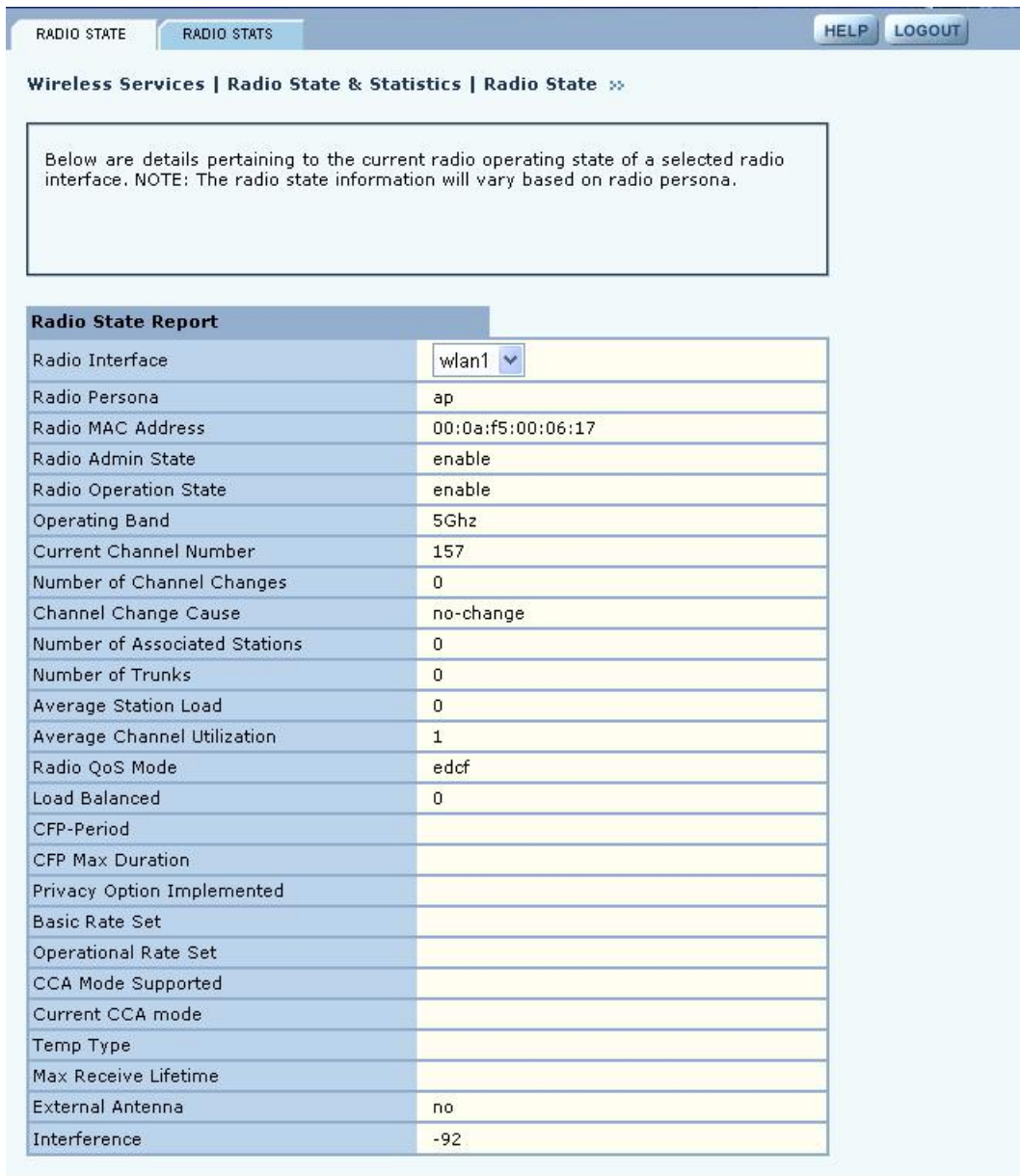


Figure 49: Radio State Tab



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

Field	Description
Radio Interface	AP radio (wlan0 or wlan1)
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 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 load balanced stations (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 amount of time allowed to reassemble a fragmented frame
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. It is advisable to wait 10 seconds or more to get new snapshot of the same statistics.



NOTE: All statistics are computed since the last radio reset or since the Clear Statistics button was last clicked.

Figure 50: Radio Statistics Tab



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

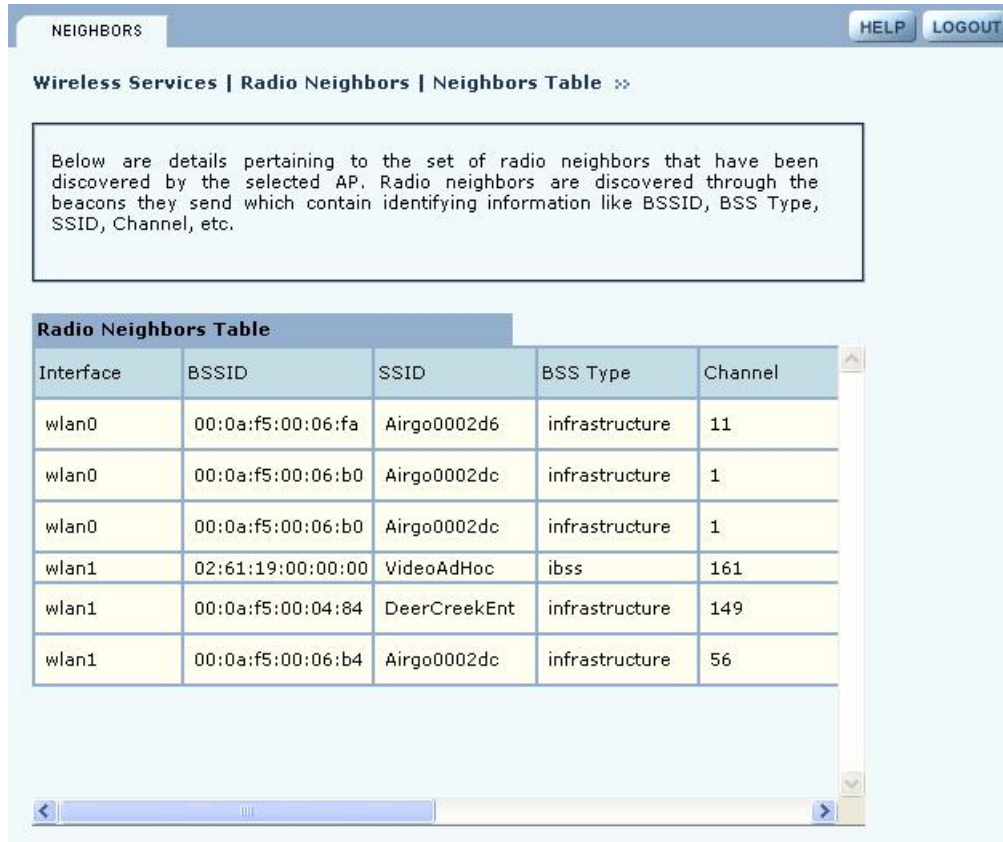
Field	Description
Radio Interface	Access point radio (wlan0 or wlan1)
Transmitted Fragments	Number of transmitted fragments (MAC Protocol Data Units) that have been acknowledged since last power-up or last Clear Statistics request
Transmitted Multicast Frames	Number of transmitted multicast frames
Transmitted Frame Count	Count for successfully transmitted MSDUs
Failed Count	Count of MSDU not transmitted successfully due to the number of transmit attempts exceeding either the dot11ShortRetryLimit or dot11LongRetryLimit
Received Fragments	Count for successfully received MPDUs of type Data or Management
Received Multicast Frames	Count when an MSDU is received with the multicast bit set in the destination MAC address

Field (continued)	Description
Received Frame Count	Count of successfully received frames (MSDUs)
FCS Error Count	Count of FCS errors detected when receiving a MPDU
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
Acknowledgement Failure Count	Count of expected acks not received
RTS Success Count	Count of successful CTS received in response to an RTS
RTS Failure Count	Count of RTS for which a CTS response is not received
WEP Undecryptable Count	Only if encryption is WEP, 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)
Dropped Count	Number of dropped frames
Transmitting 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



The summary table lists the following information:

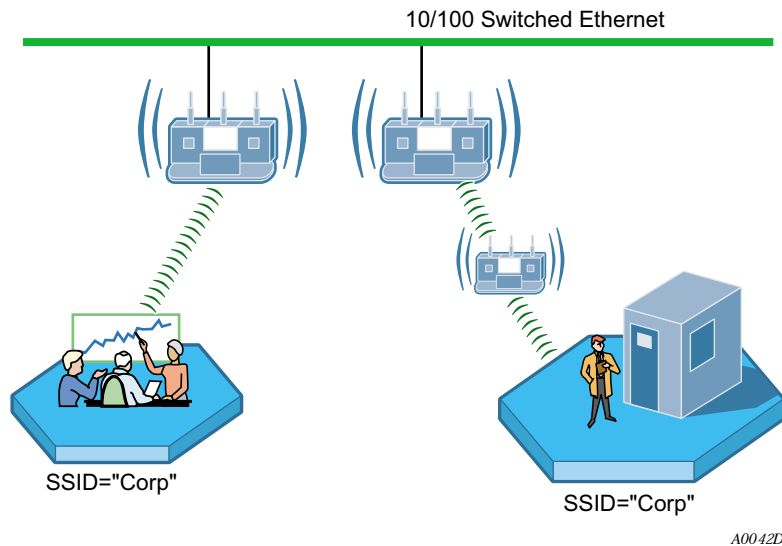
Field	Description
Interface	The AP radio (wlan0 or wlan1)
BSSID	MAC address of the neighboring AP radio, which determines the BSS
SSID	Name of the network (ESS) in which the AP is operating
BSS Type	Infrastructure or ad-hoc network arrangement
Channel	Current channel of operation for the neighboring BSS
AP Beacon Name	Name of the neighboring AP in the beacon frame
Compatibility Status	Indication of whether the neighbor is an AP with which the IAPP protocol can be established
Strength	Strength of radio neighbor signal, in percentage
Load Percentage	Load on the AP, in percentage
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



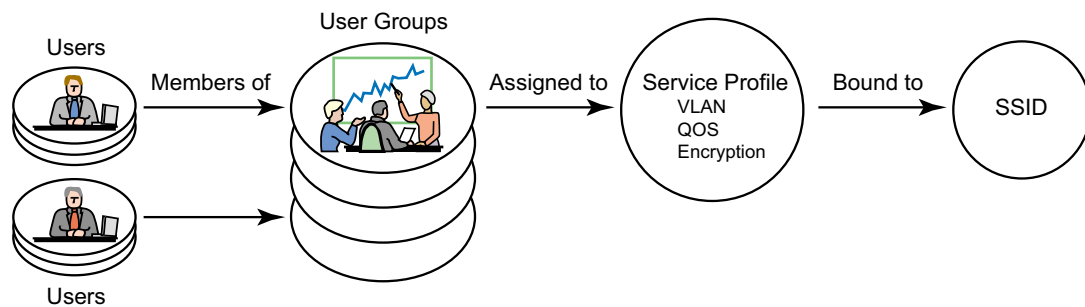
Each Airgo AP is shipped with a default SSID, which must be replaced during the bootstrap process (see “Using AP Quick Start to Initialize the Access Point” on page 34) or from the SSID Configuration panel, as explained in this section. Multiple SSIDs are also supported. “Multiple SSIDs” on page 90 explains 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, 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 the 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 133 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

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

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

Broadcast SSID in Beacon (Applies To Single SSID only)

Number of SSIDs	1
Currently Broadcasting SSID in Beacon	yes
Broadcast SSID in Beacon	<input type="radio"/> no <input checked="" type="radio"/> yes

The table lists the following information about each SSID:

Field	Description
SSID Name	Name (maximum 32 alphanumeric characters). This name is used only by the radio in AP mode and is broadcast in its beacon. For a radio in backhaul point mode, the SSID name is entered in the Backhaul Configuration, Link Criteria tab (see Chapter 6).
Max stations	The maximum number of stations that can be associated to this SSID on this AP. The range is 1-256 for each AP radio. 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 Select the checkbox for 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 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 90), then it is possible to add new SSIDs from the SSID Table tab, in addition to modifying or deleting an existing SSID.

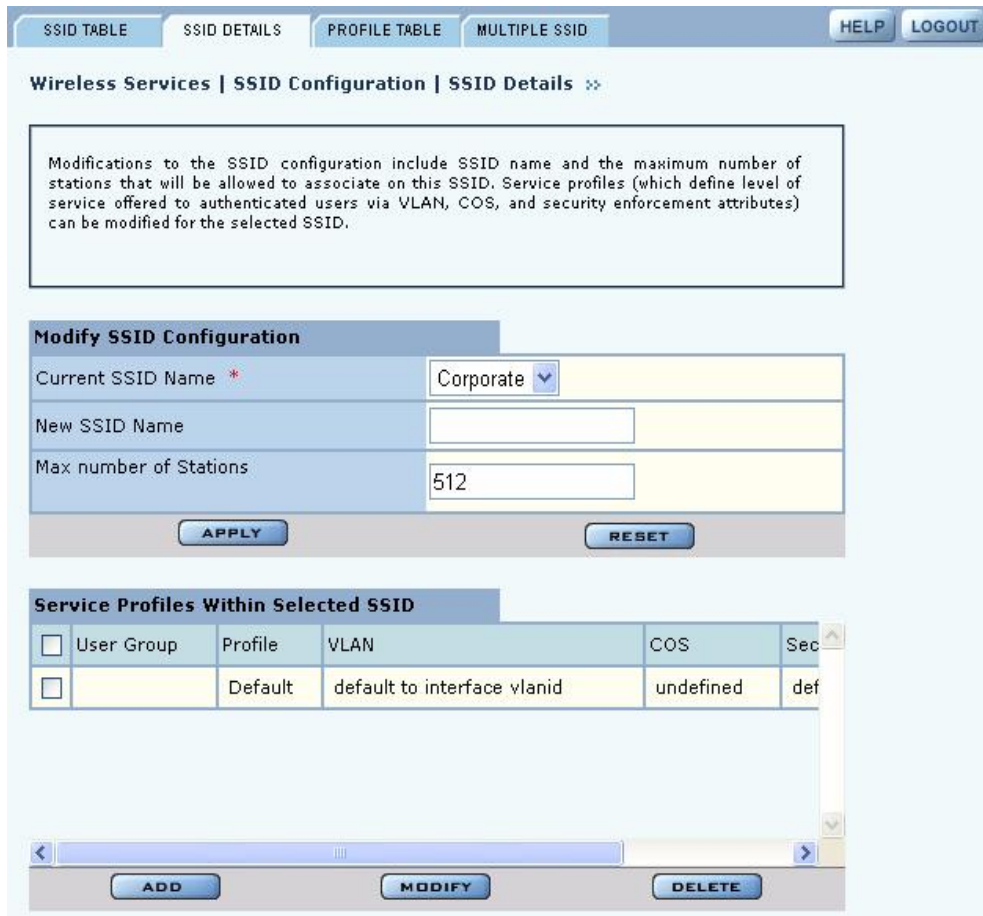
Perform the following functions on the SSID Table tab:

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 <i>Configuring a Wireless Backhaul</i>). • Max Number of Stations — Enter a maximum number of client stations, if desired. The range of values is 1-256 for each AP radio. 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 85. 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	The user group that is 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. If all the service profiles associated with an SSID are deleted, then the SSID is automatically associated to the Default service profile. If the group must be changed then the SSID to service profile binding must be deleted and re-added.
Profile	Service profile name.
VLAN	VLAN assigned to the service profile.

Feature (continued)	Description
COS	Class of service values assigned to the service profile.
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 89. 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 89. 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.

Figure 56: SSID Configuration - Bind Service Profile to SSID

The screenshot shows a configuration window titled "Bind Service Profile to SSID". It contains the following elements:

- SSID Name ***: Corporate
- User Group Name**: A dropdown menu and a checkbox labeled "New Group".
- Profile**: Finance (with a dropdown arrow) and a link "Add New Profile".
- Preview Profile Attributes**:
 - VLAN ID: 254
 - COS Value: 6
 - Security Enforcement: default-enforcement
- Buttons: 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.

i **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

Wireless Services | SSID Configuration | Profile Table »

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

<input type="checkbox"/>	Profile Name	Security Enforcement	VLAN ID
<input type="checkbox"/>	Default	default-enforcement	default to interface vlanid
<input type="checkbox"/>	Employee	aes-only	88
<input type="checkbox"/>	Guest	default-enforcement	254
<input type="checkbox"/>	Finance	default-enforcement	254

ADD MODIFY DELETE

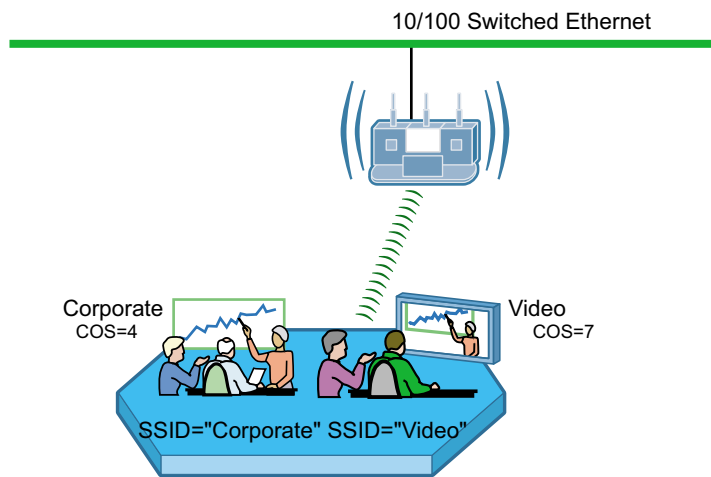
Perform the following functions from this tab:

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 117. 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

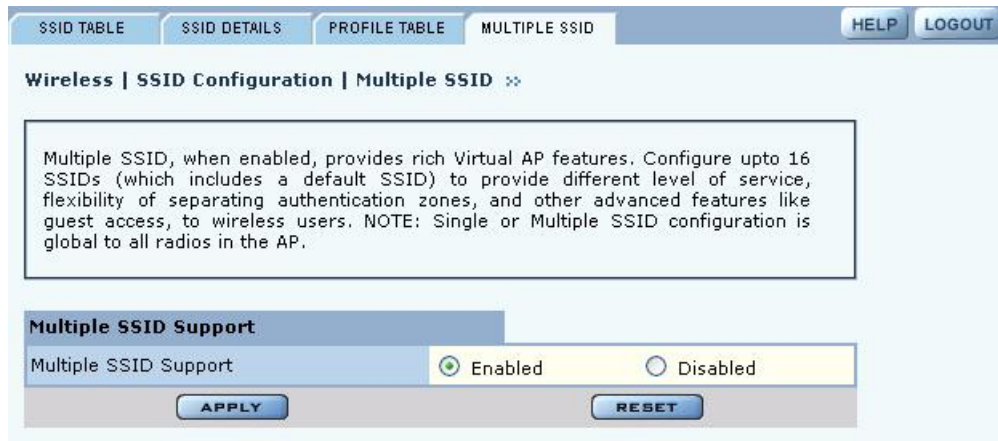


A0043B

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 85).

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 Wireless 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 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, 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 to the second AP radio)

Field (continued)	Description
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

The screenshot shows a web interface for managing wireless services. At the top, there are tabs for 'STATIONS', 'LINK STAT', and 'SECURITY STAT', along with 'HELP' and 'LOGOUT' buttons. Below the tabs, the breadcrumb path is 'Wireless Services | Station Management | Link Statistics'. A text box explains that the Station Link Statistics reports Signal Strength, Signal Quality, and IEEE 802.11 MAC level statistics. The main section is titled 'Station Link Statistics Table' and contains a table with a dropdown menu for 'Station MAC' set to '00:0a:f5:00:05:fe'. The table lists various statistics for this station, including Uplink Signal Strength (100), Uplink Signal Quality (100), Uplink Rate (18), Downlink Rate (11), Received Bytes (1096), Transmitted Bytes (0), Transmitted Fragments (4), Failed Transmitted Packets (0), Single Retry Packets (1), Multiple Retry Packets (0), and Acknowledgement Timeouts (1). At the bottom of the table are 'CLEAR STATISTICS' and 'REFRESH' buttons.

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

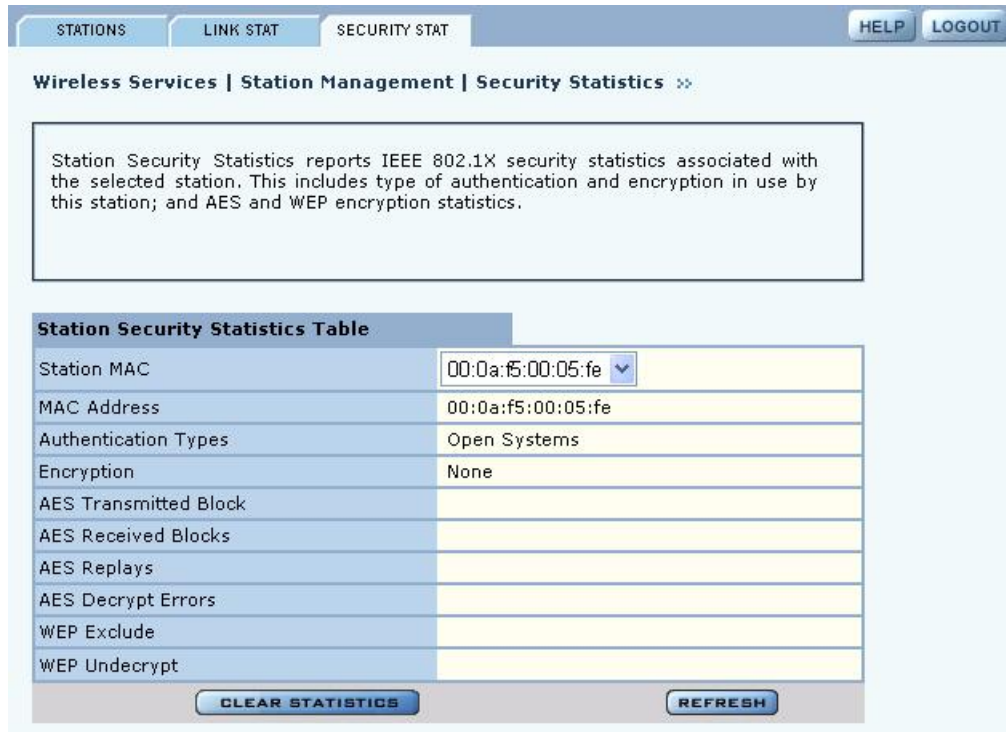
Select a station from the Station Associations table and click **Link Stats** to display the following information:

Field	Description
Station MAC address	The MAC address that identifies the station
Mode	802.11 mode used by the station (11a, 11b, or 11g)
Uplink Signal Strength	Average signal strength on uplink (station-to-AP direction) as a percentage
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 the station
Transmitted Fragments	Count of acknowledged MPDUs
Failed Transmitted Packets	Number of MSDUs that were not transmitted successfully because 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 times the AP timed out while waiting for an 802.11 ACK frame from the selected STA

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



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

Field	Description
Station MAC	The MAC address that identifies the client station
MAC Address	MAC address of the AP
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 frames received that are NOT encrypted (and thus are not decryptable)

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.

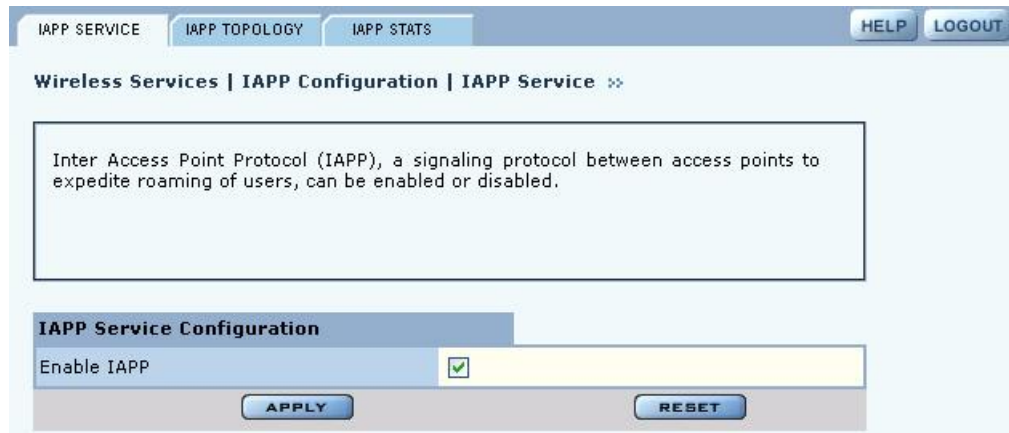
The panel contains the following tabs:

- 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 IAPP** 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

Wireless Services | IAPP Configuration | IAPP Topology

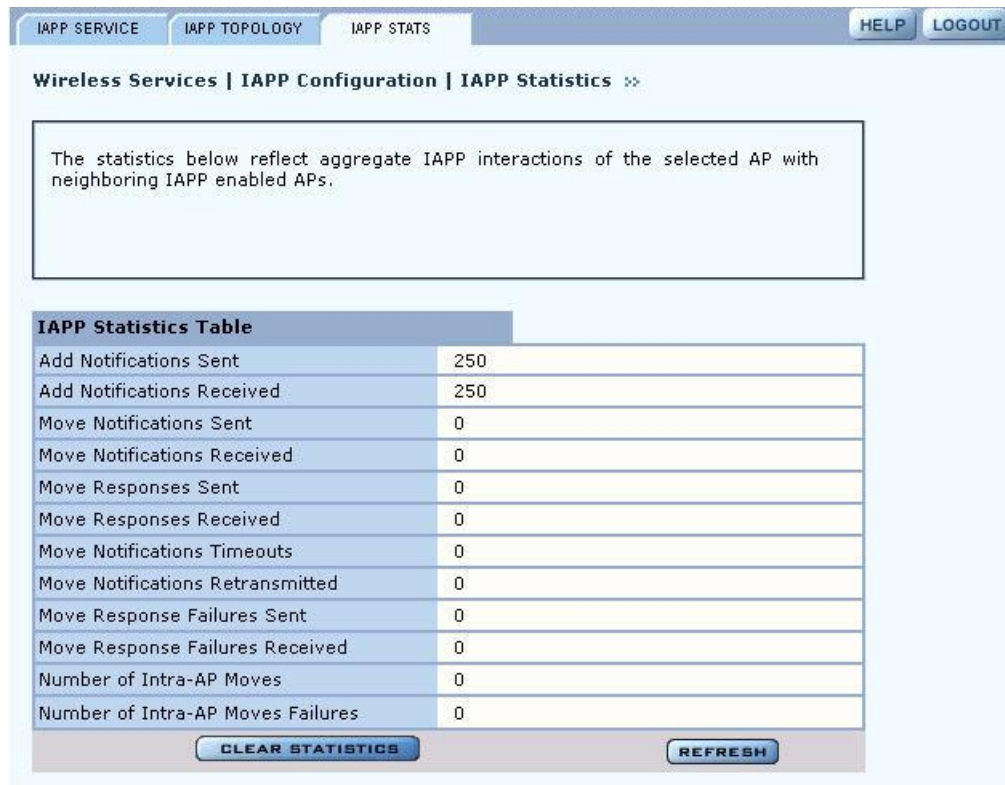
All discovered neighboring APs are listed below for the selected AP. Compatible APs are those with whom the IAPP protocol can be established.

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

IAPP Statistics

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

Figure 65: IAPP Configuration - IAPP Stats



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

Link Test Table					
	Interface	Station Mac	Packet Size	Duration	Avg Int
<input type="radio"/>	wlan0	00:0a:f5:00:05:fe	64	30	1

ADD DELETE STOP GRAPH

NOTE: The Link Test graphing feature requires the installation of Sun Java (not Microsoft Java) on your Microsoft Internet-Explorer web browser. For download instructions, go to www.java.com.

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

Field	Description
Interface	Access point radio
Station MAC	MAC address of the station included in the link test
Packet Size	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 67).

Figure 67: Radio Diagnostics - Link Test - Setup

- 2 Configure the following:

Field	Description
Interface	Select the AP radio.
Station MAC	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.

i **NOTE:** When the link test is first invoked, the Java Applet will post a standard Java security warning. Accept the warning to continue. A single link test graph can be displayed at a time.

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 five minutes (or equivalent number of packets, for example five 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 finished, until manually deleted.

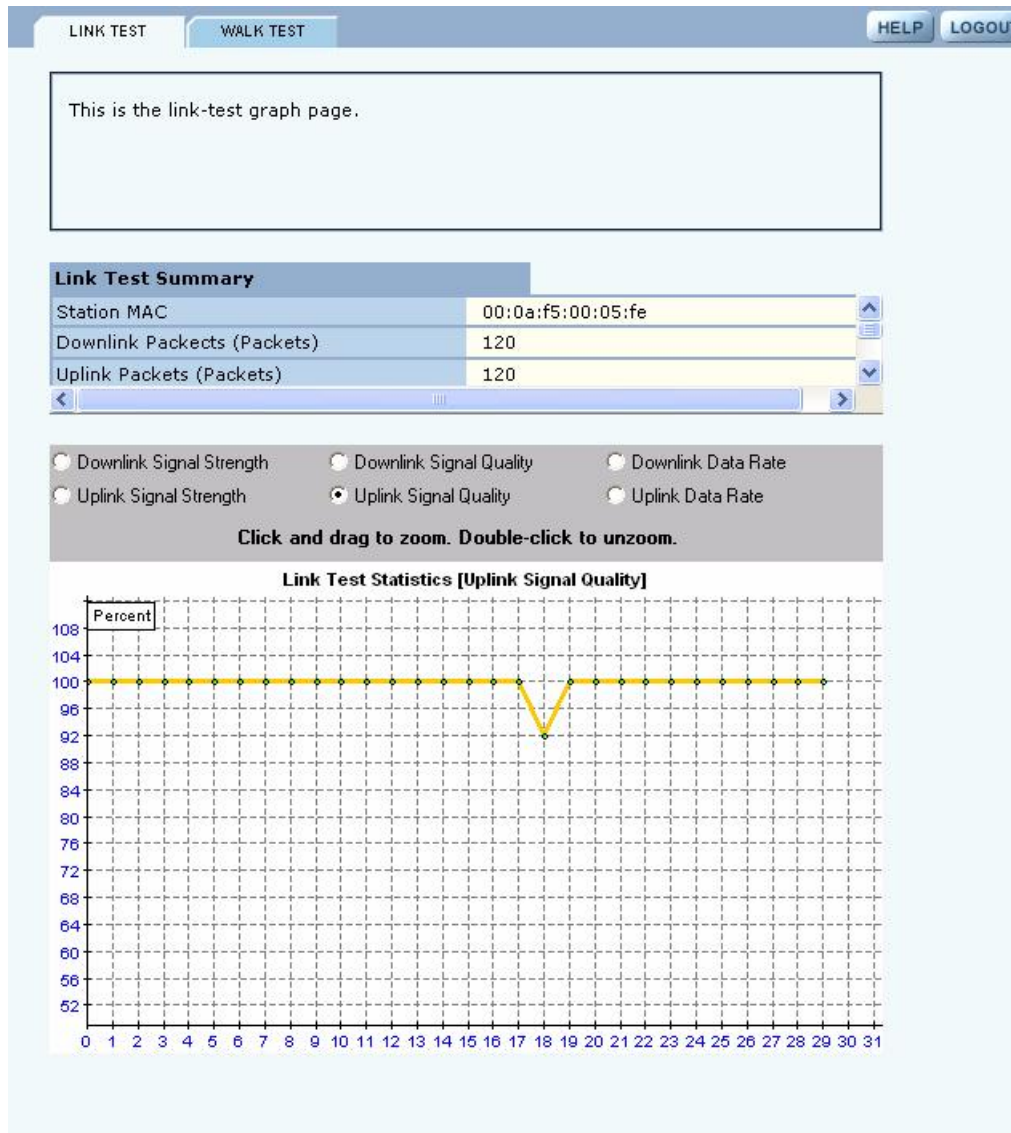
To graph the results of a link test, select the test on the Link Test tab, and click **Graph**. The Graph panel (Figure 68) opens. Only one graph can be displayed at a time.

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

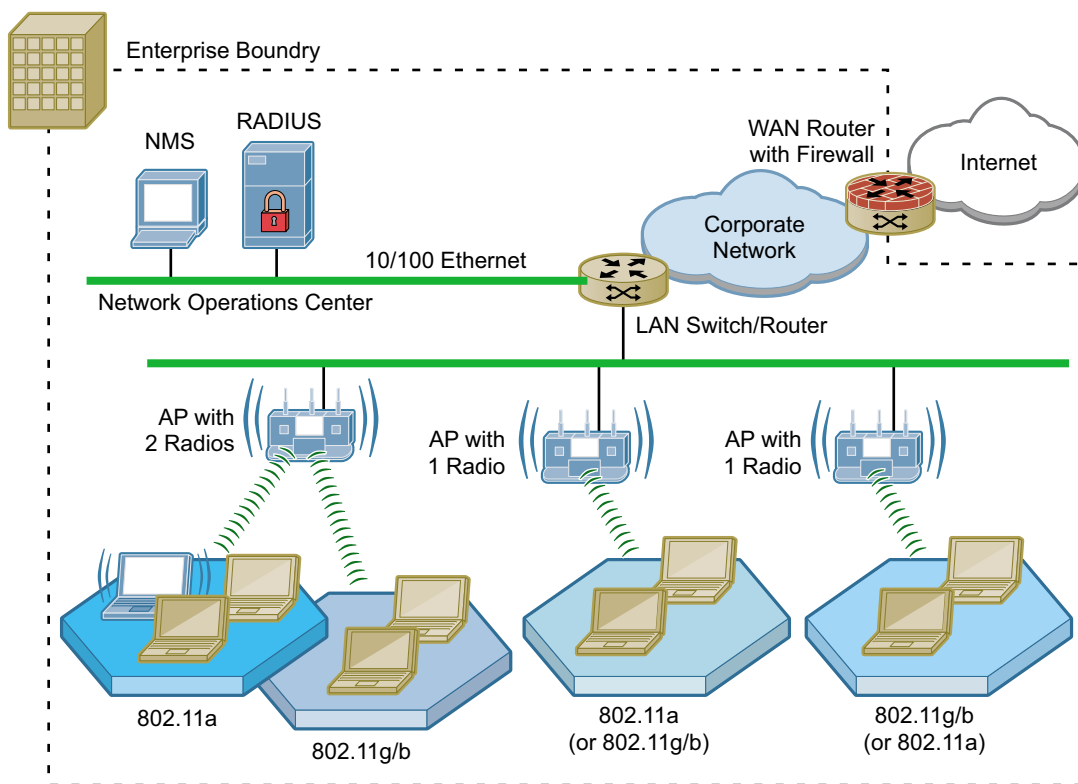
The Airgo Access Point provides advanced features to configure wireless networking services and extend services to network users. From the Networking Services menu, assign interfaces, define quality of service, configure VLANs, and define packet filters. Statistics are also available to monitor network 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 the wireless network. Each Airgo Access Point has virtual interfaces that correspond to specific communications functions, as listed in Table 11. 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 Networks Wireless Network Elements



A0008C

Table 11: 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

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. The following IDs are reserved:

- `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 the next section).

The Bridge Table 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

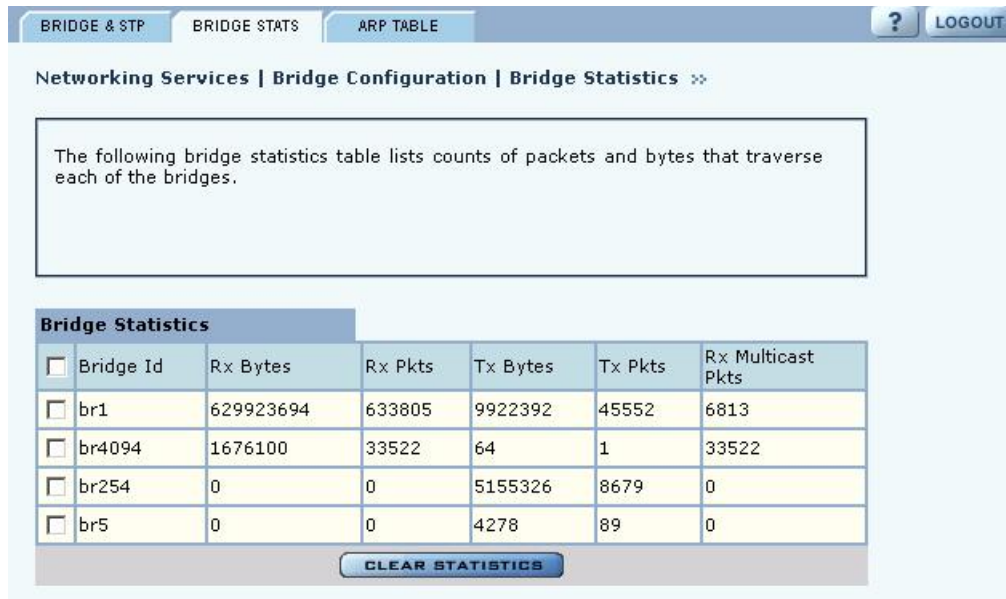
The Bridge & STP tab also provides an option for enabling or disabling spanning tree protocol (STP). STP is a protocol that prevents bridging loops from forming due to incorrectly configured networks. STP provides protection against looping, but it does increase network overhead. Before STP allows traffic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

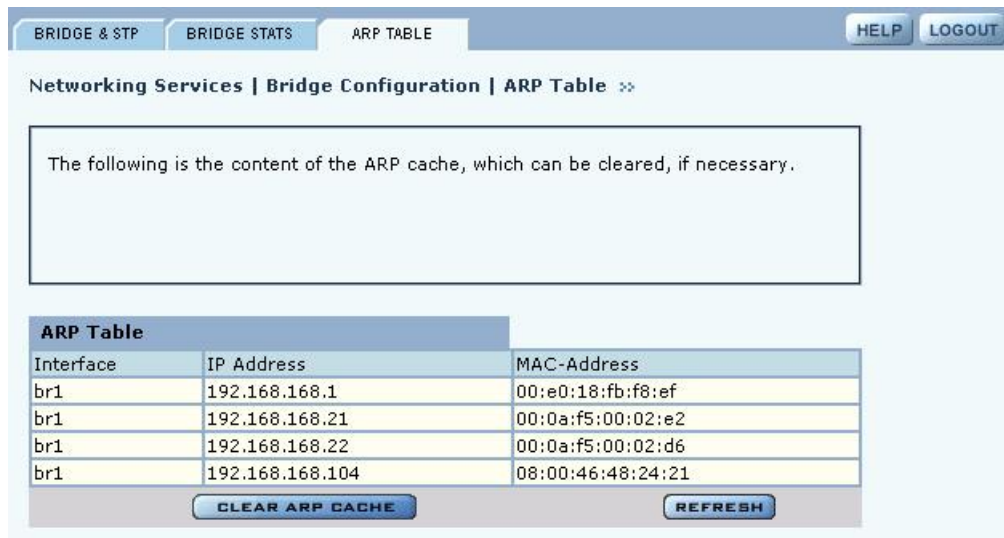
Figure 72: Bridge Configuration - Bridge Stats



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.

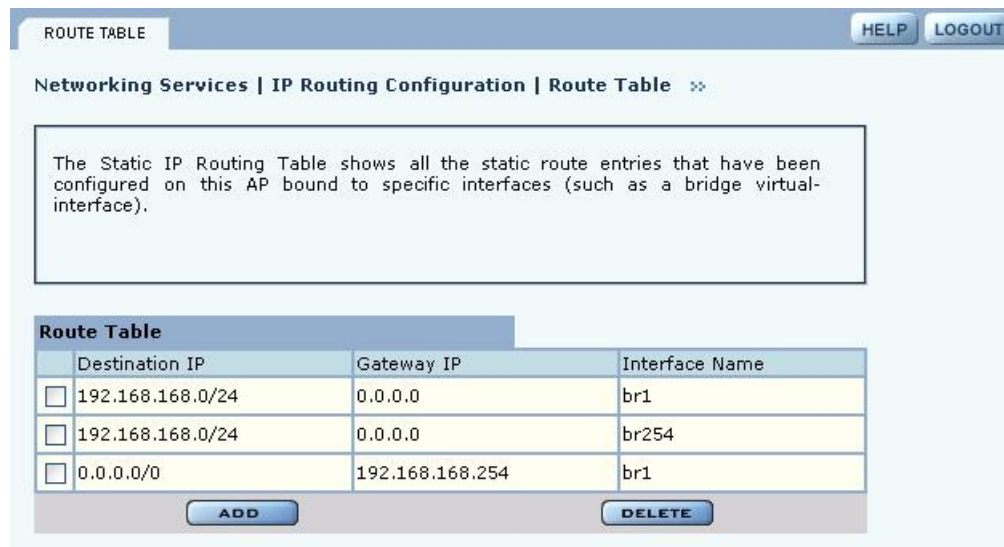
Figure 73: Bridge Configuration - ARP Table



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**.

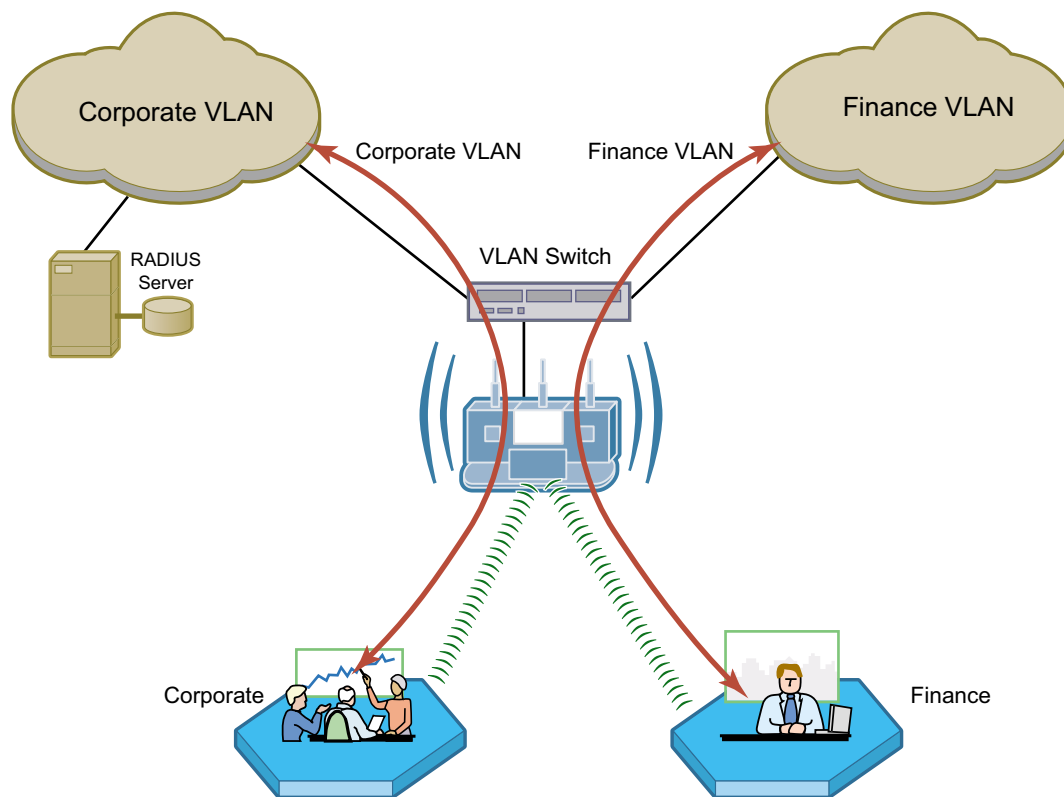
Field	Description
Destination IP	Enter the IP address of the subnet to which packets can be forwarded, along with the subnet prefix for the address.

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 106.

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 (“VLAN Table” on page 112). 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 84).

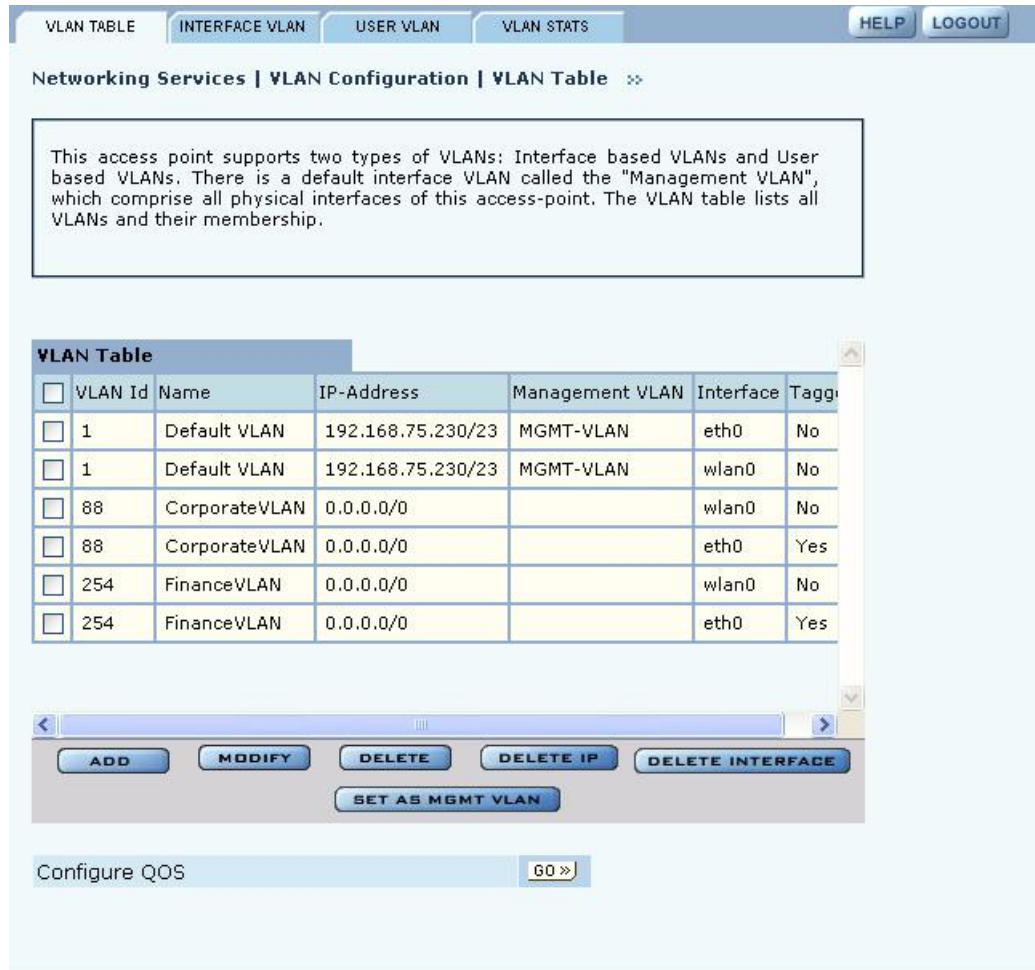
The VLAN Configuration panel contains the following tabs:

- 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 client stations 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	Numeric identifier for the VLAN. In bridging notation, this is the numeric ID that follows the br prefix.
Name	Alphanumeric name of the VLAN. The field is optional, unless it is the default VLAN. The maximum length of the VLAN name is 80 characters with no spaces.
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	Indicates whether this VLAN is the management VLAN.
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 4-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. VLAN IDs 1 and 4094 are reserved.) (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 with VLANs” on page 173.
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 **Add** 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.

NOTE: Do not add the wlan0 or wlan1 radio interfaces to the management VLAN.

Figure 78: VLAN Configuration - Interface VLAN

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

Add Interface VLAN

Select Interface *

VLAN ID * Default

Interface VLAN Table

Interface	VLAN ID
wlan1	1
wlan0	1
eth0	1

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

Field	Description
Select Interface	Select the AP interface. (required)
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

Field	Description
VLAN Name	Alphanumeric name of the VLAN
IP Address	Address used to access the VLAN
MAC Address	MAC addresses of the client stations mapped to this VLAN through their user group's service profile

See “Configuring SSID Parameters” on page 83 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**

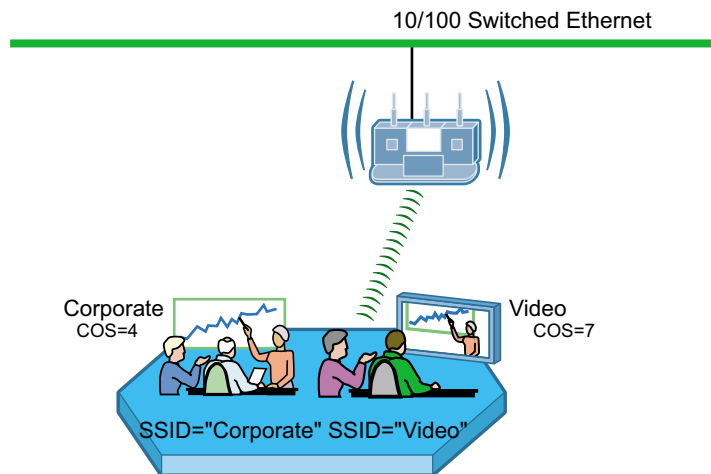
Configuring Quality of Service

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.

QoS is supported 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 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 83).
IP Precedence	Defines a mapping based on the first three 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.

Rule (continued)	Description
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 121) 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, its COS value is honored by the AP. If the packet is not VLAN-tagged, 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:

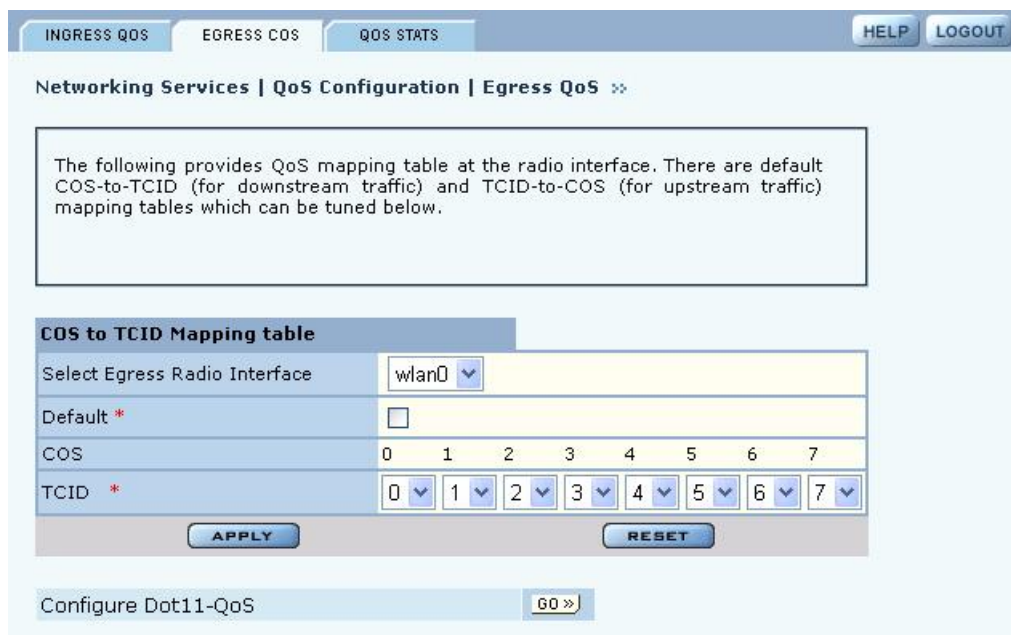
Function	Steps
Define TCI- to-COS mapping	<ol style="list-style-type: none"> 1 Select the radio interface for the mapping. 2 Select a COS value for each TCID value, or select Default to accept the default mapping. 3 Click Apply.
Define VLAN-to-COS mapping	<ol style="list-style-type: none"> 1 Click Add. 2 Select the AP interface. 3 Select the VLAN ID. (See “Configuring VLANs” on page 111 for information on VLAN IDs.) 4 Select a COS value or select Default to use the default mapping. 5 Click Apply.
Interface-to-COS mapping	<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 85) 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 Egress Radio Interface	Select the AP interface.
Default	Select to use the default mapping.
COS	Displays the COS levels.
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 85) 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
wlan1	1408,0,0,0,0,0,0,0	3650,0,0,0,0,0,0,2760
wlan0	73,0,0,0,0,0,0,0	2542,0,0,0,0,0,5,2996
eth0	11136,0,0,0,0,0,3119,0	7043,0,0,0,0,0,0,10

Configuring Advanced QoS

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

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

Class Order

The COS mappings on the QoS and Advanced QoS Configuration panels may yield conflicting results for ingress packet priority. Use the Class Order tab (Figure 85) 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 for non-VLAN tagged frames on the Ethernet interface (eth0) is:

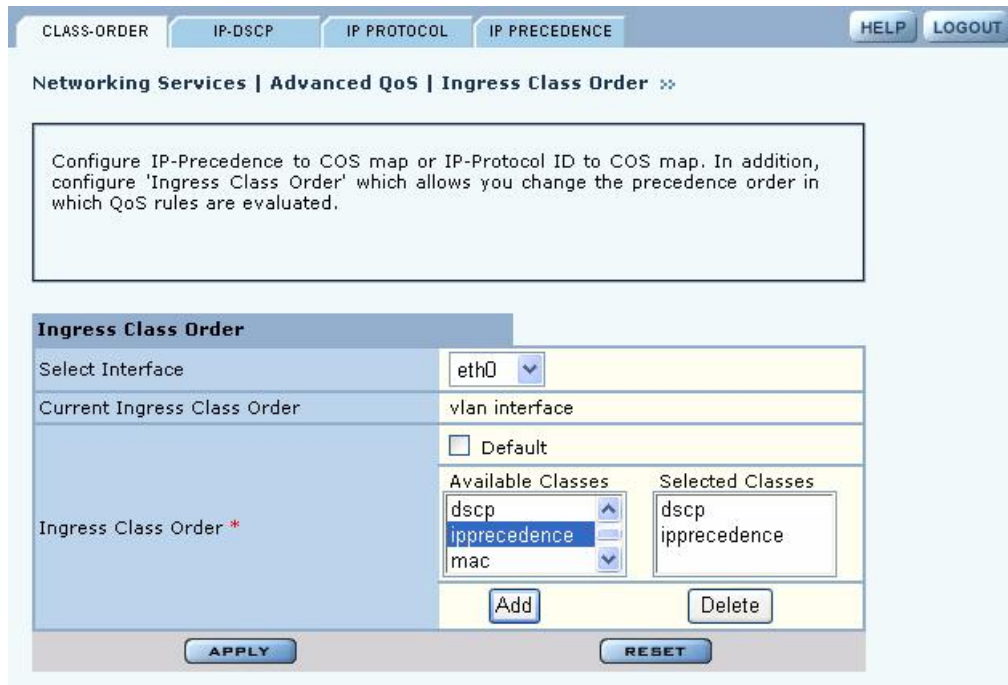
- DSCP
- VLAN
- Interface

The default class order for the wlan0 and wlan1 interfaces is:

- TCID
- DSCP
- MAC
- VLAN
- Interface

You can also select IP Protocol and IP Precedence to include in the class order.

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.

Field	Description
Current Ingress Class Order	Displays the current setting for class order.
Ingress Class Order - Default	Select to use the default mapping.
Ingress Class Order - Move to Top	If the default order is not chosen, select the class that you want to have at the top of the class order list, and click Add . This adds the class to the Selected Classes list. Continue adding classes in the order you want them to be applied. When you have finished, click Apply . The class order is saved and listed in the Current Ingress Class Order field.

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 Interface	Select the AP interface.
Default	Select to use the default mapping.

Field	Description
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/numbers.html>.

Figure 87: Advanced QoS Configuration - IP Protocol

The screenshot shows the configuration page for IP Protocol. It features a navigation bar with tabs: CLASS-ORDER, IP-DSCP, IP PROTOCOL (active), and IP PRECEDENCE. There are HELP and LOGOUT buttons. Below the navigation is a breadcrumb: Networking Services | Advanced QoS | IP Protocol ID to COS. A text box explains: "Configure IP-Precedence to COS map or IP-Protocol ID to COS map. In addition, configure 'Ingress Class Order' which allows you change the precedence order in which QoS rules are evaluated." The main configuration area is titled "QoS to IP Protocol" and includes a "Select Interface" dropdown set to "eth0". Below this is the "IP Protocol ID to COS" section with two input fields: "IP Protocol ID *" containing the value "4" and "COS" containing the value "2". There are APPLY and RESET buttons. At the bottom, there is a "Current IP Protocol ID to COS Map Table" section with a table header (Interface, IP Protocol-ID, COS) and DELETE and DELETE ALL buttons.

Configure the following fields:

Field	Description
Select 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 criteria used to accept or discard it.

Figure 89: Filter Configuration - Filter Table

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

	Interface Name	Ingress / Egress	Action	Filter
<input type="checkbox"/>	eth0	input	accept	None
<input type="checkbox"/>	eth0	output	accept	None
<input type="checkbox"/>	wlan0	input	accept	None
<input type="checkbox"/>	wlan0	output	accept	None
<input type="checkbox"/>	wlan1	input	accept	None
<input type="checkbox"/>	wlan1	output	accept	None

ADD EDIT DELETE

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

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

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

Figure 90: Filter Configuration - Add Filter Entry Panel

Filter Policy

Interface Name: eth0

Filter Direction: Input Output

Accept/Discard: Accept Discard

Select Match: Matched Unmatched Ether Type:

APPLY CANCEL

Filter Statistics

The Filter Stats tab (Figure 91) lists statistics for each defined filter. The statistics are calculated from the last time 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

Network Services | Filter Configuration | Filter Statistics

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

CLEAR STATISTICS REFRESH

Configuring Interfaces

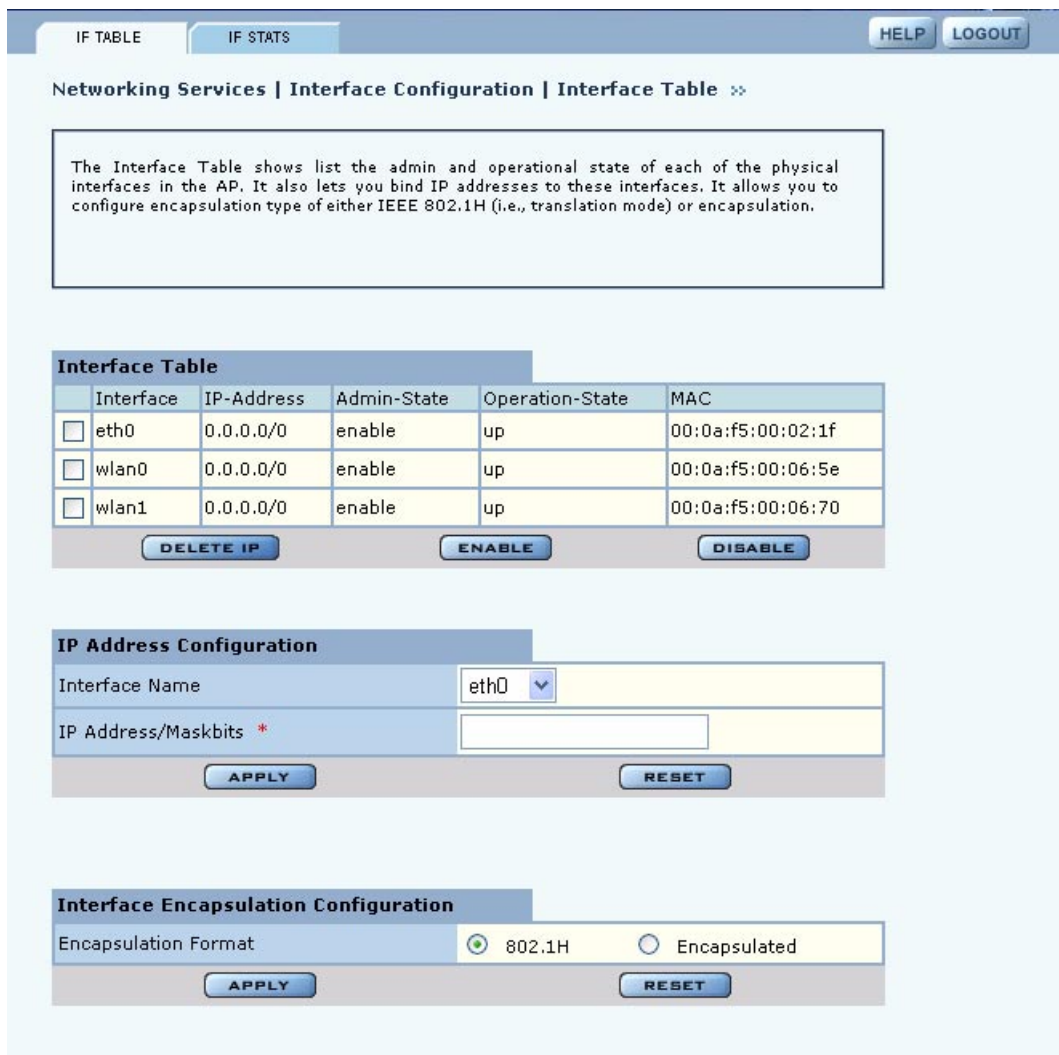
Use the Interface Configuration panel, accessible from the Networking Services menu, to configure the physical AP interfaces (wlan0, wlan1, eth0). The panel contains the following tabs:

- 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, Enable or Disable flag, and indication of whether the interface is currently operational. Modify the properties of the 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**:

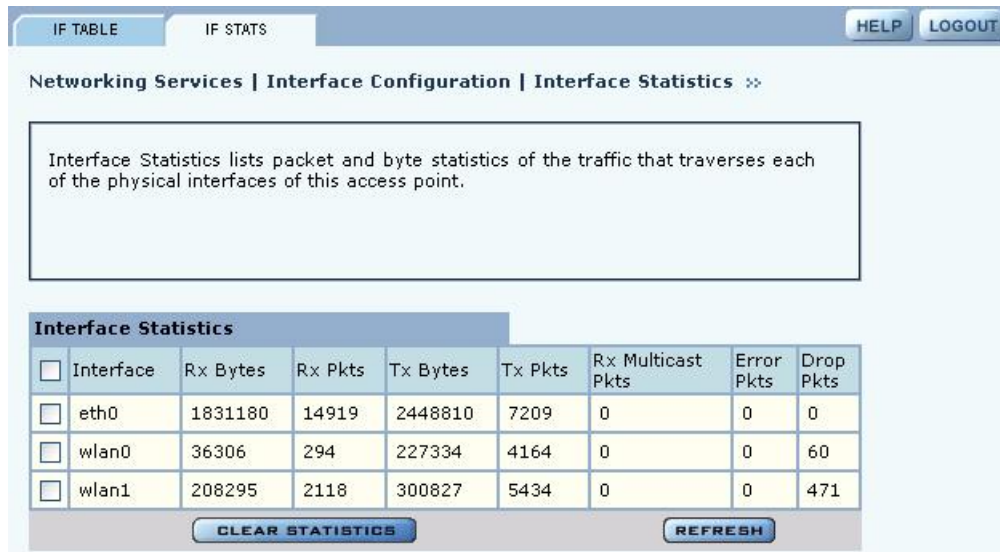
Field	Description
Interface Name	Select the AP interface name from the pull-down list.
IP Address	Enter the IP address to assign to the interface. (required)
Maskbits	Enter the subnet prefix length for the IP address. (required)

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



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

SNMP

HELP LOGOUT

Networking Services | SNMP Configuration >>

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

SNMP Configuration

Current Readonly Community String	public
Readonly Community String *	<input type="text"/>
Trap Sink IP Address *	<input type="text"/>
Trap Community	<input type="text"/>
Trap Sink Port	<input type="text"/>

APPLY RESET

SNMP Agent Table

<input type="checkbox"/>	Trap Sink Host	Trap Community	Trap Sink Port

DELETE

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

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

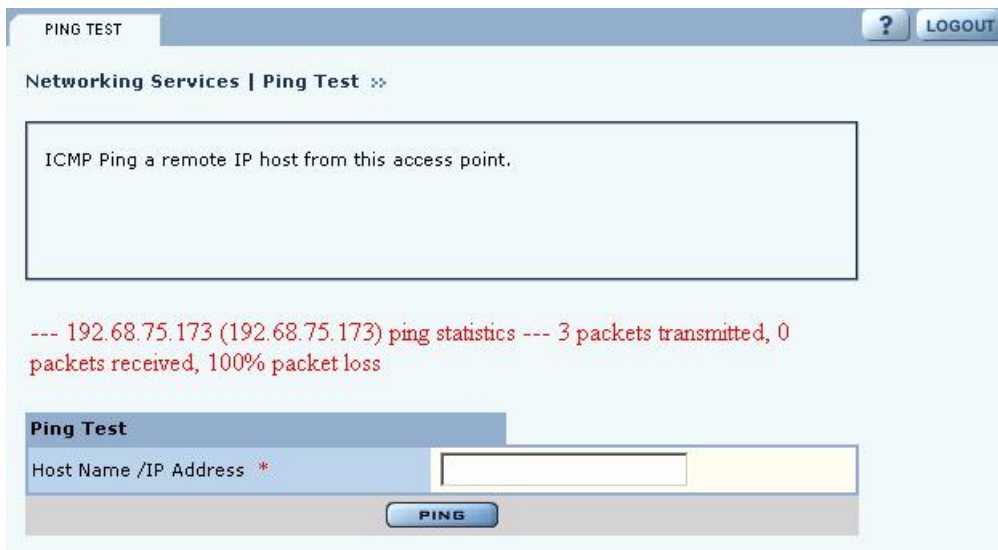
Click **Apply** to save your changes, or **Reset** to return to previously saved values.

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

Ping Test

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

Figure 95: Ping Test



6 Configuring a Wireless Backhaul

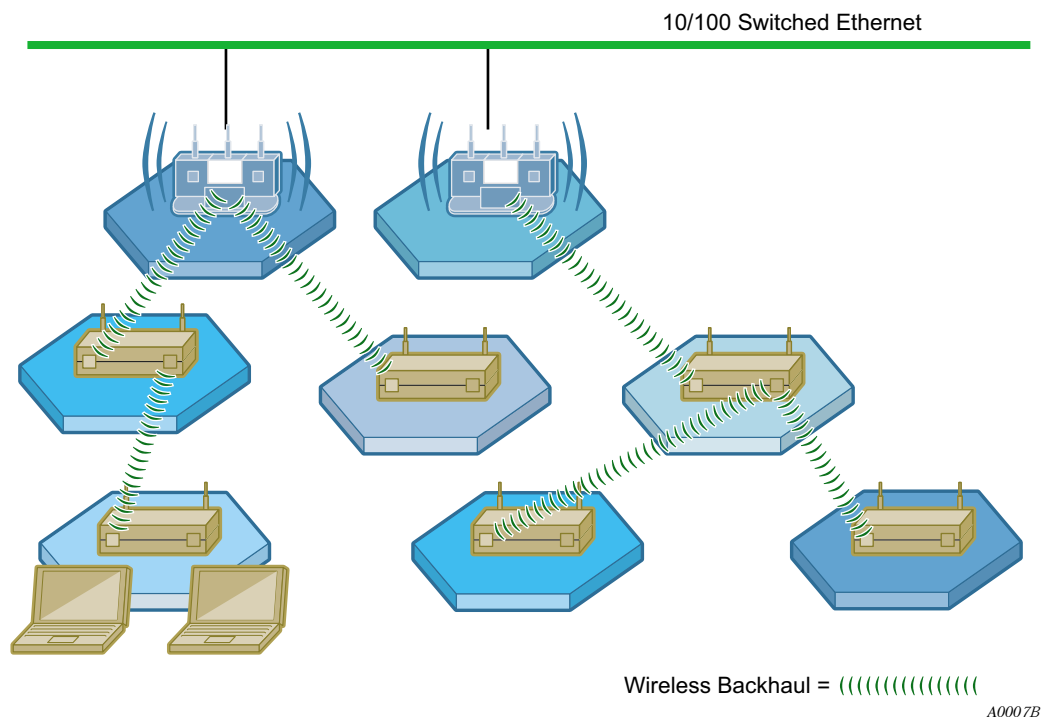
This chapter explains how to set up a wireless distribution system to cover a large area with limited wired network connectivity. It covers the following topics:

- **Introduction**
- **Use of Radios for Backhaul**
- **Wireless Backhaul Security**
- **Non-Wired or “Pseudo-Wired” Backhaul Configurations**
- **Setting Up a Wireless Backhaul**

Introduction

In a typical wireless backhaul configuration, some APs connect directly to the wired network, while others relay wireless signals from clients to the APs connected to the wired network. Wireless backhaul interconnects multiple Airgo Access Points to form a wireless distribution system in which an 802.11 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. 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

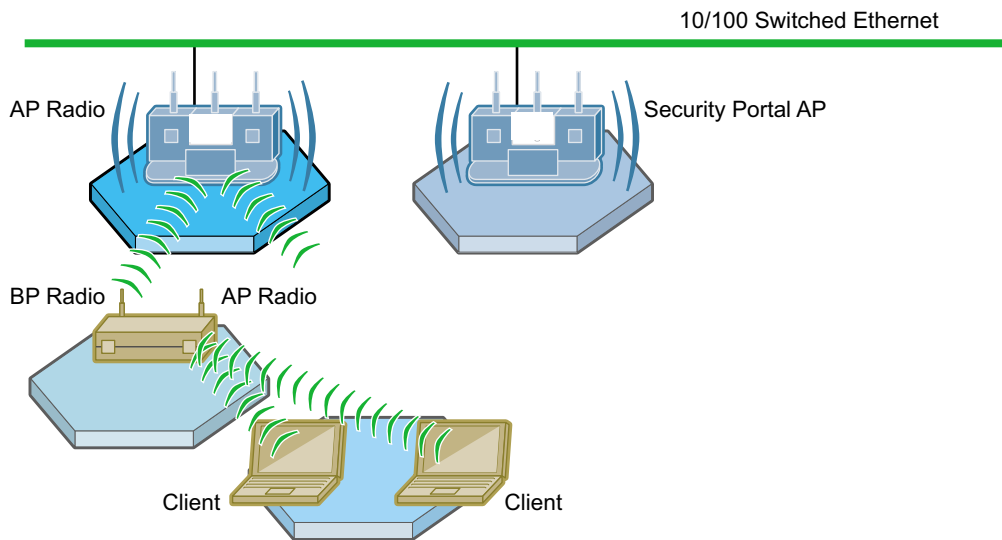
Each access point in a backhaul configuration must have two radios and be enrolled in the network.¹ Typically, one of the radios operates in normal (AP) mode to serve downstream access point radios or laptop clients. The other assumes the backhaul point (BP) role, relaying network traffic upstream from laptop clients or other access point BP radios.

A radio or radios can be configured to operate in the BP mode even if its AP is directly connected to the wired network, as in the case of building-to-building bridge applications.

Radio Bands and Backhaul Hops

Figure 97 illustrates how the AP and BP radios operate in a backhaul arrangement. For a BP radio to establish a link with an upstream access point, it must be able to receive radio signals from the AP radio in the upstream access point. Accordingly, the node with the BP radio must be within range of the upstream AP radio.

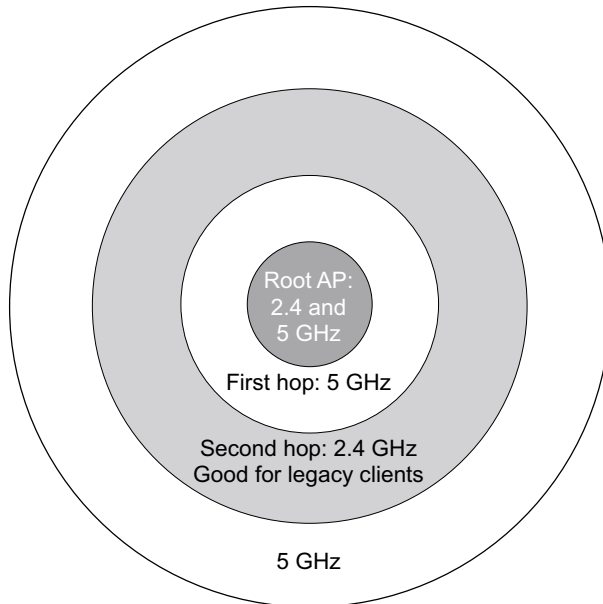
Figure 97: AP and BP Radios in Backhaul Arrangement



A00052

To prevent interference from compromising communications, the radios on each access point must operate in different bands. If the AP radio operates in the 2.4GHz band, then the BP radio must operate in the 5GHz band, and vice versa. As the number of hops increases, this creates an alternating band pattern (Figure 98).

¹ Each access point must have a wired connection to be enrolled in the network (see “Enrolling APs” on page 181). After the AP is enrolled, the wired connection can be removed.

Figure 98: Frequency Bands and Hops in Wireless Backhaul Networks

A0059

The alternating band requirement carries implications for the number of backhaul hops that may be desired to support network clients. The Airgo Access Point can technically support up to 7 backhaul hops from a client upstream to the wired AP; however, in practice, it is desirable to limit the number of hops for the following reasons:

- **Legacy client support:** To support a wide range of legacy clients, the link from clients to the downstream APs should be in the 2.4GHz band. Restricting the number of backhaul hops to two allows the client links to operate at 2.4GHz and the backhaul link to operate at 5GHz. All client types are served, and the two access point radios operate in different bands, as required (Figure 98).
- **Performance:** As the number of hops increases, maintaining performance may require advanced tuning of network parameters and restrictions on the number of supported APs and clients.

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 radio 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, 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 (in two to three 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.

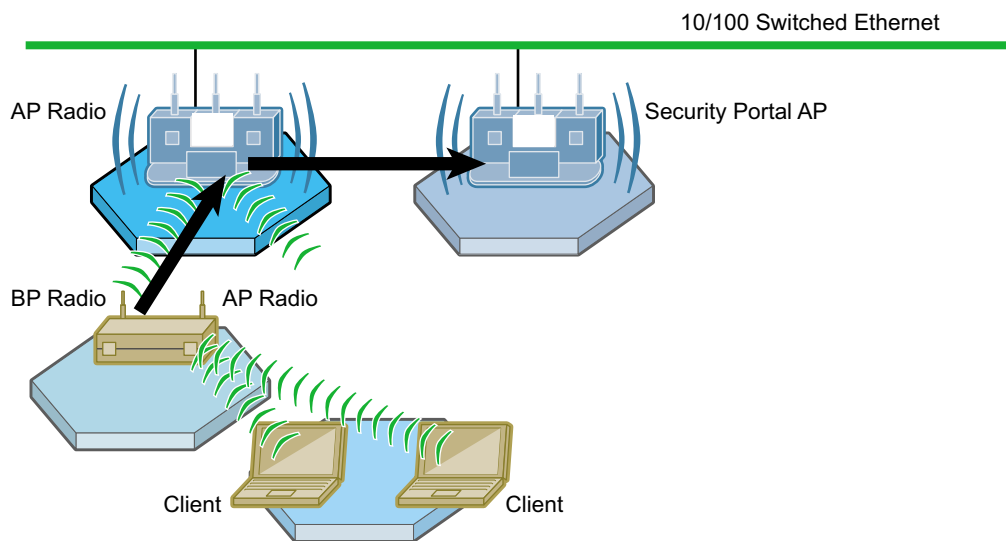
Wireless Backhaul Security

By implementing a common security policy across the network, you can provide appropriate security to clients while also ensuring that incompatibilities do not prevent formation of wireless backhaul links.

Overall wireless backhaul security depends upon the security modes assigned to all the AP and BP radios in the backhaul arrangement. The security mode assigned to the access point (see “Security Mode” on page 150) determines the security used by each AP radio, while the backhaul security policy (see “Link Criteria” on page 138) determines the security used by each BP radio. When a BP radio attempts to form a backhaul, the upstream AP authenticates locally, in the case of PSK, WEP, or Open security, or sends the request to the security portal, in the case of certificate-based security (Figure 99).

Each link from a client through to the root AP should use the same security mode; therefore, the AP and BP security modes should be the same. It is strongly recommended that you apply the same global security policy across the entire network, thereby ensuring that backhaul trunks can form wherever needed.

Figure 99: Certificate Authentication in Wireless Backhaul Network



A00053

Certificate security provides the highest level of protection and is the default option for backhaul security. The APs must be managed by NM Portal or NMS, and a security portal must be configured to service backhaul authentication requests. For backhaul authentication, requests are sent from the BP radio through to the security portal (see Figure 99).

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.

WPA-PSK provides effective security without requiring a security portal for backhaul authentication. Backhaul authentication is managed with the same PSK password used for the global security setting. When configuring a network of APs for wireless backhaul with WPA-PSK,

be sure that all APs are configured with identical SSID and PSK-password. This is necessary because PSK-password is bound to the SSID. A BP radio in a wireless backhaul network uses the PSK-password tied to the SSID to authenticate with an uplink AP. Even if you configure the BP backhaul criteria to include the correct uplink AP SSID, it will not form a backhaul if the SSID on the downlink AP is different from that of the uplink AP.

The WEP or Open option for backhaul security is compatible with either WEP or Open as the global security policy. If the global security mode is WEP on the AP and the wireless backhaul security mode is open or WEP on the BP radio, the backhaul will form with WEP security. If the global security mode is Open on the AP and the backhaul security mode is WEP or Open on the BP radio, then the backhaul will form with open security. The WEP or Open option is appropriate for hotspots, other networks that must support legacy clients, or applications such as hospitality suites that may have no security requirements.

Table 12 lists the available backhaul security options. For detailed information on these options, see Chapter 7, “Managing Security.”

Table 12: Wireless Security Settings for AP and BP Radios

Wireless Security (AP)			Backhaul Security (BP)			Comments	
Configuration of Wireless Security on Uplink AP			Configuration Required for Backhaul Security on Downlink AP (Any One of Following)			Security Portal Required	Valid BP Authentication Modes that will Allow Backhaul to Form
WPA-EAP	WPA-PSK	Open or WEP	Certif.	PSK	Open-or-WEP		
Enable	Disable	Disable	Enable	Disable	Disable	Y	BP->AP->security portal using WPA-EAP (Certificate)
Disable	Enable	Disable	Disable	Enable	Disable	N	BP->AP using WPA-PSK only
Disable	Disable	Enable	Disable	Disable	Enable	N	BP->AP using WEP, OR BP->AP using Open
Enable	Enable	Enable	Enable	Disable	Disable	Y	BP->AP->security portal using WPA-EAP (Certificate)
Enable	Enable	Enable	Disable	Enable	Disable	Y	BP->AP using WPA-PSK
Enable	Enable	Enable	Disable	Disable	Enable	Y	BP->AP using WEP, OR BP->AP using Open
Enable	Enable	Disable	Enable	Disable	Disable	Y	BP->AP->security portal using WPA-EAP (Certificate)
Enable	Enable	Disable	Disable	Enable	Disable	Y	BP->AP using WPA-PSK
Disable	Enable	Enable	Disable	Enable	Disable	N	BP->AP using WPA-PSK
Disable	Enable	Enable	Disable	Disable	Enable	N	BP->AP using WEP, OR BP->AP using Open

Non-Wired or “Pseudo-Wired” Backhaul Configurations

It is possible to configure a wireless backhaul to operate without a working connection to a wired network. This approach may be useful in a warehouse or factory setting as a means of establishing a wireless network disconnected from the corporate infrastructure. Clients can communicate with each other across the wireless distribution system without the need for administrative controls to restrict access to backend servers or the Internet.

You can configure non-wired backhaul in either of the following two ways:

Portal Method

Stage the AP deployment as if it will be connected to your wired infrastructure. Configure one of the APs as an NM Portal and enroll the other APs. Then configure the NM Portal AP to be in “wired only” mode. When you deploy the APs in the completely-wireless setting, they will automatically form a wireless backhaul with the NM Portal AP as the root, even though the NM Portal AP no longer has a wired connection.

Non-Portal Method

Manually configure each AP as a normal AP, making sure to select a global security mode that does not require use of a security portal (WPA-PSK, WEP, or Open). Select one of the APs to be in “wired-only” mode. When you deploy the APs, they will automatically form a wireless backhaul with the “wired-only” AP as the root, even though the AP does not have a wired connection.

Setting Up a Wireless Backhaul

Choose **Wireless Backhaul** from the Wireless menu to bring up the Wireless Backhaul configuration panel. The panel contains the following 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 100) to set up the network parameters for the wireless backhaul. These parameters specify the rules that apply to the BP radios which form uplink backhaul trunks by associating to normal (AP) radios. BP radios use the link criteria to determine the set of suitable APs for the backhaul trunk.

Figure 100: Backhaul Configuration - Link Criteria

LINK CRITERIA
CANDIDATE APs
TRUNK TABLE
TRUNK STATS
HELP
LOGOUT

Wireless Services | Backhaul Configuration | Uplink Criteria >>

Uplink Criteria configuration is only applicable to a downstream AP (i.e., wireless backhaul client). It provides rules for wireless trunk formation and enables a BP radio to select or reject an AP radio based on AP's SSID, IP subnet or BSSID.

Radio Interface Selection

Select Radio Interface: wlan0 All

Backhaul Security

Backhaul Security: Open-or-WEP
 PSK
 Certificate

Uplink Criteria Configuration

Uplink Criteria (Based on SSID, IP Subnet, Path Selection or BSSIDs)

SSID Criteria: New SSID JosephAP253
Detected SSID --select--

IP Subnet Criteria: IP-Address/Maskbits:

Path Selection Criteria: Lowest Weighted Cost
 Smallest Hop Count
 Highest Node Priority

Uplink BSSID Criteria: Accept from BSSIDs
 Discard from BSSIDs

Maximum Hops from Wired Network:

BSSIDs For Uplink Criteria

Available BSSID list:

Add BSSID: --select--

e.g. 0A:0B:0C:0D:0E:0F or 0A-0B-0C-0D-0E-0F

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.
Backhaul Security	Select from the following options (see “Wireless Backhaul Security” on page 136 for more information): <ul style="list-style-type: none">• Open-or-WEP: Compatible with the WEP or Open global security mode.• PSK: Compatible with the WPA-PSK global security mode using the same pre-shared key.• Certificate: Compatible with the WPA-EAP global security mode. Requires that the network have a security portal configured to provide backhaul authentication.
SSID Criteria	Select Detected SSID to connect to a specific network. To add an SSID that has not been detected, 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 previously 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 101) to identify the access points that can be used to create the uplink to the wired network.

Figure 101: 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 able to provide uplink connectivity. The table of uplink candidate APs shows the following information:

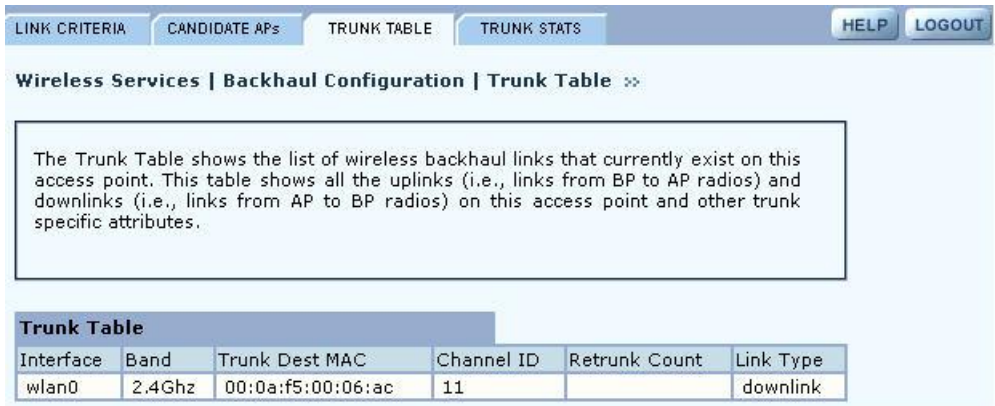
Item	Description
Interface	Radio interface of uplink candidate parent
Destination MAC Address	BSSID of the remote uplink candidate parent
AP Beacon Name	Name of the AP node of the candidate parent, sent in beacons

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

Trunk Table

Select the Trunk Table tab (Figure 102) 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 102: Backhaul Configuration - Trunk Table



This tab contains the following information:

Feature	Description
Interface Name	Radio interface of the BP radio (uplink) or AP radio (downlink) to which downlink trunks are connected. Applies to uplink and downlink trunks.
Band (2.4GHz or 5GHz, 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 103) to view statistics for the available backhaul trunks. If no trunks are detected, the table is empty. To clear the cumulative statistics, click **Clear Statistics**.

Figure 103: Backhaul Configuration - Trunk Stats

LINK CRITERIA CANDIDATE APs TRUNK TABLE TRUNK STATS HELP LOGOUT

Wireless Services | Backhaul Configuration | Trunk Statistics »

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

<input type="checkbox"/> Interface	Rx Bytes	Rx Pkts	Tx Bytes	Tx Pkts	Rx Multicast Pkts
<input type="checkbox"/> wlan0.tk0	52678	256	60401	785	8

CLEAR STATISTICS

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
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:

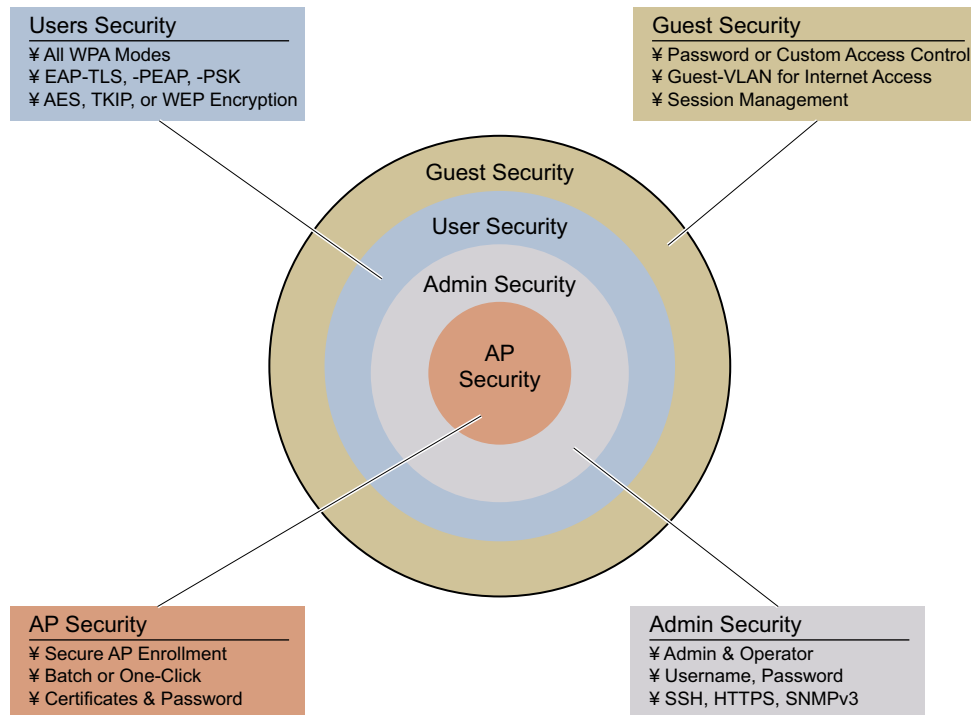
- [Introduction](#)
- [Security Elements](#)
- [Data Encryption](#)
- [Zone Privacy](#)
- [Configuring Wireless Security](#)
- [Configuring Authentication Zones](#)
- [Configuring Administrator Security](#)
- [Viewing Security Statistics](#)
- [Configuring Advanced Parameters](#)
- [Configuring Zone Privacy](#)

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

Introduction

Airgo Networks offers the strongest available security options for wireless networking, as listed here and illustrated in Figure 104:

- 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 a 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 104: Wireless Security Elements

A0047

Security Elements

Each security element emphasizes a different aspect of wireless network security. Guest security is described in Chapter 8, “Configuring Guest Access.”

AP Security

A highly secure process is provided 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.”) Several modes of authentication are supported, as listed in Table 13. WPA-PSK uses pre-shared keys (PSK) 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 which 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. Integration is also supported with RADIUS servers that support EAP-TLS or EAP-PEAP.

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

Table 13: Authentication Options

Type	Description
EAP-TLS	Certificate-based authentication, used by the security 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 a RADIUS server is 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 14 lists the available options for data encryption, in order of decreasing protection. The current standard for data encryption is WPA-AES, which provides financial-grade protection. The WEP encryption options use 64-bit or 128-bit encryption keys, assigned manually or dynamically, as dictated by the capabilities of the client. These offer some protection against casual interlopers; however, the WEP algorithms are vulnerable to compromise and can be difficult to maintain. WPA-TKIP closes the major WEP loopholes and can be an acceptable alternative to standard WEP.

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

Table 14: Encryption Options

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

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

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

Zone Privacy

Zone Privacy improves security for users in public hot spots by isolating client stations from each other. When zone privacy is deployed, a station can connect to the wired network but is not able to reach other stations associated to the same AP or stations associated to other APs over wireless backhaul. This section provides an overview of zone privacy. For configuration instructions, see “Configuring Zone Privacy” on page 164.

Zone privacy isolates client stations from each other by limiting the paths along which APs forward traffic. When zone privacy is enabled, the AP forwards traffic from client stations to the Ethernet interface but does not redistribute the traffic back to the AP BSS, nor to the BSS on the second AP radio. When zone privacy is enabled on APs interconnected over wireless backhaul, traffic from client stations is forwarded toward the wired network over wireless backhaul connections. APs receiving traffic from a BP (backhaul point) radio only forward traffic to another AP over a wireless backhaul connection or to the Ethernet interface. APs in the wireless distribution system do not forward traffic received from a BP radio to any other BSS.

The zone privacy rules governing traffic forwarding apply to traffic from client stations and to management traffic from APs. Consequently, the partial network connectivity resulting from zone privacy can affect features such as client roaming and peer-to-peer communications between APs. To mitigate against any issues that may arise, enable zone privacy only on non-management VLANs that carry only user data traffic. Specifically, subscriber privacy can be enforced if ports attached to APs are members of different VLANs carrying user data. When zone privacy is desired between two wired APs, all clients that associate to the two different APs are part of different user

VLANs. A VLAN switch is able to segregate traffic between the two VLANs such that any client of the first AP is not able to contact any client on the second AP.

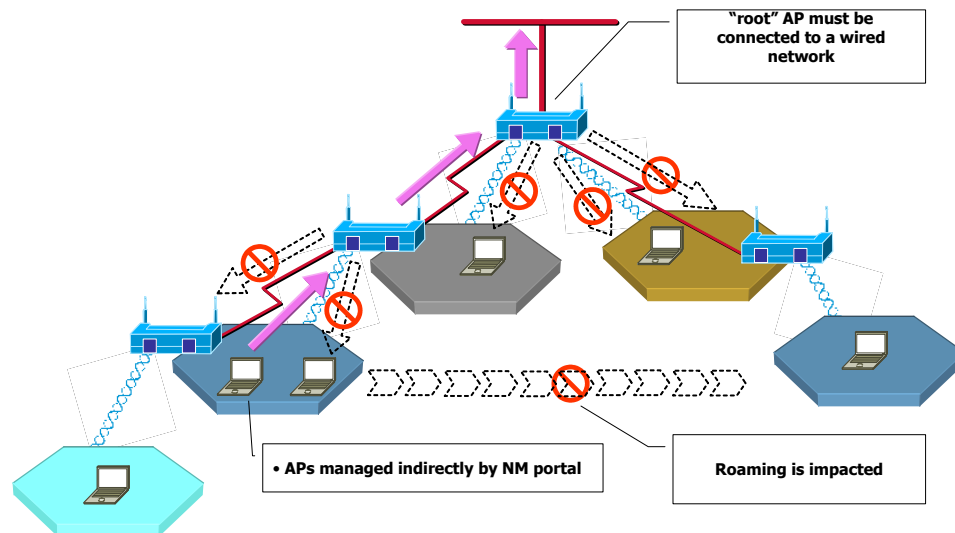
To provide full connectivity between APs for management traffic, assign all ports on the APs to the management VLAN.

Zone Privacy Deployment without VLANs

When zone privacy is implemented without VLANs, communication forwarding rules can affect station and management traffic between the APs. The following deployment constraints apply (Figure 105):

- The root AP for the wireless backhaul network must be attached to the wired network because all downstream APs are guaranteed connectivity only to the root AP.
- APs should be managed using policy distribution from NM Portal because the station has connectivity to only a subset of APs over the wireless backhaul.
- Station reassociation fails if a station roams to a BSS started by an AP that cannot exchange Inter Access Point Protocol (IAPP) messages with the AP from which the station has moved. The IAPP messages are used to support roaming of client stations between APs and enable neighboring APs to keep up-to-date information concerning the status of roaming client stations.

Figure 105: Zone Privacy Using a Single VLAN

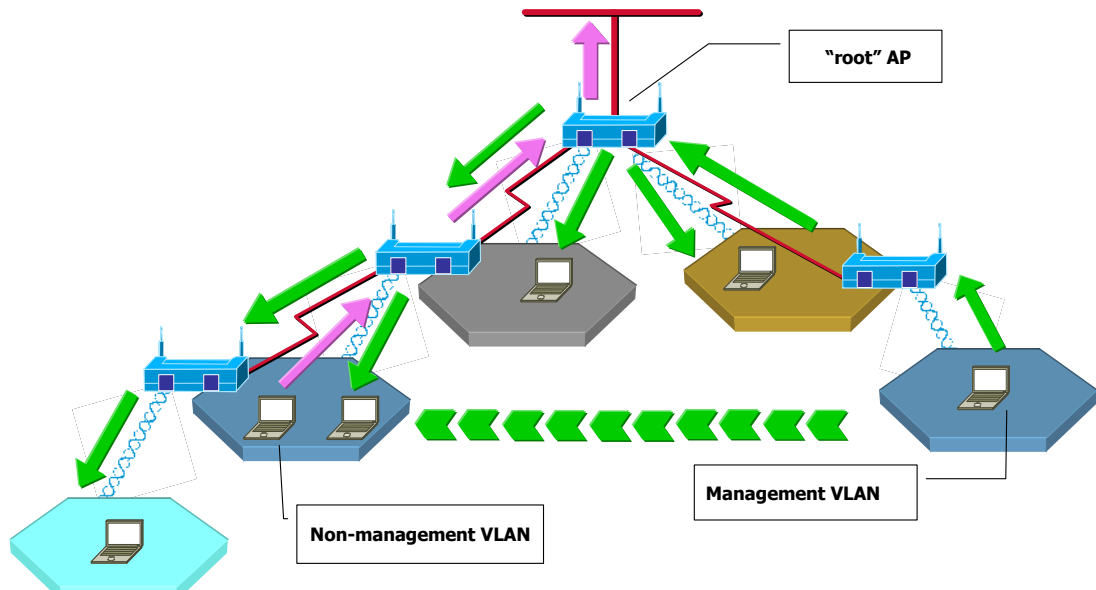


Zone Privacy Deployment on Multiple VLANs

When zone privacy is deployed using multiple VLANs, you can designate one VLAN for management traffic and others for user data. Enabling zone privacy only on the VLANs that carry user data traffic eliminates several of the constraints caused by connectivity limitations. The following requirements apply when using multiple VLANs to deploy zone privacy:

- The root AP for the wireless backhaul network must be attached to the wired network.
- Zone privacy for subscribers must be enabled on a non-management VLAN.
- APs can be managed directly from any station, if that the station is on the management VLAN.
- Roaming is unaffected by zone privacy because IAPP messages are sent on the management VLAN that has full connectivity over the wireless distribution system.

Figure 106: Zone Privacy - using a Management VLAN



Configuring Wireless Security

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

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

Security Mode

Use the Security Mode tab (Figure 107) to assign the encryption and authentication methods, including WPA, WEP, or Open. Allowing multiple encryption modes can be useful to support installations with a mixture of client wireless adapters. The allowed combinations have some limitations; it is not possible to enable both WEP and Open simultaneously. Also, Open and WPA encryption modes require each mode to be mapped to a separate VLAN (see “Configuring VLANs” on page 111).

Figure 107: Security Services - Security Mode

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

Security Configuration	
WPA Security Mode	
Enable WPA	<input checked="" type="checkbox"/>
WPA-EAP	<input checked="" type="checkbox"/> (RADIUS based Automatic Network Keying) Configure Auth Server for SSID
WPA Pre-Shared Key	<input type="checkbox"/> (Manual Key Distribution) Configure Key for SSID
Encryption Type	aes-only
WEP Security Mode	
Enable WEP Based Security	<input type="checkbox"/>
WEP Key-Length	128 - bit
Dynamic WEP with 802.1x	(RADIUS based Automatic Network Keying) Configure Auth Server for SSID
Static WEP	<input type="checkbox"/> (Manual Key Distribution)
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
Open Access Security Mode (No Encryption)	
Enable Open Access	<input checked="" type="checkbox"/>

WPA Security

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

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

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

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

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



NOTE: Selecting WPA-EAP or WPA-PSK displays a link that leads to the SSID Authentication tab. Refer to “SSID Authentication” on page 152 for instructions on using this tab.

WEP Security

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

Field	Description
Enable WEP	Activate the WEP settings. The Airgo AP supports WEP with dynamic and manually entered keys. To use dynamic keys, select WEP, but do not enter values in the Key fields.
Key-Length	Select 64-bit or 128-bit.
Key 1 - Key 4	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)

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

Open Access

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

SSID Authentication

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

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

Figure 108: Security Services - SSID Auth

SECURITY MODE **SSID AUTH** [HELP](#) [LOGOUT](#)

Security Services | Wireless Security | SSID Authentication >>

SSID Security Configuration includes:

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

SSID Authentication

SSID Name * [SSID Details](#)

WPA Pre-Shared Key

Auth Server Configuration

Security Portal * RADIUS Servers: 192.168.168.24

External Auth Servers *

RADIUS Servers:

Enable MAC Access Control List (RADIUS based MAC-ACL)

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

Configure External Auth Server List [GO >>](#)

Assign the following values to configure SSID authentication:

Feature	Description
SSID Name	Select from the SSID pull-down list. Click SSID Details to view more SSID-related information, enable multiple SSIDs, or change other SSID attributes.
WPA Pre-Shared Key	Enter the pre-shared key for WPA, if appropriate. This field is grayed out if WPA-PSK is not the selected authentication type.
Authentication Server Configuration	Select the Security Portal or External Authentication Servers radio button. For Security Portal, the IP addresses of all security portals are displayed below the radio button. For External security, select from the list of RADIUS servers or click Go at the bottom of the tab to configure the authentication server list (see “Authentication Zones” on page 155). (required)
Enable MAC Access Control List	Select to enable authentication using MAC addresses centrally managed in a RADIUS server. For MAC-ACL authentication, it is necessary to use a security portal or external RADIUS server.

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

An external RADIUS server can also be added from this tab. Click **Go** at the bottom of the tab to open the Authentication Zone tab of the Authentication Zones panel. For instructions on adding a server, refer to “Configuring Authentication Zones” on page 155.

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

- 1 The RADIUS server must have PAP authentication enabled for these MAC ACL users
- 2 The RADIUS server can expect the AP to send the following standard RADIUS attributes in the authentication request for purposes of policy configuration and interoperability. (MAC addresses must have no colon or hyphen separators):

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

- 3 The RADIUS server should enforce a policy such that MAC ACL users are only allowed to use PAP authentication for Wireless. This is important because the username and password are not secret.
- 4 The RADIUS server may optionally send back the Session-Timeout attribute to override the AP default session-timeout.
- 5 The RADIUS server may optionally send back an attribute encoded with the user group.

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

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

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

- 2 The RADIUS server can use these attributes to enforce policies such that EAP based authentication is mandatory for Wireless.
- 3 The RADIUS server may optionally send back the Session-Timeout attribute to override the AP default session-timeout.

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

Configuring Authentication Zones

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

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

The Authentication Zone panel contains two tabs:

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

Authentication Zones

On the Auth Zones tab (Figure 109), you can create new authentication zones or modify existing ones. Select check boxes for authentication zones you want to modify or delete, or click **Add** to add a new zone.

Figure 109: Authentication Zones - Auth Zones

Security Services | Auth Zones | Auth Zone Table »

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

Auth Zone	Auth Servers	Admin Zone
<input type="checkbox"/> DeerCreekCoAuth	192.168.168.1	NO

ADD DELETE MODIFY

Set the following values on the Add Auth Zone entry panel (Figure 110):

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

Click **Add** after making selections.

Figure 110: Authentication Zones - Add Auth Zones

<input type="checkbox"/>	Auth Server	Port
<input type="checkbox"/>	192.168.168.24	1812
<input type="checkbox"/>	192.168.168.1	1812

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

Field	Description
Auth Server	IP address of the RADIUS authentication server
Shared Secret	Secret key to be entered and confirmed
Port Number	Port number for the server (default is 1812)

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

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

Authentication Servers

Open the Authentication Servers tab (Figure 111) to view the current authentication servers and add or delete servers. This table shows the list of internal authentication servers (security portals) and external authentication servers. The servers that do not have an associated check box are security portals.

Figure 111: Authentication Zones - Auth Servers

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

<input type="checkbox"/>	Auth Server	Shared Secret	Port
<input type="checkbox"/>	192.168.168.24	*****	1812
<input type="checkbox"/>	192.168.168.1	*****	1812

Configuring Administrator Security

Use the Administrator Security menu item to administer the administrator password and view AP certification information.

Administrator Password

Choose **Administrator Security** from the Security Services menu to open the Administrator Security panel, Admin Password tab (Figure 112).

Figure 112: Administrator Security - Admin Password

Set the following values on this panel:

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

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

External RADIUS Server Settings

The following rules apply for an external RADIUS server:

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

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

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

AP Certificate

To view information about the unique X.509 security certificate assigned to the AP, choose **Administrator Security** from the Security Services menu to open the Administrator Security panel, and then select AP Certification (Figure 112).

Figure 113: Administrator Security - AP Certificate

The AP has a unique X.509 digital certificate. The details of this certificate are displayed in the table below.

- * The X.509 Thumbprint is used for authentication in the enrollment process and web (https) authentication.
- * The SSH Fingerprint is used to authenticate SSH communications.

AP Certificate Table	
Subject Name	"AP_00-0A-F5-00-02-1F"
Issuer Name	"AP_00-0A-F5-00-02-1F"
Serial Number	0
X.509 Thumbprint	1d:5b:5f:3e:b9:97:4c:79:a8:0d:3a:e9:03:f8:8c:d3:6f:3e:bb:f3
SSH Fingerprint	93:18:fd:5e:be:9f:0f:e9:13:67:5e:08:84:e8:b4:f1

This tab contains the following information:

Item	Description
Subject Name	AP Device ID.
Issuer Name	Device ID of the certificate issuing entity.
Serial Number	Serial number of the AP.
X.509 Thumbprint	SHA1 hash of the AP digital certificate. Used to authenticate the identity of the AP device during AP enrollment and when managing the AP using the Web browser interface.
SSH Fingerprint	MD5 hash of the AP digital certificate. Used to authenticate the identity of the AP when using SSH to remotely manage the AP.

Viewing Security Statistics

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

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

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

Authentication Statistics

The Authenticator Statistics tab (Figure 114) contains EAPOL statistics, which correspond to authentication messages sent between a station and an AP. These are generated by the traffic from WPA or 802.1x-based wireless authentication. Only radios in AP mode produce this data.

Figure 114: Security Statistics - Authenticator Stats

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

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

The tab contains the following information:

Field	Description
Interface	Select the radio interface of interest for viewing statistics.
Last RX EAPOL Frame Source	The source MAC address from the last EAPOL frame received by the AP. This identifies a station or BP that is currently authenticating or re-authenticating with the AP.

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

Supplicant Statistics

The Supplicant Stats tab (Figure 115) reports on authentication messages sent between a local BP radio and the upstream AP. Only radios in BP mode return these statistics. The statistics are generated from the EAPOL protocol, which is used for 802.1x authentication.

Figure 115: Security Statistics - Supplicant Stats

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

802.1x Supplicant Statistics

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

CLEAR STATISTICS REFRESH

The tab contains the following information:

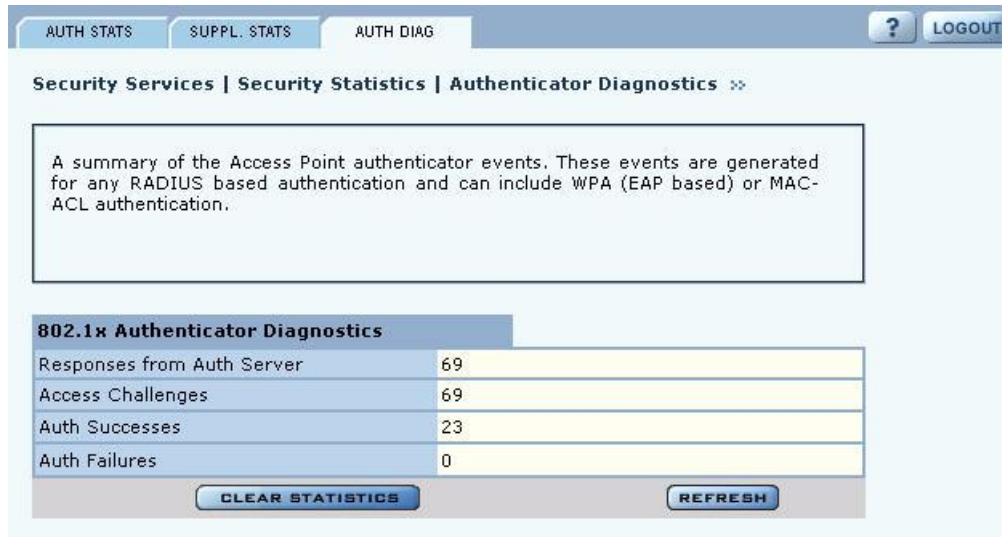
Field	Description
Interface	Select the radio interface of interest for viewing statistics.
Last RX EAPOL Frame Source	The source MAC address from the last EAPOL frame received by the BP. This identifies the upstream AP that is currently authenticating or re-authenticating with the BP.
Last RX EAPOL Frame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

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

Authenticator Diagnostics

The Authenticator Diagnostics tab (Figure 116) contains a summary of the AP authenticator events received from a backend authentication server. These events are generated for any RADIUS based authentication and can include WPA (EAP-based), MAC-ACL, or dynamic WEP authentication.

Figure 116: Security Statistics - Authenticator Diagnostics



The tab contains the following information:

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

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

Configuring Advanced Parameters

Choose **Advanced Configuration** from the menu tree to open the Advanced RADIUS configuration panel (Figure 117). It is not necessary to modify any settings on this panel.

Figure 117: Advanced Configuration - Timeouts

TIMEOUTS HELP LOGOUT

Security Services | Advanced Configuration | Timeouts & Misc. >>

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

Timeouts

Session Timeout (in seconds)	<input type="text" value="28800"/>
Group Key Interval (in seconds)	<input type="text" value="3600"/>
RADIUS Timeout (in seconds)	<input type="text" value="3"/>
RADIUS Retries	<input type="text" value="2"/>

RADIUS Attribute for User-Groups

RADIUS Standard Attribute	<input type="radio"/>
Attribute Type	<input type="text"/>
Vendor-Specific Attribute	<input checked="" type="radio"/>
Vendor ID	<input type="text" value="13586"/>
Vendor Sub-type	<input type="text" value="1"/>
Interpretation	<input checked="" type="radio"/> String <input type="radio"/> Integer

The panel contains the following fields:

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

Field	Description
RADIUS Retries	Number of retransmit attempts after which the RADIUS request is marked a failure.
External RADIUS Group-Key Attribute (for User Group ID)	RADIUS attribute used by the AP to determine the user group (see “SSID Details” on page 87). When a wireless user is authenticated by a RADIUS server, the server can optionally send the AP the user group for the association. If a user group is not returned, the user is not assigned a group and gets the default service profile for the SSID. By default, a Vendor Specific Attribute is used (13586, 1, String).

Other standard or vendor-specific attributes can be used to determine service policies. For example, an enterprise having an existing RADIUS attribute for VLANs (Tunnel-Private-Group-ID) can reuse the attribute for service profile assignment by configuring it as the RADIUS attribute for user groups. This can be accomplished by selecting RADIUS Standard Attribute Type 81, with a string interpretation. The VLAN string that is returned by the RADIUS server will then be used as the name of the user-group.

For attributes that return integer values, the group name will be the string representation of the same integer. For example, the integer 1 will be treated as the group name “1.”

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

Configuring Zone Privacy

Choose **Zone Privacy** from the menu tree to open the configuration panel for zone privacy (Figure 118).

Figure 118: Zone Privacy

CONFIGURATION HELP LOGOUT

Security Services | Zone Privacy | Zone Privacy

Modify the Zone Privacy of a VLAN from here. User can also view the Zone Privacy details of all VLAN's here.

Enable Zone Privacy All VLAN

ENABLE **DISABLE**

Zone Privacy Table

VLAN-Id	VLAN-Name	Zone-Privacy	Blocked-Frames
1	Default VLAN	disable	0

REFRESH

The panel contains the following settings:

Item	Description
Enable Zone Privacy	<p>Allows you to enable zone privacy on one or more VLANs.</p> <ol style="list-style-type: none">1 Select a VLAN to which zone privacy will apply or select All VLANs to apply the feature across all defined VLANs.2 Click Enable.3 Repeat if desired to enable zone privacy on additional VLANs.
Zone Privacy Table	<p>Displays a list of VLANs and their current zone privacy status. Each row contains the following information:</p> <ul style="list-style-type: none">• VLAN ID• VLAN Name• Zone privacy status: Enabled or Disabled• Blocked frames: number of frames blocked due to enforcement of zone privacy rules

8 Configuring Guest Access

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

- [Overview](#)
- [Internal Landing Page](#)
- [External Landing Page](#)
- [Configuring Guest Access with VLANs](#)
- [Guest Access Services Panel](#)

Overview

Guest access allows visitors to a facility to access the Internet through the wireless network without gaining access to the corporate network. Unauthenticated users are permitted to associate to an AP, but any web communications are captured and directed to a controlled landing page or captive portal. The landing page allows the guest user to log in using web-based authentication, and can be implemented by way of an internal or external URL. The page can inform unauthenticated users of the network access policies and provide instructions on obtaining the guest password. Following successful authentication, the guest user is released from the captive pages and allowed to access resources permitted to guest users.

The Airgo AP supports guest access administration with or without the use of VLANs to segregate guest traffic from other network traffic. Both approaches are compatible with the use of external and internal landing pages.

Guest Access without VLANs

This option is ideal for hot spot deployments in which guest authentication is required, but it is not necessary to segregate guest traffic from other network traffic. Once guests are authenticated, they are automatically assigned a default guest service profile, which includes the default security mode for the AP, and provided with full network access.

Guest access without VLANs is compatible with open or mixed security modes. Mixed security modes are desirable if some users have need for ongoing network access, while others will only access the network periodically as guests. Open access only is desirable for hot spot settings that cater almost exclusively to guests.

If the security mode is Open access only, then all users connecting to the configured SSID are treated as guest users and are directed to the guest login page. Once they successfully log in to the network, they are connected to the network, but their data traffic is not encrypted.

If the security mode is mixed (with WPA-PSK configured), then users who know the WPA-PSK password can connect to the network using that password. Their data traffic will be encrypted over the air. Users who try to connect to the network using open authentication will automatically be presented the guest login page. Once authenticated, they will be provided network access, but their traffic will not be encrypted.