

Aruba AP-80 MB/SB Outdoor Wireless Access Point/Bridge



Installation and User Guide

Copyright

© 2007 Aruba Networks, Inc. All rights reserved.

Trademarks

Aruba Networks® is a registered trademark, and Mobility Management System, RFprotect, and Bluescanner are trademarks of Aruba Networks, Inc.

All other trademarks or registered trademarks are the property of their respective holders.

Specifications are subject to change without notice.

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.



www.arubanetworks.com

1322 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Preface	Overview of this Manual	7
	Text Conventions	8
	Contacting Aruba Networks	8
Chapter 1	Hardware Overview	11
	About the Aruba AP-80SB and AP-80MB	11
	AP-80SB	11
	AP-80MB	11
	Package Checklist	12
	Recommended Optional Items—Supplied Separately	12
	Hardware Model Overview	13
	AP-80SB	13
	AP-80MB	14
	Ports, Connectors, and Antennas	14
	Power over Ethernet Injector/Adapter	15
Chapter 2	Installation	17
	Installation Overview	17
	AP-80 MB/SB Setup Process	17
	AP-80MB/SB Installation	17
	Preparing for Installation	18
	Staging the Installation	18
	Mounting the Unit	18
	Using the Pole-Mounting Bracket	18
	Mounting on Larger Diameter Poles	19
	Using the Wall-Mounting Bracket (Optional Part)	20
	Connect External Antennas	21
	Connect the Ethernet Cable to the Unit	21
	Connect the Internal Power Injector Module	22
	Align Antennas	23
Chapter 3	Planning and Deployment Considerations	27
	Point-to-Point and Multipoint Wireless Links	27
	Data Rates	27
	Radio Path Planning	28
	Antenna Height	29
	Antenna Position and Orientation	31
	Antenna Polarization	31
	Radio Interference	31
	Weather Conditions	32
	Ethernet Cabling and Grounding	32
	Grounding	32
	Sample Network Topologies	32
	Point-Point WDS Bridge	32
	Point-Multipoint WDS Bridge	33

	Fat Access Point with Wireless Backhaul	33
	Fat Access Point with Wired Backhaul	34
Chapter 4	Provisioning and Initial Setup	35
	Management Interfaces	35
	Factory Default Configuration	35
	Connecting to the AP-80 MB/SB for the First Time	38
	Using the Web-Based Management Setup Wizard	38
Chapter 5	Advanced Configuration	45
	System Identification	47
	TCP / IP Settings	48
	RADIUS	51
	Authentication	54
	Filter Control	57
	SNMP	58
	VLAN	61
	AP Management	63
	Administration	64
	Changing the Password	65
	Setting the Session Timeout	65
	Upgrading Firmware	65
	Backing Up and Restoring the Configuration File	66
	Resetting the AP	66
	System Log	67
	Set the following parameters on this page:	68
	Wireless Distribution System (WDS)	70
	STP	72
	RSSI	74
	Radio Interface	76
	Radio Settings	77
	Security	84
	Wired Equivalent Privacy (WEP)	87
	Wi-Fi Protected Access (WPA)	91
	802.1x	94
	AP Status	95
	Station Status	98
	WDS-STP Status	99
	Event Logs	100
Chapter 6	CLI Commands	103
	Using the Command Line Interface	103
	Telnet Connection	103
	Entering Commands	104
	Keywords and Arguments	104
	Minimum Abbreviation	104
	Command Completion	104
	Getting Help on Commands	104
	Partial Keyword Lookup	105
	Negating the Effect of Commands	105
	Using Command History	105
	Understanding Command Modes	105

	Exec Commands	106
	Configuration Commands	106
	Command Line Processing	107
	Command Groups	107
	General Commands	108
	System Management Commands	112
	System Logging Commands	125
	System Clock Commands	129
	DHCP Relay Commands	133
	SNMP Commands	135
	Flash/File Commands	146
	RADIUS Client Commands	149
	802.1x Authentication Commands	155
	MAC Address Authentication Commands	160
	Filtering Commands	163
	WDS Bridge Commands	167
	Ethernet Interface Commands	179
	Wireless Interface Commands	183
	Rogue AP Detection Commands	205
	Link Integrity Commands	209
	IAPP Commands	213
	VLAN Commands	213
	WMM Commands	215
Appendix A	Troubleshooting	219
Appendix B	Cables, Pinouts	221
	Aruba 80 8-Pin DIN Ethernet Connector Pinout	221
	Aruba 80 8-Pin DIN to RJ-45 Cable Wiring	221
	Aruba 80 Power over Ethernet Injector Module 10/100BASE-TX Pin Assignments	222
Appendix C	Specifications	223
	Product Features	223
	Power Over Ethernet	223
	Radio Characteristics	223
	Compliance	224
	United States	224
	Canada	224
	Japan	225
	Korea	225
	Europe	226
	Taiwan	226
	Specifications	228
	Aruba 80 Detachable Antennas	230
	AP-80SB Integrated Antenna	231
	Proper Disposal of Aruba Equipment	232
	Waste of Electrical and Electronic Equipment	232
	European Union RoHS	232
	China RoHS	232

Glossary

235

Index

239



Aruba Wireless Access Points are radio transmission devices and as such are subject to governmental regulations. Aruba Wireless Access Points are sold through authorized, non-retail, distribution channels and are required to be deployed by a Professional Installer / Qualified Network Administrator. The professional installer responsible for the configuration and operation of Access Points must ensure the installation complies with local regulations, frequencies, channels and output power.

This preface includes the following information:

- An overview of the sections in this manual
- A key to the various text conventions used throughout this manual
- Related documentation
- Contacting Aruba Networks

Overview of this Manual

This manual is for trained technicians responsible for installing the Aruba AP-80 MB/SB Outdoor Wireless Access Point/Bridge. This manual is organized as follows:

- [Chapter 1, “Hardware Overview”](#) — Describes the main features of this product and explains the process for setting up the AP-80 MB/SB.
- [Chapter 2, “Installation”](#) — Provides instructions for provisioning and installing the AP-80 MB/SB.
- [Chapter 3, “Planning and Deployment Considerations”](#) — Provides information for deploying fixed point-to-point or point-to-multipoint wireless links.
- [Chapter 4, “Provisioning and Initial Setup”](#) — Provides instructions for creating the initial configuration.
- [Chapter 5, “Advanced Configuration”](#) — Provides instructions for creating advanced system configurations.
- [Chapter 6, “CLI Commands”](#) — Explains the use of the command line interface and command details.
- [Appendix A, “Troubleshooting”](#) — Explains strategies and techniques for solving common operational problems with the AP-80 MB/SB.
- [Appendix B, “Cables, Pinouts”](#) — Describes interface, cable, and adapter specifications for system ports.
- [Appendix C, “Specifications”](#) — Describes the system specifications.
- [“Glossary”](#) — Describes the terms used in this document.

For the current versions of user manuals, or to obtain the latest product release notes, visit the support section of our Web site.

Text Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Table 1 *Text Conventions*

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
System items	This fixed-width font depicts the following: <ul style="list-style-type: none">● Sample screen output● System prompts● Filenames, software devices, and certain commands when mentioned in the text
Commands	In the command examples, this bold font depicts text that the user must type exactly as shown.
<Arguments>	Italicized text within angle brackets represents items that the user should replace with information appropriate to their specific situation. For example: # send <text message> In this example, the user would type “send” at the system prompt exactly as shown, followed by the text of the message they wish to send. Do not type the angle brackets.
{keyword1 keyword2}	Options enclosed in curly brackets and separated by pipe symbols represent choices. For example: AP-80(config)# logging level {Emergency Alert Critical Error Warning Notice Informational Debug} In this example, the user can choose to set the logging level to any one of the options.
[Optional]	In the command examples, items enclosed in brackets are optional. Do not type the brackets.

Contacting Aruba Networks

Web Site Support	
Main Site	http://www.arubanetworks.com
Support Site	http://www.arubanetworks.com/support
Software Licensing Site	https://licensing.arubanetworks.com
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt
Support Email	support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Telephone Support Numbers	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support <ul style="list-style-type: none"> ● United States ● France ● United Kingdom ● Germany ● All Other Countries 	800-WI-FI-LAN (800-943-4526) +33 (0) 1 70 72 55 59 +44 (0) 20 7127 5989 +49 (0) 69 38 09 77 22 8 +1 (408) 754-1200

About the Aruba AP-80SB and AP-80MB

The Aruba AP-80 MB/SB Outdoor Wireless Access Point/Bridges are dual-radio outdoor-rated wireless access points/Wireless Distribution System (WDS) bridges that are designed for the deployment of advanced IEEE 802.11 wireless services in harsh environments.

As an outdoor wireless access point, the AP-80 MB and AP-80SB can provide IEEE 802.11 wireless service to local wireless clients. The AP-80SB provides 802.11b/g service only, while the AP-80MB can provide 802.11a/b/g services simultaneously.

When deployed for wireless bridging, two or more AP-80 MB/SB models provide point-to-point or point-to-multipoint bridge links between remote Ethernet LANs, and can simultaneously serve wireless service for local clients on the non-bridging radio. The wireless bridge system offers a fast, reliable, and cost-effective solution for connectivity between remote Ethernet LANs or to provide Internet access to an isolated site.

The AP-80SB and AP-80MB are stand-alone devices that operate independent of an Aruba Mobility Controller. They provide the following capabilities:

AP-80SB

- Stand-alone wireless access point (802.11b/g) with support for wireless backhaul over 5 GHz
- Point-to-point WDS bridge for 5 GHz or 2.4 GHz
- Integrated 17dBi 5GHz directional panel antenna (for bridging or wireless backhaul purposes only)
- Two 2.4 GHz N-type female detachable antenna interfaces

AP-80MB

- Stand-alone wireless access point (802.11a/b/g) with support for wireless backhaul over either 5 GHz or 2.4 GHz
- Point-to-point WDS Bridge for either 5 GHz or 2.4 GHz
- Point-to-multipoint WDS Bridge for either 5 GHz or 2.4 GHz
- One 2.4 GHz N-type female detachable antenna interface
- One 5 GHz N-type female detachable antenna interface



NOTE

The AP-80SB and AP-80MB require detachable antennas (see Table 44, “Detachable Antennas,” on page 230).

Package Checklist

- One Aruba AP-80MB or AP-80SB Outdoor Wireless Access Point/Bridge



The Aruba AP-80 MB/SB Outdoor Wireless Access Point/Bridge must be powered over Ethernet using the supplied adapter. The AP-80 MB/SB supports only non-standard 802.3af Power over Ethernet (PoE).

- One pole mount hardware kit
- One Installation Guide (this document), provided on CD
 - One auto-sensing 110/240 VAC to 48 VDC Power over Ethernet (PoE) Injector/Adapter suitable for use with all Aruba AP-80 MB/SB Outdoor Wireless Access Point/Bridges



The adapter is rated for indoor use only and is non-802.3af compliant.

- One 50-meter (164-foot) outdoor Ethernet cable with 8-pin DIN to 10/100Base-T RJ-45 connectors

Inform your supplier if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials, and use them to repack the product in case there is a need to return it.

Recommended Optional Items—Supplied Separately

The following items are optional and are supplied separately:

- One wall mount hardware kit (AP-80-MNT)
- Antenna Interface Lightning Arrester Hardware (Aruba AP-LAR-1; required for warranty): The lightning surge arrester for the AP-80 MB/SB Outdoor Access Point/Bridge is a single, in-line lightning arrester with N-type male to N-type female interface. It supports RF frequency passthrough of 2 GHz – 6 GHz.
- Antenna extension cable is a 3-meter (10-foot), low-loss LMR 400 antenna extension cable (Aruba AP-CBL-1) for use with AP-80 MB/SB Outdoor Access Point/Bridges. It provides an AP-80 MB/SB N-type female interface to N-type male antenna interface.
- Outdoor mounting kit

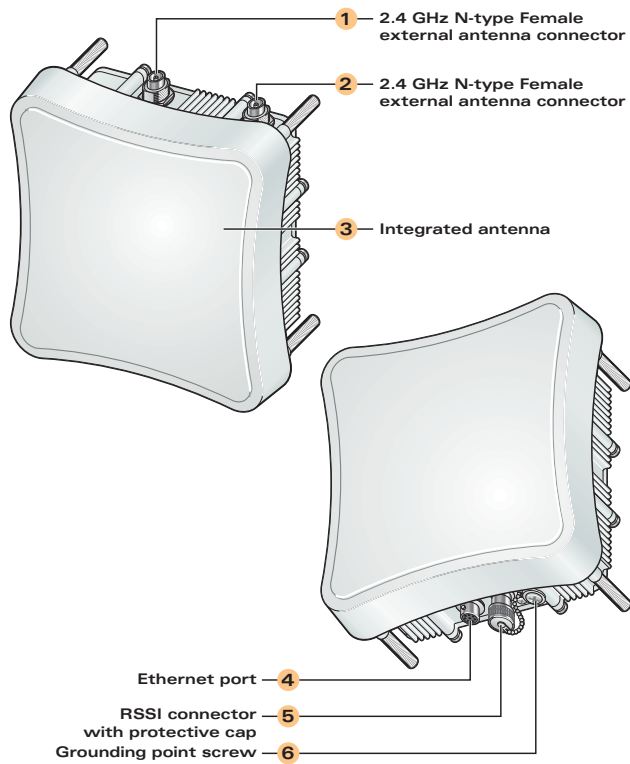
Check with your Aruba sales representative for the availability of optional items.

Hardware Model Overview

AP-80SB

Stand-alone wireless access point (802.11b/g).

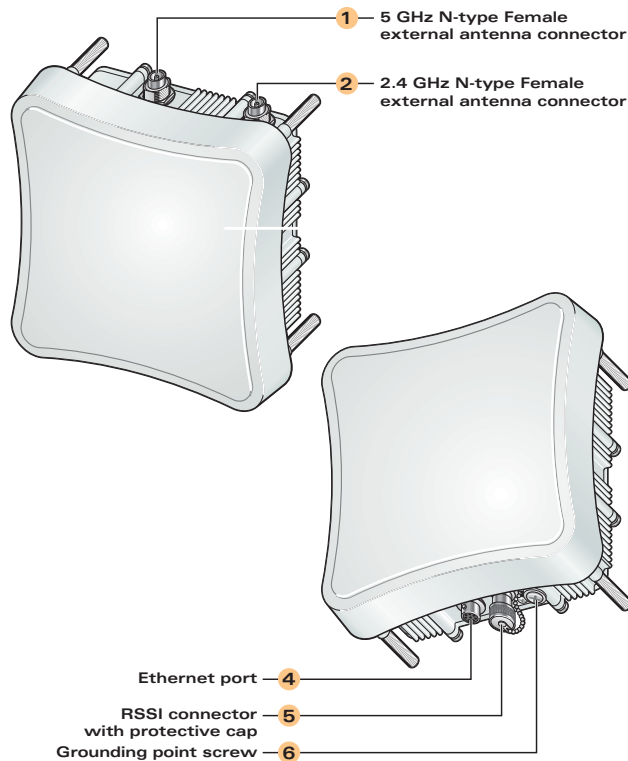
Figure 1 AP-80SB



AP-80MB

Stand-alone wireless access point (802.11a/b/g).

Figure 2 AP-80MB



Ports, Connectors, and Antennas

Table 2 describes the connections on the AP-80 MB/SB.

Table 2 AP-80MB/SB Ports and Connections

Item	Description
1	External Antenna Connector <ul style="list-style-type: none">For AP-80SB: 2.4 GHz, N-Type, Female connectorFor AP-80MB: 5 GHz, N-Type, Female connector
2	External Antenna Connector <ul style="list-style-type: none">For AP-80SB: 2.4 GHz, N-Type, Female connectorFor AP-80MB: 2.4 GHz, N-Type, Female connector
3	Integrated Antenna 5 GHz 17.0 dBi, Flat-panel Directional Antenna (AP-80SB only)
4	FE (Ethernet) Port AP-80SB and AP-80MB models have one 10BASE-T/100BASE-TX 8-pin DIN Ethernet port that connects to the power injector module using the included Ethernet cable. The Ethernet port connection also provides power to the wireless Access Point as well as a data link to the local network. The power injector module does not support Power over Ethernet (PoE) based on the IEEE 802.3af standard. The wireless Access Point unit must always be powered on by being connected to the power injector module. See Appendix B on page 221 for port and cable specifications.

Table 2 AP-80MB/SB Ports and Connections (Continued)

Item	Description
5	<p>RSSI Connector</p> <p>The Receive Signal Strength Indicator (RSSI) BNC connector provides a DC low output voltage that is proportional to the received radio signal strength. A DC voltmeter can be connected to this port to assist in aligning the antennas at both ends of a wireless bridge link.</p>
6	<p>Grounding Screw</p> <p>Even though the AP-80 MB/SB includes its own built-in lightning protection, it is important that the unit is properly connected to ground. A grounding screw is provided for attaching a ground wire to the unit.</p> <p>The AP-80 MB/SB requires lightning protection. Aruba recommends the use of lightning arresters. Failure to provide protection from lightning strikes will void the warranty for this product.</p>

External Antenna Options

- Both AP-80SB and AP-80MB models support a variety of certified, detachable antenna options. When performing wireless bridging, the AP-80SB offers an integrated 5GHz, 17dBi 30 degree beam-width panel antenna for point-point radio link communications.



The AP-80SB and AP-80MB require detachable antennas (see [Table 44, “Detachable Antennas,”](#) on [page 230](#)).

The AP-80SB integrated antenna is primarily designed for WDS bridging applications only and therefore is not ideally suitable for serving wireless clients. The AP-80SB only supports detachable antennas for the 2.4 GHz band.

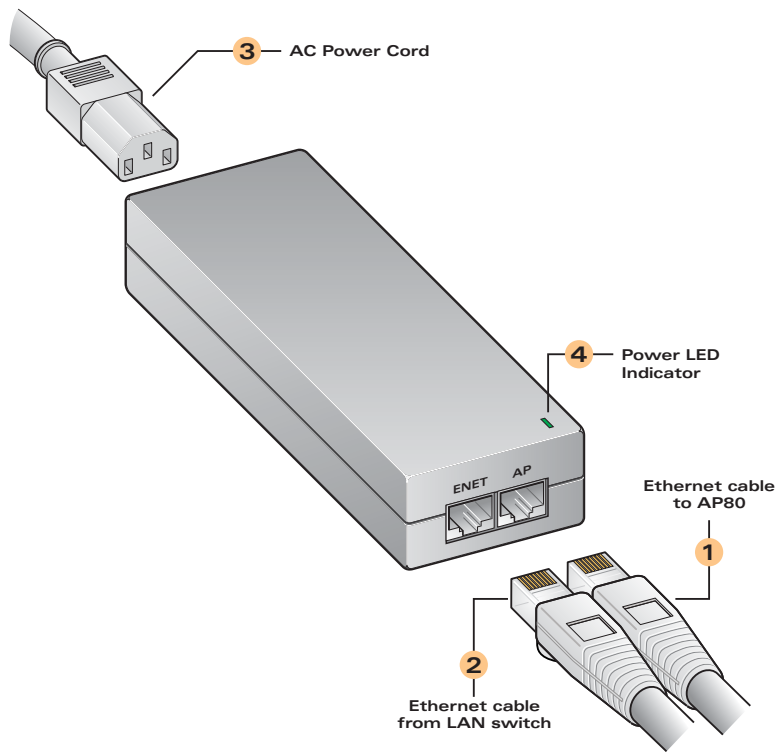
The AP-80MB does not include an integrated antenna, but provides instead one 2.4 GHz and one 5 GHz N-type detachable antenna interface. In a point-to-multipoint configuration, an external high-gain omnidirectional, sector, or high-gain panel antenna can be attached to communicate with wireless bridges spread over a wide area and from differing directions.

The AP-80SB and AP-80MB units both require a suitable 2.4 GHz external antenna for 2.4 GHz wireless client serving operation.

Power over Ethernet Injector/Adapter

All Aruba AP-80 MB/SB models are required to be powered over Ethernet using the supplied power over Ethernet injector/adapter. The power injector provides two RJ-45 Ethernet ports (illustrated below): one for connecting to the AP-80 MB/SB (AP), and one for connecting to a local LAN switch (ENET).

Figure 3 Power over Ethernet Injector/Adaptor



The AP-80 MB/SB does not have a power switch and is powered on when its Ethernet port is connected to the power injector, and the power injector module is connected to an AC power source. The power injector includes one LED indicator that turns on when AC power is applied.

The power injector module automatically adjusts to any AC voltage between 100-240 volts at 50 or 60 Hz. No voltage range settings are required.



The power injector module is designed for indoor use only. Never mount the power injector outside with the AP-80 MB/SB or where it may be exposed to the elements.



The AP-80 MB/SB does NOT support standard 802.3af compliant power, therefore the supplied injector must be used.

The Ethernet port uses an MDI (internal straight-through) pin configuration. You can use a straight-through twisted-pair cable to connect the Ethernet port to most network interconnection devices (such as a switch or router) that provide MDI-X ports.

Installation Overview

The Aruba AP-80 MB/SB Outdoor Wireless Access Point/Bridge is designed to be deployed outdoors, exposed to all elements (extreme heat or sun, rain, snow, ice, cold) and mounted on a wall, pole, or mast. The AP-80 MB/SB is supplied complete with its own mounting hardware kit for attaching the unit to a 1.5" to 2" diameter steel pole or tube or as part of a radio mast or tower structure.

The Aruba AP-80 MB/SB indoor-rated Power over Ethernet injector (model AP-AC-80-1) must be deployed indoors, or within an enclosure protecting it from the elements.

AP-80 MB/SB Setup Process

Setting up an AP-80SB or AP-80MB device consists of the following steps:

1. **WLAN planning:** The network administrator determines how many AP-80 MB/SBs are needed for their wireless network strategy and where they will be deployed, deciding on an appropriate radio band and channel plan to accommodate the deployment needs.

WLAN planning is discussed in more detail in [Chapter 3, "Planning and Deployment Considerations."](#)

2. **AP provisioning:** This is typically performed at a staging facility in a safe location, where the AP-80 MB/SBs are easily accessible by the network administrator and can be verified as fully operational and provided with configuration settings prior to physical installation of the device. AP-80 MB/SB provisioning is discussed in more detail in [Chapter 3, "Planning and Deployment Considerations."](#)



Due to the typically remote, hostile environmental or precariously positioned location of the installed device, Aruba recommends that the AP-80 MB/SB be fully provisioned in advance of physical installation.

3. **AP-80 MB/SB installation:** Once provisioned, each AP-80 MB/SB can be physically installed at its intended place of operation. See ["AP-80MB/SB Installation"](#) on page 17.
4. **Additional AP-80 MB/SB configuration/maintenance:** The administrator may now remotely alter configuration and maintain the AP-80 MB/SB (for example, monitoring the device and updating software versions) via remote Telnet or WebUI. Configuring and maintaining the AP-80 MB/SB is discussed in more detail in [Chapter 5, "Advanced Configuration."](#)

AP-80MB/SB Installation

Hardware installation involves these tasks, as described in this chapter:

1. Mount the unit on a wall, pole, mast, or tower using the mounting bracket.
2. Mount external antennas on the same supporting structure as the bridge and connect them to the bridge unit.
3. Connect the Ethernet cable and a grounding wire to the unit.
4. Connect the power injector to the Ethernet cable, a local LAN switch, and an AC power source.

5. Align antennas at both ends of the link.

Before mounting antennas to set up your wireless bridge links, be sure you have selected appropriate locations for each antenna. Follow the guidance and information in [Chapter 3, “Planning and Deployment Considerations.”](#)

Also before mounting units in their intended locations, you should first configure the devices as described in [Chapter 4, “Provisioning and Initial Setup”](#) and [Chapter 5, “Advanced Configuration.”](#) You should also test the basic operation of the wireless bridge links in a controlled environment over a very short range, as described in [“Staging the Installation” on page 18.](#)



Do not work on the AP-80 MB/SB or connect or disconnect cables during periods of lightning activity.

Preparing for Installation

Before installing your Aruba AP-80 MB/SB Outdoor Wireless Access Point/Bridge, verify that you are supplied and prepared with the following items:

- One Outdoor Ethernet cable of required length of 50 meters (164 feet), or a cable meeting the pin-out configuration specification to the required length (not to exceed 90 meters total), shielded CAT-5 Ethernet 8-pin DIN to RJ-45
- One power adapter shipped with the Aruba AP-80 MB/SB
- An appropriate and stable mounting location
- A suitable electrical grounding point (on mounting mast/pole)
- Appropriate tools (wrench for mounting bolts, phillips head screwdriver, DC voltmeter (if RSSI-based link alignment is to be performed))

Mounting items not supplied with the AP-80MB/SB — screws, bolts, and straps — should be available and at hand prior to installation.

Due to the typically inaccessible location often best suited to deploying an outdoor wireless bridge (for example, on rooftops, sides of buildings, or on a radio tower) it is recommended that the network administrator pre-provision the AP-80 MB/SB system to be installed (taking note of settings, passwords, MAC and IP addresses) prior to physical installation, and confirm that the device is fully operational and free from fault.

Staging the Installation

Set up the units over a very short range (15 to 25 feet), either outdoors or indoors. Connect the units as indicated in this chapter and be sure to perform all the basic configuration tasks outlined in [Chapter 4, “Provisioning and Initial Setup”](#) When you are satisfied that the links are operating correctly, proceed to mount the units in their intended locations.

Mounting the Unit

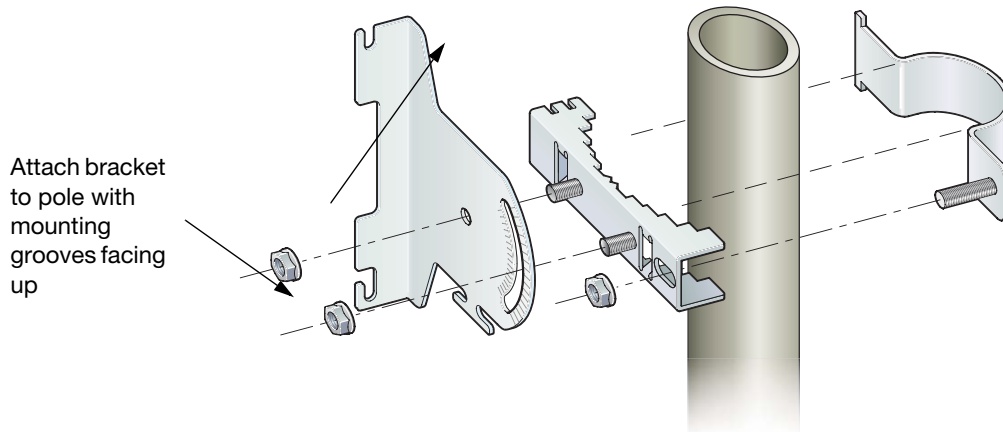
Using the Pole-Mounting Bracket

Perform the following steps to mount the unit to a 1.5 to 2 inch diameter steel pole or tube using the mounting bracket:

1. Always attach the bracket to a pole with the open end of the mounting grooves facing up.

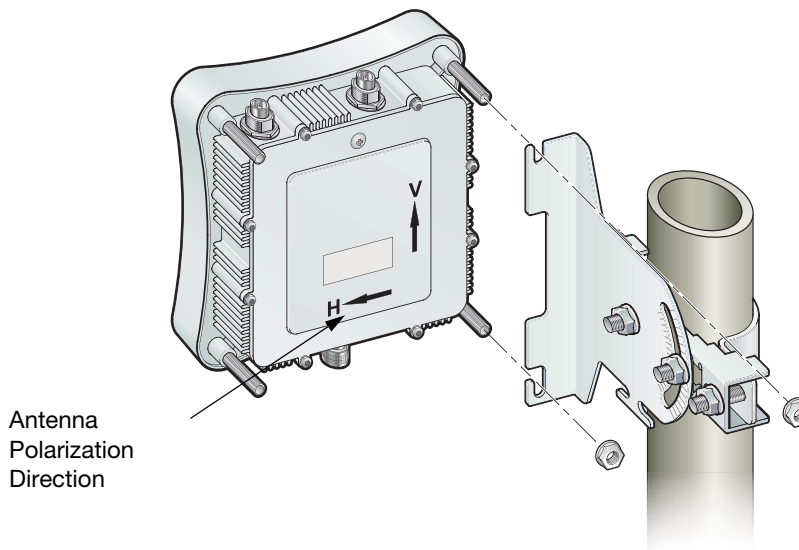
2. Place the U-shaped part of the bracket around the pole and tighten the securing nut just enough to hold the bracket to the pole (Figure 4). (The bracket may need to be rotated around the pole during the alignment process.)

Figure 4 Pole Mounting



3. Use the included nuts to tightly secure the wireless bridge to the bracket. Be sure to take account of the antenna polarization direction; both antennas in a link must be mounted with the same polarization (Figure 5).

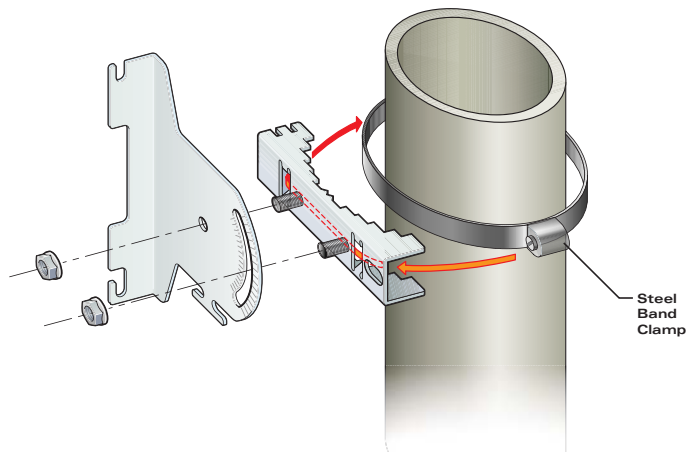
Figure 5 Attaching the AP-80 MB/SB to a Pole.



Mounting on Larger Diameter Poles

There is a method for attaching the pole-mounting bracket to a pole that is 2 to 5 inches in diameter using an adjustable steel band clamp (not included in the kit). A steel band clamp up to 0.5 inch (1.27 cm) wide can be threaded through the main part of the bracket to secure it to a larger diameter pole without using the U-shaped part of the bracket. This method is illustrated (Figure 6).

Figure 6 Mounting on Larger Diameter Poles

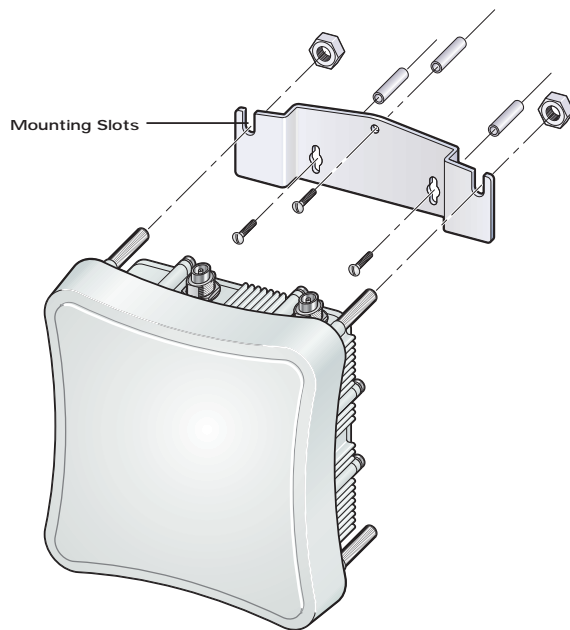


Using the Wall-Mounting Bracket (Optional Part)

The wall-mounting bracket does not allow the wireless bridge's integrated antenna to be aligned. When mounted on the wall, the unit should use an external antenna. Perform the following steps to mount the unit to a wall using the wall-mounting bracket:

1. Always attach the bracket to a wall with the open end of the mounting grooves facing up (Figure 7).

Figure 7 Using the Wall-Mounting Bracket



2. Position the bracket in the intended location and mark the position of the three mounting screw holes.
3. Drill three holes in the wall that match the screws and wall plugs included in the bracket kit, then secure the bracket to the wall.
4. Use the included nuts to tightly secure the wireless bridge to the bracket.

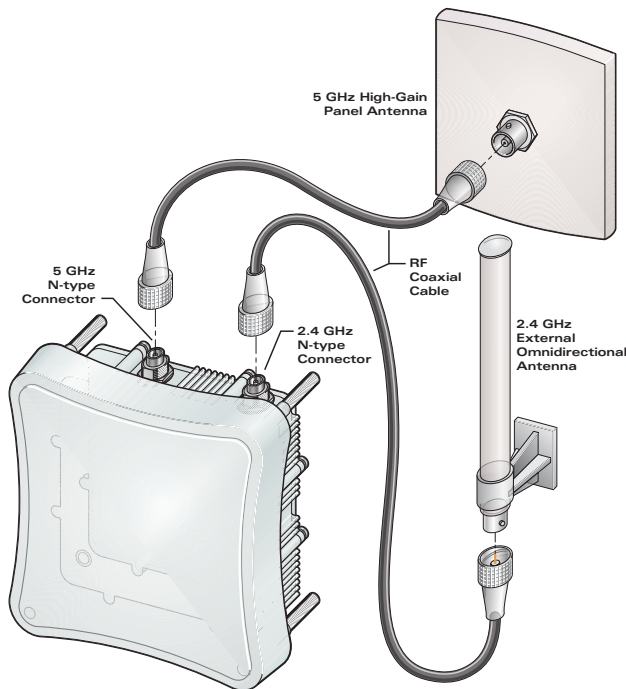
Connect External Antennas

When deploying an AP-80MB Master bridge unit for a bridge link or an access point operation, you need to mount external antennas and connect them to the bridge. Typically, a bridge link requires a 5 GHz antenna, and an access point operation requires a 2.4 GHz antenna. AP-80SB Slave units also require an external antenna for 2.4 GHz operation.

Perform these steps (Figure 8):

1. Mount the external antenna to the same supporting structure as the bridge, within 3 m (10 ft) distance, using the bracket supplied in the antenna package.
2. Connect the antenna to the bridge's N-type connector using the RF coaxial cable provided in the antenna package.
3. Apply weatherproofing tape to the antenna connectors to help prevent water entering the connectors.

Figure 8 Connecting External Antennas



Connect the Ethernet Cable to the Unit

1. Attach the Ethernet cable to the Ethernet port on the wireless bridge (Figure 8).



The Ethernet cable included with the package (AP-AC-80-1, indoor Power Injector) is 50 meters (164 feet) long. Use the connector pinout information in [Appendix B on page 221](#).



The combined cable lengths connecting the store-and-forward Ethernet device, the PoE injector, and the access point must not exceed 90 meters (295 feet).

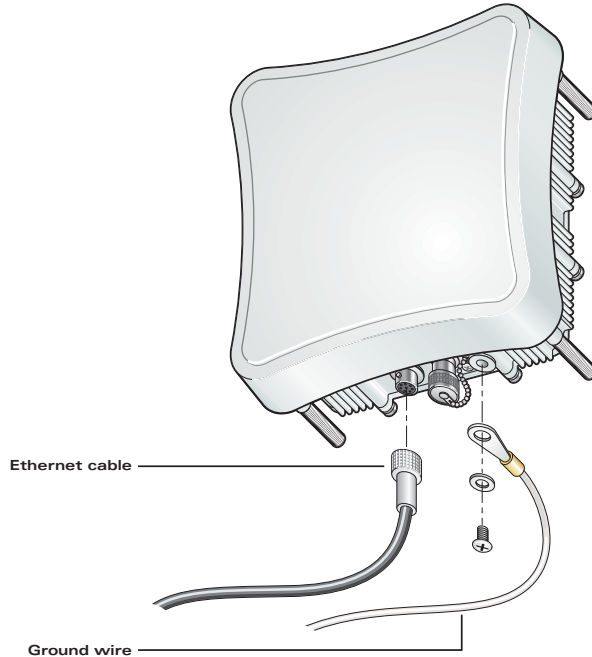
2. For extra protection against rain or moisture, apply weatherproofing tape (not included) around the Ethernet connector.

3. Be sure to ground the unit with an appropriate grounding wire (not included) by attaching it to the grounding screw on the unit.



Be sure that grounding is available and that it meets local and national electrical codes. For additional lightning protection, use lightning rods, lightning arrestors, or surge suppressors.

Figure 9 *Connecting the Ethernet Cable*



Connect the Internal Power Injector Module

To connect the AP-80 MB/SB to a power source:



Do not install the power injector module (AP-AC-80-1) outdoors. The unit is for indoor installation only.



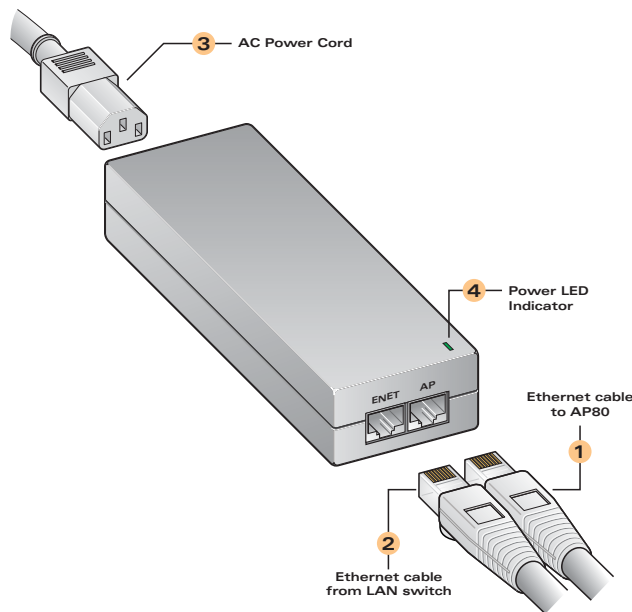
The wireless bridge's Ethernet port does not support Power over Ethernet (PoE) based on the IEEE 802.3af standard. Do not try to power the unit by connecting it directly to a network switch that provides IEEE 802.3af. Always connect the unit to the included power injector module.

1. Connect the Ethernet cable from the wireless bridge to the RJ-45 port labeled “AP” on the power injector.
2. Connect a straight-through unshielded twisted-pair (UTP) cable from a local LAN switch to the RJ-45 port labeled “ENET” on the power injector. Use Category 5 or better UTP cable for 10/100BASE-TX connections.



The RJ-45 port on the power injector is an MDI port. If connecting directly to a computer for testing the link, use a crossover cable.

Figure 10 *Connecting the Power Injector*



3. Insert the power cable plug directly into the standard AC receptacle on the power injector.
4. Plug the other end of the power cable into a grounded, 3-pin socket, AC power source.



For international use, you may need to change the AC line cord. You must use a line cord set that has been approved for the receptacle type in your country.

5. Check the LED on top of the power injector to be sure that power is being supplied to the wireless bridge through the Ethernet connection.

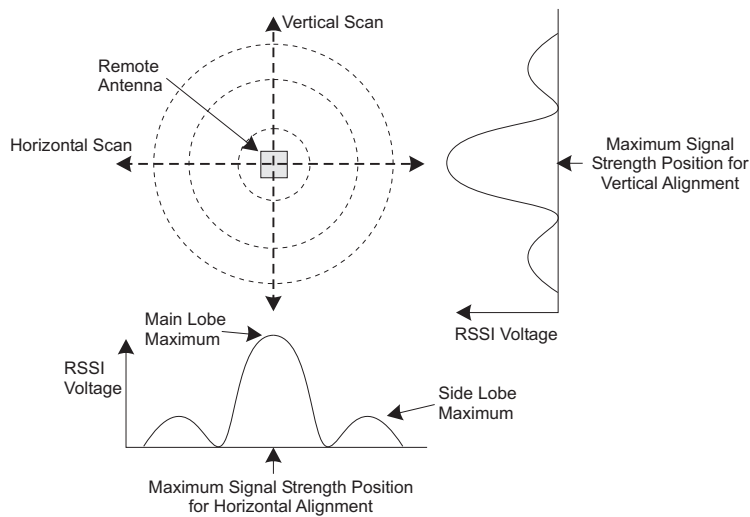
Align Antennas

After wireless bridge units have been mounted, connected, and their radios are operating, the antennas must be accurately aligned to ensure optimum performance on the bridge links. This alignment process is particularly important for long-range point-to-point links. In a point-to-multipoint configuration the Master bridge uses an omnidirectional or sector antenna, which does not require alignment, but Slave bridges still need to be correctly aligned with the Master bridge antenna.

- **Point-to-Point Configurations** – In a point-to-point configuration, the alignment process requires two people at each end of the link. The use of cell phones or two-way radio communication may help with coordination. To start, you can just point the antennas at each other, using binoculars or a compass to set the general direction. For accurate alignment, you must connect a DC voltmeter to the RSSI connector on the wireless bridge and monitor the voltage as the antenna moves horizontally and vertically.
- **Point-to-Multipoint Configurations** – In a point-to-multipoint configuration all Slave bridges must be aligned with the Master bridge antenna. The alignment process is the same as in point-to-point links, but only the Slave end of the link requires the alignment.

The RSSI connector provides an output voltage between 0 and 3.28 VDC that is proportional to the received radio signal strength. The higher the voltage reading, the stronger the signal. The radio signal from the remote antenna can be seen to have a strong central main lobe and smaller side lobes. The object of the alignment process is to set the antenna so that it is receiving the strongest signal from the central main lobe.

Figure 11 *Aligning Antennas*



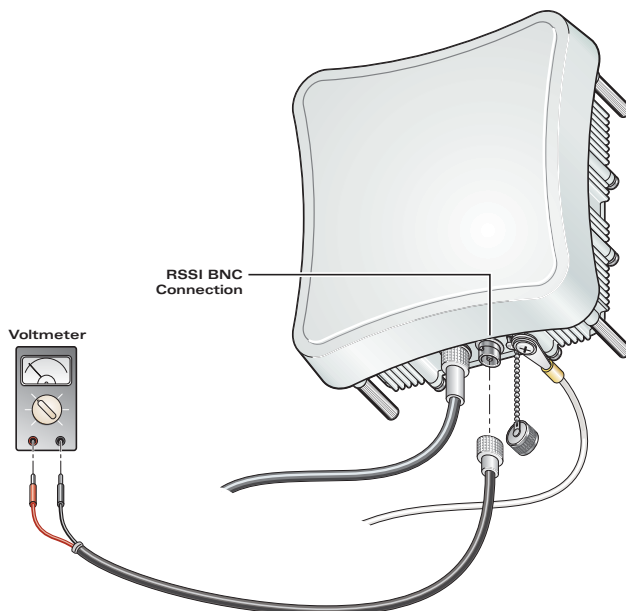
To align the antennas in the link using the RSSI output voltage, start with one antenna fixed and then perform the following procedure on the other antenna:



RSSI output can be configured through management interfaces to output a value for specific WDS ports. See [“RSSI” on page 74](#) for more information.

1. Remove the RSSI connector cover and connect a voltmeter using a cable with a male BNC connector (not included).

Figure 12 *Connecting a Voltmeter*



2. Pan the antenna horizontally back and forth while checking the RSSI voltage. If you are using the pole-mounting bracket with the unit, you must rotate the mounting bracket around the pole. Other external antenna brackets may require a different horizontal adjustment.

3. Find the point where the signal is strongest (highest voltage) and secure the horizontal adjustment in that position.



Sometimes there may not be a central lobe peak in the voltage because vertical alignment is too far off; only two similar peaks for the side lobes are detected. In this case, fix the antenna so that it is halfway between the two peaks.

4. Loosen the vertical adjustment on the mounting bracket and tilt the antenna slowly up and down while checking the RSSI voltage.
5. Find the point where the signal is strongest and secure the vertical adjustment in that position.
6. Remove the voltmeter cable and replace the RSSI connector cover.

Point-to-Point and Multipoint Wireless Links

The AP-80 MB/SB supports fixed point-to-point or point-to-multipoint wireless links. A single link between two points can be used to connect a remote site to a larger core network. Multiple bridge links can provide a way to connect widespread Ethernet LANs. “[Sample Network Topologies](#)” on page 32 describes typical deployment scenarios.

For each link in a wireless bridge network to be reliable and provide optimum performance, some careful site planning is required. This chapter provides guidance and information for planning your wireless bridge links.



The planning and installation of the wireless bridge requires professional personnel who are trained in the installation of radio transmitting equipment. The user is responsible for compliance with local regulations concerning items such as antenna power, use of lightning arrestors, grounding, and radio mast or tower construction. Therefore, it is recommended to consult a professional contractor knowledgeable in local radio regulations prior to equipment installation.

Data Rates

Under ideal deployment conditions (low line of sight, low interference, and low moisture content), the AP-80 MB/SB bridge can operating over a range of up to 15.4 km (9.6 miles) or provide a high-speed connection of 54 Mbps (108 Mbps in turbo mode) using the 5 GHz integrated antenna. The range also depends on the type of antenna used. The maximum data rate for a link decreases as the operating range increases. A 15.4 km link can only operate up to 6 Mbps, whereas a 108 Mbps connection is limited to a range of 1.3 km.

When planning a wireless bridge link, take into account the maximum distance and data rates for the various antenna options. A rate range summary for the 5 GHz (802.11a) antennas using normal and turbo mode is provided in the following tables. For full specifications for each antenna, see “[Aruba 80 Detachable Antennas](#)” on page 230. These values are for ideal conditions.

Table 3 5 GHz Antennas Coverage Distance, Normal Mode

Data Rate	17 dBi Integrated	8 dBi Omni	13.5 dBi 120-degree Sector	16.5 dBi 60-degree Sector	23 dBi Panel
6 Mbps	15.4 km	3.3 km	10.3 km	14 km	24.4 km
9 Mbps	14.7 km	2.9 km	9.2 km	13.4 km	23.3 km
12 Mbps	14 km	2.6 km	8.2 km	12.8 km	22.2 km
18 Mbps	12.8 km	2.1 km	6.5 km	11.7 km	20.3 km
24 Mbps	11.1 km	1.5 km	4.6 km	9.2 km	17.7 km
36 Mbps	6.5 km	0.8 km	2.6 km	5.2 km	14 km

Table 3 5 GHz Antennas Coverage Distance, Normal Mode (Continued)

Data Rate	17 dBi Integrated	8 dBi Omni	13.5 dBi 120-degree Sector	16.5 dBi 60-degree Sector	23 dBi Panel
48 Mbps	2.9 km	0.4 km	1.2 km	2.3 km	9.2 km
54 Mbps	1.8 km	0.2 km	0.7 km	1.5 km	5.8 km

Distances provided in this table are an estimate for a typical deployment and may be reduced by local regulatory limits. For accurate distances, you need to calculate the power link budget for your specific environment.

Table 4 5 GHz Antennas Coverage Distance, Turbo Mode

Data Rate	17 dBi Integrated	8 dBi Omni	13.5 dBi 120-Degree Sector	16.5 dBi 60-Degree Sector	23 dBi Panel
12 Mbps	13.4 km	2.3 km	7.3 km	12.2 km	21.2 km
18 Mbps	12.8 km	2.1 km	6.5 km	11.7 km	20.3 km
24 Mbps	12.2 km	1.8 km	5.8 km	11.1 km	19.4 km
36 Mbps	11.1 km	1.5 km	4.6 km	9.2 km	17.7 km
48 Mbps	8.2 km	1 km	3.3 km	6.5 km	15.4 km
72 Mbps	4.6 km	0.6 km	1.8 km	3.7 km	12.2 km
96 Mbps	2.1 km	0.3 km	0.8 km	1.6 km	6.5 km
108 Mbps	1.3 km	0.2 km	0.5 km	1 km	4.1 km

Distances provided in this table are an estimate for a typical deployment and may be reduced by local regulatory limits. For accurate distances, you need to calculate the power link budget for your specific environment.

For information about radio sensitivities, see [“Radio Characteristics”](#) on page 223.

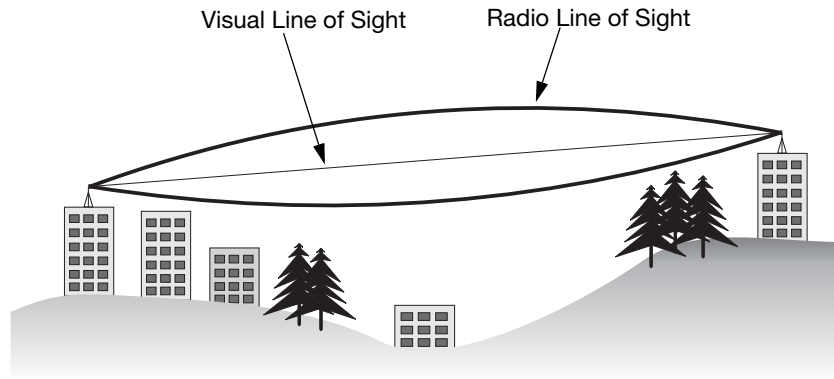
Radio Path Planning

The wireless bridge link requires a “radio line of sight” between the two antennas for optimum performance.

The concept of radio line of sight involves the area along a link through which the bulk of the radio signal power travels. This area is known as the first Fresnel Zone of the radio link. For a radio link, no object (including the ground) must intrude within 60% of the first Fresnel Zone.

[Figure 13](#) illustrates the concept of a good radio line of sight.

Figure 13 *Radio Line of Sight*



If there are obstacles in the radio path, there may still be a radio link but the quality and strength of the signal will be affected. Calculating the maximum clearance from objects on a path is important as it directly affects the decision on antenna placement and height. It is especially critical for long-distance links, where the radio signal could easily be lost.



For wireless links less than 500 m, the IEEE 802.11a radio signal will tolerate some obstacles in the path and may not even require a visual line of sight between the antennas.

When planning the radio path for a wireless bridge link, consider these factors:

- Avoid any partial line of sight between the antennas.
- Be cautious of trees or other foliage that may be near the path, or may grow and obstruct the path.
- Be sure there is enough clearance from buildings and that no building construction may eventually block the path.
- Check the topology of the land between the antennas using topographical maps, aerial photos, or even satellite image data (software packages are available that may include this information for your area).
- Avoid a path that may incur temporary blockage due to the movement of cars, trains, or aircraft.

Antenna Height

A reliable wireless link is usually best achieved by mounting the antennas at each end high enough for a clear radio line of sight between them. The minimum height required depends on the distance of the link, obstacles that may be in the path, topology of the terrain, and the curvature of the earth (for links over 3 miles).

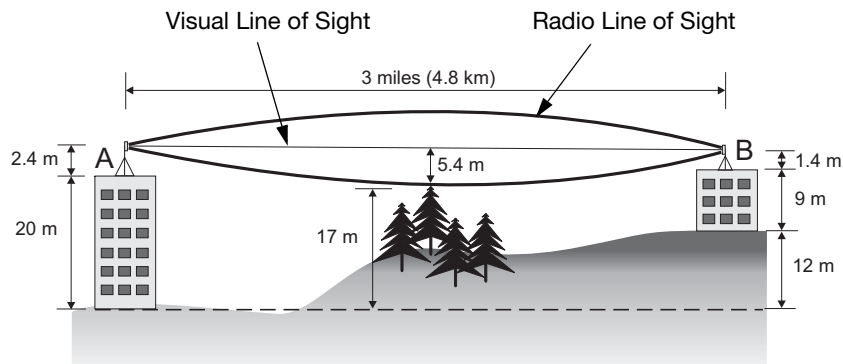
For long-distance links, the access point may have to be mounted on masts or poles that are tall enough to attain the minimum required clearance. Use the following table to estimate the required minimum clearance above the ground or path obstruction (for 5 GHz bridge links).

Table 5 Antenna Minimum Height and Clearance Requirements

Total Link Distance	Max Clearance for 60% of First Fresnel Zone at 5.8 GHz	Approximate Clearance for Earth Curvature	Total Clearance Required at Mid-point of Link
0.25 mile (402 m)	4.5 ft (1.4 m)	0	4.5 ft (1.4 m)
0.5 mile (805 m)	6.4 ft (1.95 m)	0	6.4 ft (1.95 m)
1 mile (1.6 km)	9 ft (2.7 m)	0	9 ft (2.7 m)
2 miles (3.2 km)	12.7 ft (3.9 m)	0	12.7 ft (3.9 m)
3 miles (4.8 km)	15.6 ft (4.8 m)	1.8 ft (0.5 m)	17.4 ft (5.3 m)
4 miles (6.4 km)	18 ft (5.5 m)	3.2 ft (1.0 m)	21.2 ft (6.5 m)
5 miles (8 km)	20 ft (6.1 m)	5 ft (1.5 m)	25 ft (7.6 m)
7 miles (11.3 km)	24 ft (7.3 m)	9.8 ft (3.0 m)	33.8 ft (10.3 m)
9 miles (14.5 km)	27 ft (8.2 m)	16 ft (4.9 m)	43 ft (13.1 m)
12 miles (19.3 km)	31 ft (9.5 m)	29 ft (8.8 m)	60 ft (18.3 m)
15 miles (24.1 km)	35 ft (10.7 m)	45 ft (13.7 m)	80 ft (24.4 m)

Note that to avoid any obstruction along the path, the height of the object must be added to the minimum clearance required for a clear radio line of sight. Consider the following simple example, illustrated in Figure 14.

Figure 14 Visual and Radio Line of Sight



A wireless bridge link is deployed to connect building A to building B, which is located three miles (4.8 km) away. Mid-way between the two buildings is a small tree-covered hill. From the above table it can be seen that for a three-mile link, the object clearance required at the mid-point is 5.3 m (17.4 ft). The tree tops on the hill are at an elevation of 17 m (56 ft), so the antennas at each end of the link need to be at least 22.3 m (73 ft) high. Building A is six stories high, or 20 m (66 ft), so a 2.3 m (7.5 ft) mast or pole must be constructed on its roof to achieve the required antenna height. Building B is only three stories high, or 9 m (30 ft), but is located at an elevation that is 12 m (39 ft) higher than building A. To mount an antenna at the required height on building B, a mast or pole of 1.3 m (4.3 ft) is needed.



CAUTION

Never construct a radio mast, pole, or tower near overhead power lines.



Local regulations may limit or prevent construction of a high radio mast or tower. If your wireless bridge link requires a high radio mast or tower, consult a professional contractor for advice.

Antenna Position and Orientation

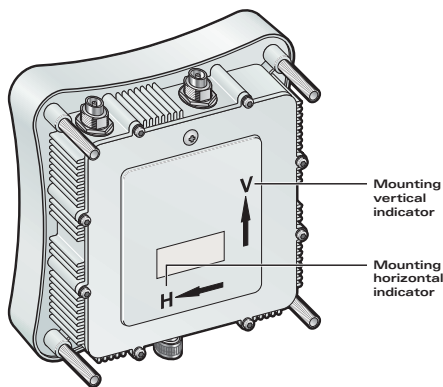
Once the required antenna height has been determined, other factors affecting the precise position of the wireless bridge must be considered:

- Be sure there are no other radio antennas within 2 m (6 ft) of the wireless bridge. These include other WiFi radio antennas.
- Place the wireless bridge away from power and telephone lines.
- Avoid placing the wireless bridge too close to any metallic reflective surfaces, such as roof-installed air-conditioning equipment, tinted windows, wire fences, or water pipes. Ensure that there is at least 5 feet clearance from such objects.
- The wireless bridge antennas at both ends of the link must be positioned with the same polarization direction, either horizontal or vertical. Proper alignment helps to maximize throughput.

Antenna Polarization

The wireless bridge's integrated antenna sends a radio signal that is polarized in a particular direction. The antenna's receive sensitivity is also higher for radio signals that have the same polarization. To maximize the performance of the wireless link, both antennas must be set to the same polarization direction. The antenna polarization is marked on the wireless bridge, as indicated in [Figure 15](#).

Figure 15 *Antenna Polarization*



Radio Interference

The avoidance of radio interference is an important part of wireless link planning. Interference is caused by other radio transmissions using the same or an adjacent channel frequency. You should first scan your proposed site using a spectrum analyzer to determine if there are any strong radio signals using the 802.11a channel frequencies. Always use a channel frequency that is furthest away from another signal.

If radio interference is still a problem with your wireless bridge link, changing the antenna polarization direction may improve the situation.

Weather Conditions

When planning wireless bridge links, you must take into account any extreme weather conditions that are known to affect your location. Consider these factors:

- **Temperature** — The wireless bridge is tested for normal operation in temperatures from -33°C to 55°C. Operating in temperatures outside of this range may cause the unit to fail.
- **Wind Velocity** — The wireless bridge can operate in winds up to 90 miles per hour and survive higher wind speeds up to 125 miles per hour. You must consider the known maximum wind velocity and direction at the site and be sure that any supporting structure, such as a pole, mast, or tower, is built to withstand this force.
- **Lightning** — The wireless bridge includes its own built-in lightning protection. However, you should make sure that the unit, any supporting structure, and cables are all properly grounded. Additional protection using lightning rods, lightning arrestors, or surge suppressors may also be employed.
- **Rain** — The wireless bridge is weatherproofed against rain. Also, prolonged heavy rain has no significant effect on the radio signal. However, it is recommended to apply weatherproof sealing tape around the Ethernet port and antenna connectors for extra protection. If moisture enters a connector, it may cause a degradation in performance or even a complete failure of the link.
- **Snow and Ice** — Falling snow, like rain, has no significant effect on the radio signal. However, a buildup of snow or ice on antennas may cause the link to fail. In this case, the snow or ice has to be cleared from the antennas to restore operation of the link.

Ethernet Cabling and Grounding

When a suitable antenna location has been determined, you must plan a cable route from the wireless bridge outdoors to the power injector/adaptor module indoors. (The power injector/adaptor is for indoor installation only.) Consider these points:

- The Ethernet cable length should never be longer than 90 m (295 ft).
- Determine a building entry point for the cable.
- Determine if conduits, bracing, or other structures are required for safety or protection of the cable.
- For lightning protection at the power injector end of the cable, consider using a lightning arrestor immediately before the cable enters the building.

Grounding

It is important that the wireless bridge, cables, and any supporting structures are properly grounded. The wireless bridge unit includes a grounding screw for attaching a ground wire. Be sure that grounding is available and that it meets local and national electrical codes.

Sample Network Topologies

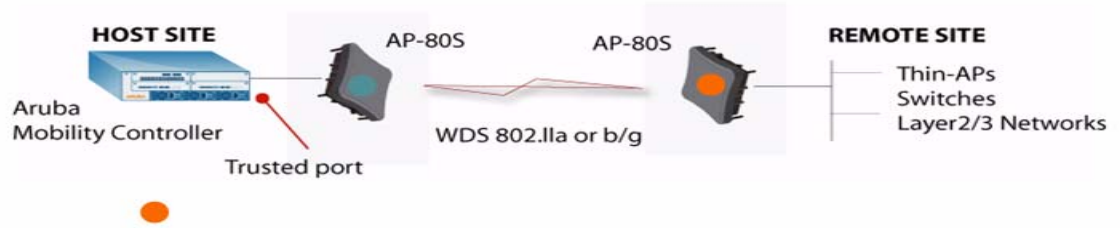
The wireless bridge units can be used as normal 802.11a/b/g access points connected to a local wired LAN, providing connectivity and roaming services for wireless clients in an outdoor area. Units can also be used purely as bridges to connect remote LANs. Alternatively, you can employ both access point and bridging functions together, offering a flexible and convenient wireless solution for many applications.

This section describes sample topologies for the AP-80SB/MB.

Point-Point WDS Bridge

This topology provides a wireless bridge between an Aruba mobility controller and a remote wired network. The AP-80 MB/SB is not integrated with Aruba equipment or managed by an Aruba switch.

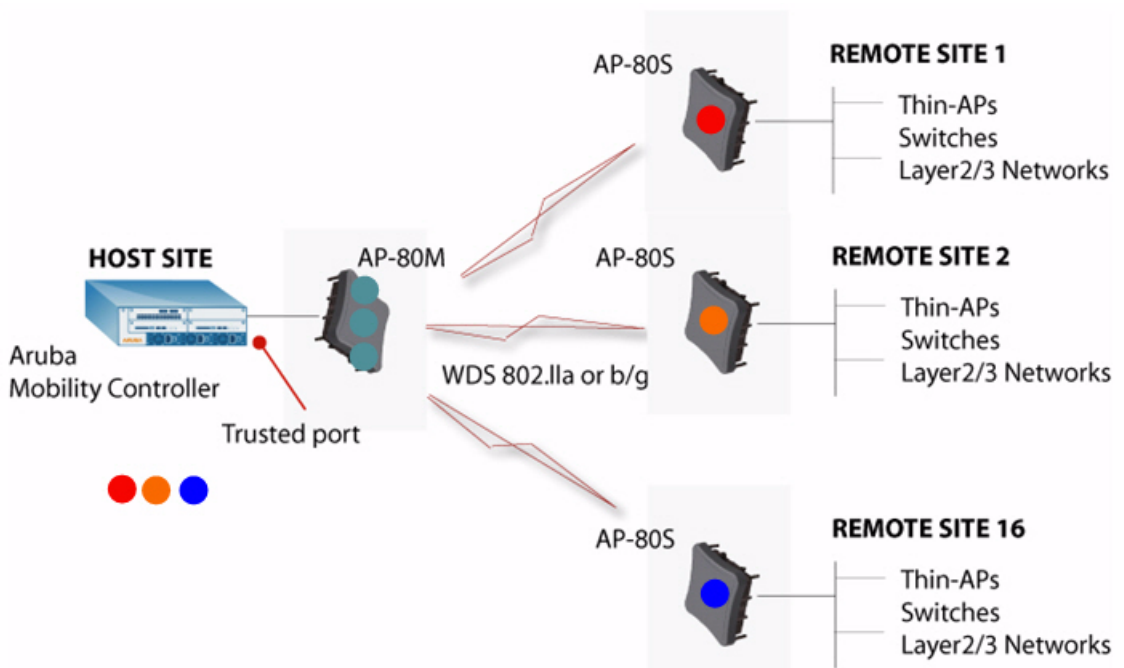
Figure 16 *Point-Point WDS Bridge Topology*



Point-Multipoint WDS Bridge

This topology provides a wireless bridge between an Aruba mobility controller and multiple remote wired networks. The AP-80 MB/SB is not integrated with Aruba equipment or managed by an Aruba switch.

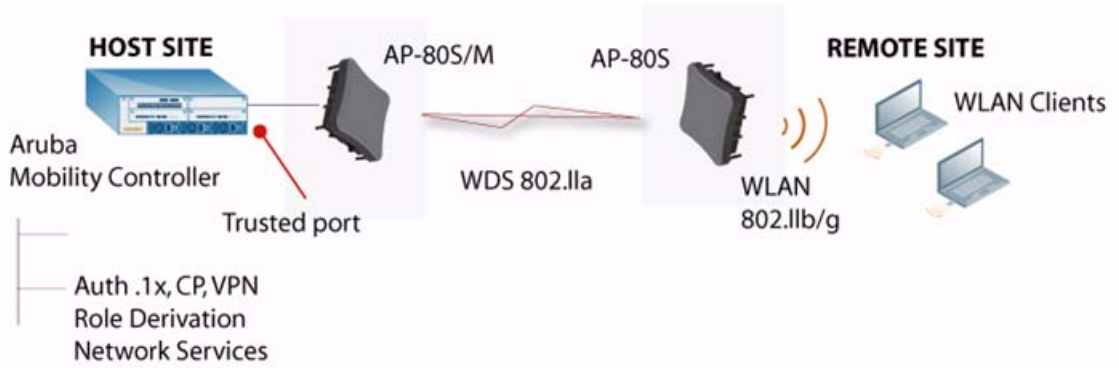
Figure 17 *Point-Multipoint WDS Bridge Topology*



Fat Access Point with Wireless Backhaul

In this topology, the AP-80 MB/SB serves as a Fat access point or WDS bridge to provide wireless backhaul for a remote site. In this stand-alone configuration, the AP-80 MB/SB provides authentication services between the two wired networks. The AP-80 MB/SB is not integrated with Aruba equipment or managed by an Aruba switch.

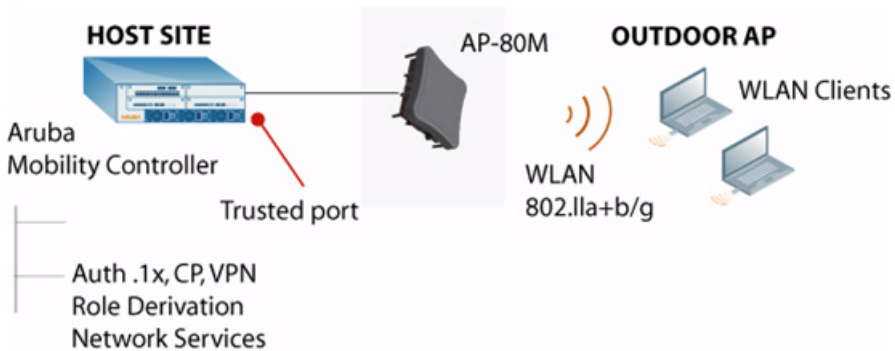
Figure 18 *Fat Access Point with Wireless Backhaul*



Fat Access Point with Wired Backhaul

In this topology, the AP-80 MB/SB serves as a fat access point or WDS bridge to provide wireless backhaul for a remote site. In this stand-alone configuration, the AP-80 MB/SB provides authentication services between the two wired networks. The AP-80 MB/SB is not integrated with Aruba equipment or managed by an Aruba switch

Figure 19 *Fat Access Point with Wired Backhaul*



Management Interfaces

The AP-80 MB/SB Outdoor Wireless Access Point/Bridge offers the following management options:

- Web-based interface
- Command line interface (CLI) using a Telnet session
- SNMP management software

You can perform most initial configuration of the AP-80 MB/SB through the web browser interface using the Setup Wizard (page 38). However, you must first set the country code using the CLI through a Telnet connection to the device, as described in “Connecting to the AP-80 MB/SB for the First Time” on page 38.



The AP-80SB and AP-80MB systems are not configured with a specific country code. You must use the CLI to set the country code and enable wireless operation (see “country” on page 113).

The AP-80 MB/SB uses a static, default IP address 192.168.1.1. You must perform initial configuration using a workstation that has IP settings for this subnet (for example, set the IP address of the PC to 192.168.1.2) and connect it directly to the Ethernet port on the AP-80 MB/SB. When the initial configuration is completed, you can set a different IP address for the device before connecting it to your network. You can alternatively configure the device to request its IP address from a DHCP server on your network.

Factory Default Configuration

The Aruba AP-80MB/SB Outdoor Wireless Access Point / Bridge devices are pre-configured at the time of manufacture with the following system defaults.

Table 6 AP-80MB/SB System Defaults

Feature	Parameter	Default
Identification	System Name	Dual Band Outdoor AP
Administration	User Name	admin
	Password	null
General	HTTP Server	Enabled
	HTTP Server Port	80
Radio	ISO Country Regulating Domain Setting	US for units sold in the United States; 99 (no country set) for units sold in other countries—you must use the CLI to set the country setting (see Chapter 6, “CLI Commands” for details)

Table 6 AP-80MB/SB System Defaults (Continued)

Feature	Parameter	Default
TCP/IP	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	Primary DNS IP	0.0.0.0
	Secondary DNS IP	0.0.0.0
VLANs	Status	Disabled
	Native VLAN ID	1
Filter Control	Ethernet Type	Disabled
SNMP	Status	Enabled
	Location	null
	Contact	Contact
	Community (Read Only)	Public
	Community (Read/Write)	Private
	Traps	Enabled
	Trap Destination IP Address	null
	Trap Destination Community Name	Public
System Logging	Syslog	Disabled
	Logging Host	Disabled
	Logging Console	Disabled
	IP Address / Host Name	0.0.0.0
	Logging Level	Informational
	Logging Facility Type	16
Spanning Tree	Status	Enabled
Ethernet Interface	Speed and Duplex	Auto
WDS Bridging	Outdoor Bridge Band	Disabled

Table 6 AP-80MB/SB System Defaults (Continued)

Feature	Parameter	Default
Wireless Interface 802.11a	Status	Disabled
	SSID	DualBandOutdoor
	Turbo Mode	Disabled
	Radio Channel	Default to first channel
	Auto Channel Select	Enabled
	Transmit Power	Full
	Maximum Data Rate	54 Mbps
	Beacon Interval	100 TUs
	Data Beacon Rate (DTIM Interval)	2 beacons
	RTS Threshold	2347 bytes
Wireless Security 802.11a	Authentication Type	Open System
	AES Encryption	Disabled
	WEP Encryption	Disabled
	WEP Key Length	128 bits
	WEP Key Type	Hexadecimal
	WEP Transmit Key Number	1
Wireless Interface 802.11b/g	Status	Disabled
	SSID	DualBandOutdoor
	Radio Channel	Default to first channel
	Auto Channel Select	Enabled
	Transmit Power	Full
	Maximum Data Rate	54 Mbps
	Beacon Interval	100 TUs
	Data Beacon Rate (DTIM Interval)	2 beacons
	RTS Threshold	2347 bytes
Wireless Security 802.11b/g	Authentication Type	Open System
	AES Encryption	Disabled
	WEP Encryption	Disabled
	WEP Key Length	128 bits
	WEP Key Type	Hexadecimal
	WEP Transmit Key Number	1
	WEP Keys	null
	WEP Keys	null

Connecting to the AP-80 MB/SB for the First Time

When you connect to the AP-80 MB/SB for the first time, access the CLI through a Telnet connection so that you can set the country code. Once you set the country code, you can configure the device using the Setup Wizard in the web-based interface or the CLI.

You can open a Telnet session by performing these steps:

1. Configure your workstation to be on the 192.168.1.1 subnetwork. Refer to your workstation documentation for instructions on how to do this.
2. From your workstation, enter the Telnet command and the default IP address of the AP-80 MB/SB unit (for example, enter `telnet 192.168.1.1`).
3. At the prompt, enter `admin` for the user name.
4. The default password is null, so just press [Enter] at the password prompt.

The CLI displays the Aruba Networks AP-80MB# or Aruba Networks AP-80SB# prompt to show that you are using executive access mode.

```
Username: admin
Password:
Aruba Networks AP-80MB#
```

Regulations for wireless products differ from country to country. Setting the country code restricts the AP-80 MB/SB to only use the radio channels and power settings permitted in the specified country of operation.



If you need to change the country code after it has been set, you must set the AP-80 MB/SB to its factory default configuration before you can set a different country code. See [“Resetting the AP” on page 66](#).

At the Exec prompt, type `country ?` to display the list of country codes. Check the code for your country, then enter the `country` command again followed by your country code (for example, enter `ie` for Ireland).

```
Aruba Networks AP-80MB#country ie
Aruba Networks AP-80MB#
```

Once you have set the country code on the AP-80 MB/SB, you can configure the device using either the Setup Wizard in the web-based interface (described in the following section) or the CLI.

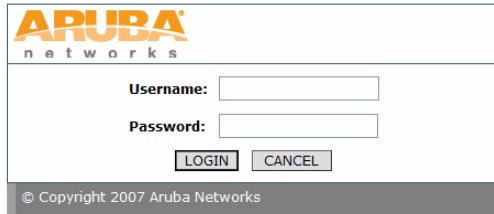
For a full description of how to use the CLI, see [“Using the Command Line Interface” on page 103](#). For a list of all the CLI commands and detailed information on using the CLI, refer to [“Command Groups” on page 107](#).

Using the Web-Based Management Setup Wizard

There are only a few basic steps you need to complete to set up the AP-80 MB/SB for your network. The Setup Wizard takes you through configuration procedures for the radio channel selection, IP configuration, and basic WEP encryption for wireless security.

The AP-80 MB/SB can be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above). Enter the IP configured for the unit or the default IP address: `http://192.168.1.1`.

Logging In – Enter the default username **admin** and click LOGIN (there is no default password). For information on configuring a user name and password, refer to “[Changing the Password](#)” on page 65.

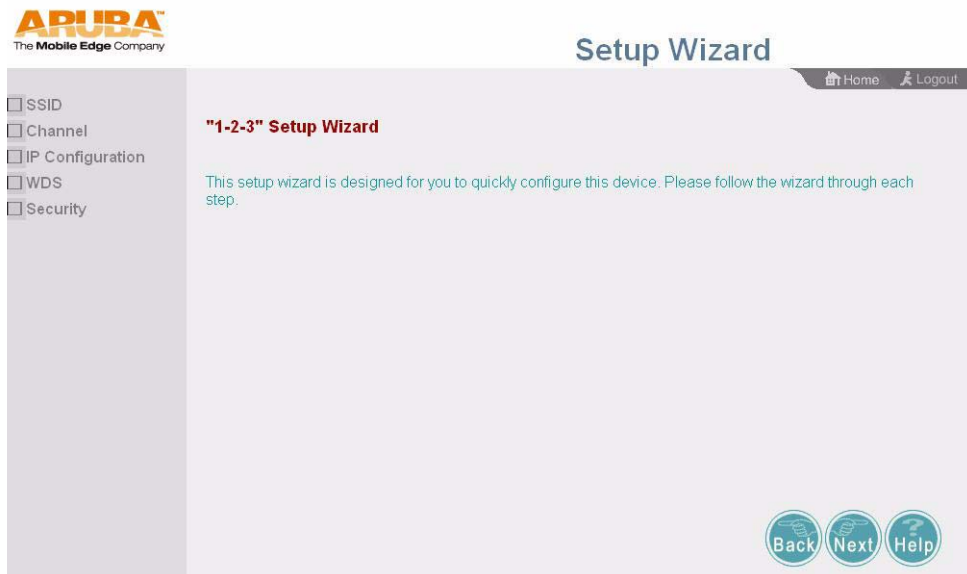


The image shows the Aruba Networks login interface. At the top left is the Aruba Networks logo. Below it, there are two input fields: "Username:" and "Password:". To the right of the "Password:" field is a "LOGIN" button and a "CANCEL" button. At the bottom of the form, there is a copyright notice: "© Copyright 2007 Aruba Networks".

The home page displays the Main Menu:

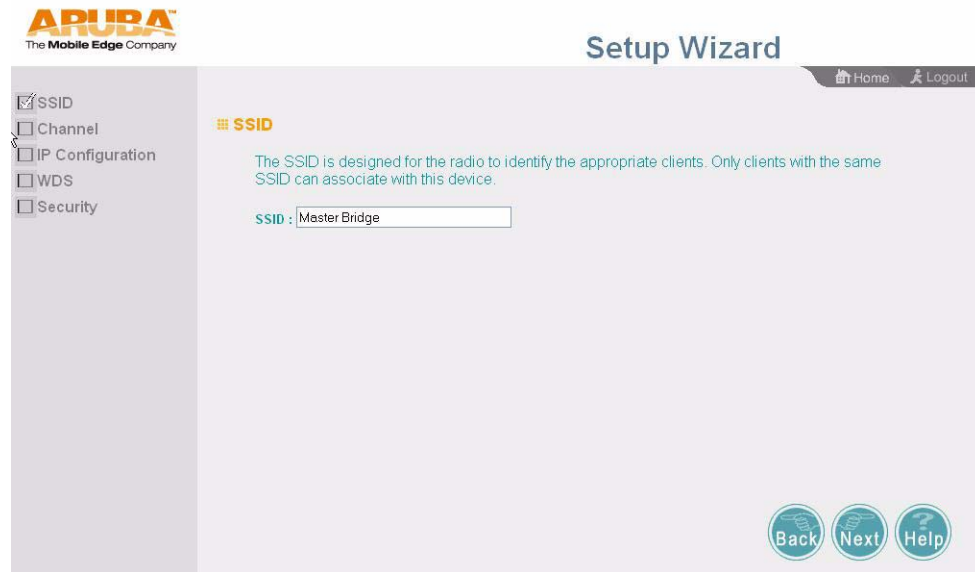


Launching the Setup Wizard – To perform initial configuration, click Setup Wizard on the home page, then click on the [Next] button to start the process.

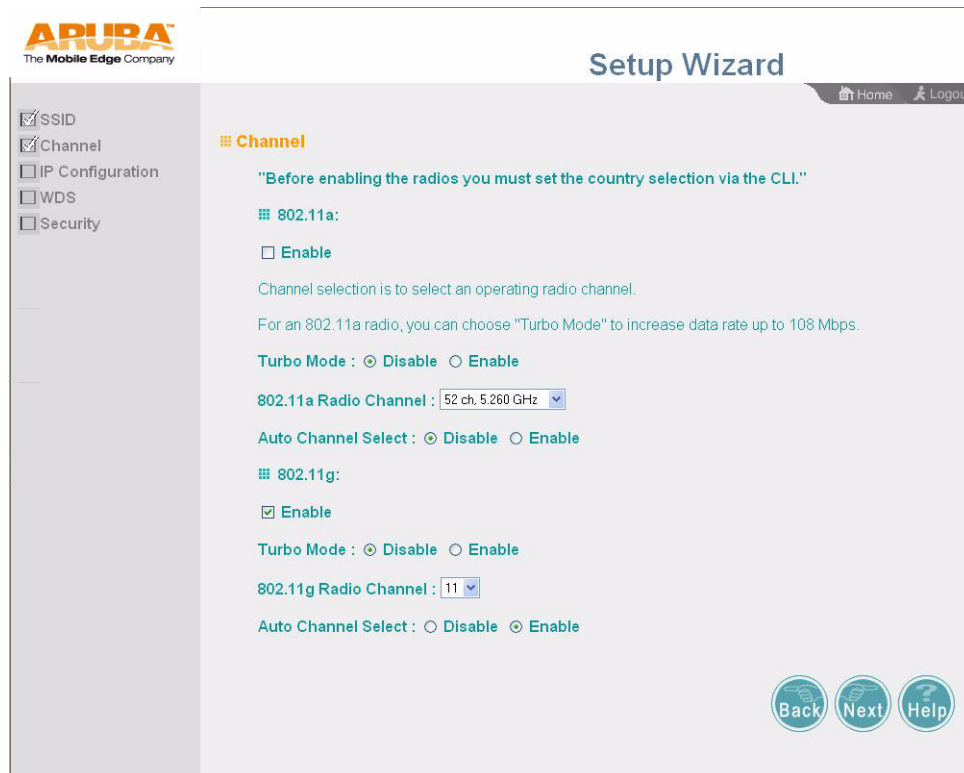


1. **Service Set Identification** – Enter the service set identification (SSID). All wireless 802.11g clients must use the SSID to associate with the access point. The SSID is case sensitive and can

consist of up to 32 alphanumeric characters. The default is DualBandOutdoor.



2. **Radio Channel** – You must enable radio communications for the 802.11a and 802.11g radios and set the operating channel.



- 802.11a
 - *Turbo Mode* – If you select **Enable**, the AP-80 MB/SB will operate in turbo mode with a data rate of up to 108 Mbps. Normal mode supports 13 channels, Turbo mode supports only 5 channels. (Default: Disable)
 - *802.11a Radio Channel* – Set the operating radio channel number. (Default: 56ch, 5.280 GHz)

- *Auto Channel Select* – Choose **Enable** to automatically select an unoccupied radio channel. (Default: Enable)
- 802.11b/g
 - *802.11g Radio Channel*: Set the operating radio channel number. (Range 1-11; Default: 1)



Available channel settings are limited by local regulations which determine which channels are available.

3. **IP Configuration** – Either enable or disable Dynamic Host Configuration Protocol (DHCP) for automatic IP configuration. If you disable DHCP, then manually enter the IP address and subnet mask. If a management station exists on another network segment, then you must enter the IP address for a gateway that can route traffic between these segments. Then enter the IP address for the primary and secondary Domain Name Servers (DNS) servers to be used for hostname-to-IP address resolution.



4. *DHCP Client* – With DHCP Client enabled, the IP address, subnet mask and default gateway can be dynamically assigned to the AP-80 MB/SB by the network DHCP server. This is enabled by default.

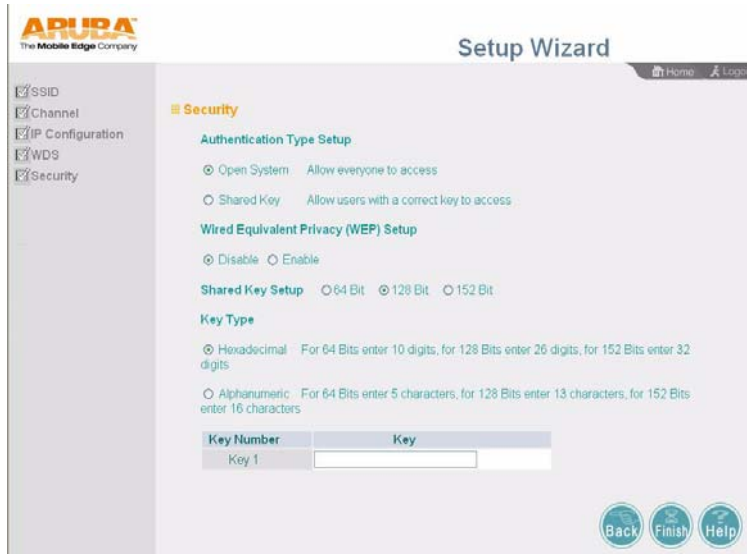


If there is no DHCP server on your network, the AP-80 MB/SB automatically starts up with its default IP address, 192.168.1.1.

5. **WDS** – Enable or disable your Wireless Distribution System (WDS) configuration Master mode settings. To enable a connection with a Slave device, provide the MAC address of the Slave in the appropriate port field. Set your WDS data rate speed and select either Normal or Turbo (aggregate all Master radio channels into one channel) mode, and enter the distance (in kilometers) between the Slave and Master devices.



6. **Security (802.11g)** – Set the Authentication Type to Open System to allow open access without authentication, or Shared Key to require authentication based on a shared key. Enable Wired Equivalent Privacy (WEP) to encrypt data transmissions. To configure other security features use the Advanced Setup menu as described in [Chapter 5, “Advanced Configuration.”](#)



Authentication Type – Select Open System to allow open access to all wireless clients without performing authentication, or Shared Key to perform authentication based on a shared key that has been distributed to all stations. By default, Open System is selected.

WEP – Wired Equivalent Privacy is used to encrypt transmissions passing between wireless clients and the access point. This is disabled by default.

Shared Key Setup – If you selected Shared Key authentication type or enabled WEP, then you also need to configure the shared key by selecting 64-bit or 128-bit key type, and entering a hexadecimal or ASCII string of the appropriate length. The key can be entered as alphanumeric characters or hexadecimal (0~9, A~F, e.g., D7 0A 9C 7F E5). By default, 128-bit, hexadecimal key type is selected.

64-Bit Manual Entry: The key can contain 10 hexadecimal digits, or 5 alphanumeric characters.

128-Bit Manual Entry: The key can contain 26 hexadecimal digits or 13 alphanumeric characters.



All wireless devices must be configured with the same key values to communicate with the AP-80 MB/SB device.

7. Click Finish.
8. Click the OK button to restart the AP-80 MB/SB.



You can manage the AP-80 MB/SB using a web browser (Internet Explorer 5.0 or later, or Netscape Navigator 6.2 or later).



Before continuing with advanced configuration, first complete the initial configuration steps described in [Chapter 4, “Provisioning and Initial Setup”](#) to set up an IP address for the AP-80 MB/SB.

Follow these steps to log into the AP-80 MB/SB WebUI.

1. Enter the IP address configured for the unit or the default IP address: `http://192.168.1.1`.
2. Enter the default user name **admin** and click **LOGIN** (there is no default password).

The WebUI opens to display the Identification page.

Each WebUI page contains the following buttons:

- **Apply**—Save and implement the changes. After clicking **Apply**, click **OK** to confirm.
- **Cancel**—Reset the entries on the page to the previously applied values.
- **Help**—Display online help for the page.
- **Logout**—Log out of the WebUI and displays the login page.



Before continuing with advanced configuration, it is recommended that you configure a user name and password, as described in [“Administration” on page 64](#).

The information in this chapter is organized to reflect the structure of the web screens for easy reference (Table 7).

Table 7 *Advanced Configuration Page Options*

Menu	Description	Section and Page
Identification	Specifies the system name, location and contact information	“System Identification” on page 47
TCP / IP Settings	Configures the IP address, subnet mask, gateway, and domain name servers	“TCP / IP Settings” on page 48
RADIUS	Configures the RADIUS server for wireless client authentication	“RADIUS” on page 51
Authentication	Configures 802.1X client authentication and MAC address authentication	“Authentication” on page 54
Filter Control	Enables VLAN support and filters traffic matching specific Ethernet protocol types	“Filter Control” on page 57
SNMP	Controls access to this AP-80 MB/SB from management stations using SNMP, as well as the hosts that will receive trap messages	“SNMP” on page 58
VLAN	Control access to network resources and increase security through assignment of VLAN IDs	“VLAN” on page 61
AP Management	Controls access to network resources and increase security.	“AP Management” on page 63
Administration	Configures user name and password for management access; upgrades software from local file, FTP or TFTP server; resets configuration settings to factory defaults; and resets the AP-80 MB/SB	“Administration” on page 64
System Log	Controls logging of error messages; sets the system clock via SNTP server or manual configuration	“System Log” on page 67
WDS	Sets the MAC addresses of other units in the AP-80 MB/SB network	“Wireless Distribution System (WDS)” on page 70
STP	Configures Spanning Tree Protocol parameters	“STP” on page 72
RSSI	Controls the maximum RSSI voltage output for specific WDS ports	“RSSI” on page 74
Radio Settings	Configures radio signal parameters, such as radio channel, transmission rate, and beacon settings for the 802.11a and 802.11g radios	“Radio Interface” on page 76
Security	Configures data encryption using Wired Equivalent Protection (WEP) or Wi-Fi Protected Access (WPA)	“Security” on page 84
AP Status	Displays basic system configuration settings and settings for the wireless interfaces	“AP Status” on page 95

Table 7 Advanced Configuration Page Options (Continued)

Menu	Description	Section and Page
Station Status	Lists the wireless clients currently associated with the access point.	“Station Status” on page 98

System Identification

The system information parameters for the AP-80 MB/SB can be left at their default settings. However, modifying these parameters can help you to more easily distinguish different devices in your network.

Choose **Identification** to open the System Identification page.

■ Identification

System Name :

The system name is designed for the user to uniquely identify this device.

Location :

Contact :

Set the following parameters on this page:

- *System Name*—Alias for the AP-80 MB/SB, enabling the device to be uniquely identified on the network. The default is Dual Band Outdoor. (Range: 1-22 characters)
- *Location*—Text string that describes the system location. (Maximum length: 20 characters)
- *Contact*—Text string that describes the system contact. (Maximum length: 255 characters)

CLI Commands for System Identification

Enter the global configuration mode and use the **system name** command to specify a new system name. Use the **snmp-server location** and **snmp-server contact** commands to indicate the physical location of the AP-80 MB/SB and define a system contact. Then return to the Exec mode, and use the **show system** command to display the changes to the system identification settings.

```
Aruba Networks AP-80MB#show system

System Information
=====
Serial Number       : 0A80001590
System Up time     : 3 days, 22 hours, 55 minutes, 2 seconds
System Name        : Aruba Networks AP-80B
System Location    : Company A
System Contact     : Amy Yee
System Country Code : US - UNITED STATES
MAC Address        : 00-0B-86-C3-91-93
802.11a MAC Address : Default=00-0B-86-39-19-10   VAP1=00-0B-86-39-19-11
                   :                   VAP2=00-0B-86-39-19-12   VAP3=00-0B-86-39-19-13
802.11b/g MAC Address : Default=00-0B-86-39-19-20   VAP1=00-0B-86-39-19-21
                   :                   VAP2=00-0B-86-39-19-22   VAP3=00-0B-86-39-19-23
IP Address         : 10.0.6.87
Subnet Mask        : 255.255.255.0
Default Gateway    : 10.0.6.1
Management VLAN ID(AP) : 1
IAPP State         : ENABLED
DHCP Client        : DISABLED
HTTP Server        : ENABLED
HTTP Server Port   : 80
HTTP Session Timeout : 0 sec(s)
HTTPS Server       : ENABLED
HTTPS Server Port  : 443
Slot Status        : Dual band(a/g)
Boot Rom Version   : v1.1.1
Software Version   : v2.0.2.18b04
SSH Server         : ENABLED
SSH Server Port    : 22
Telnet Server      : ENABLED
DHCP Relay         : ENABLED
=====

Aruba Networks AP-80MB#
```

TCP / IP Settings

You can use the web browser interface to access IP addressing only if the AP-80 MB/SB already has an IP address that is reachable through your network.

By default, the AP-80 MB/SB is configured with a static IP address (192.168.1.1). However, you can change the IP address or configure the device to obtain its IP address from a DHCP server. After you have network access to the AP-80 MB/SB, you can use the web browser interface to modify the initial IP configuration, if needed.

Choose **TCP/IP** to open the TCP/IP Settings page.

■ TCP / IP Settings

DHCP Client

- Enable The Access Point will obtain the IP Address from the DHCP server.
 Disable The Access Point will use the following IP setup

IP Address

IP Address	<input type="text" value="10.0.6.87"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="10.0.6.1"/>
Primary DNS Address	<input type="text" value="64.81.79.2"/>
Secondary DNS Address	<input type="text" value="216.231.41.2"/>

■ DHCP Relay Settings

DHCP Relay Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Relay Agent Primary Server	<input type="text" value="10.0.6.3"/>
Relay Agent Secondary Server	<input type="text" value="10.0.6.4"/>

■ Telnet / SSH Settings

Telnet Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
SSH Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
SSH Port	<input type="text" value="22"/>

■ Speed-Duplex

Opera. speed-duplex	100Base-TX Full
Admin. speed-duplex	<input type="text" value="Auto"/>

■ Ethernet Interface Information

[Ethernet Interface Statistics Information](#)

[Apply

Set the following parameters on this page:

DHCP Client

- *DHCP Client (Enable)*—Select this option to obtain the IP settings for the AP-80 MB/SB from a DHCP (Dynamic Host Configuration Protocol) server. The IP address, subnet mask, default gateway, and Domain Name Server (DNS) address are dynamically assigned to the AP-80 MB/SB by the network DHCP server. (Default: Enabled)
- *DHCP Client (Disable)*—Select this option to manually configure a static address for the AP-80 MB/SB.

IP Address

- *IP Address*—IP address of the AP-80 MB/SB. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- *Subnet Mask*—Mask that identifies the host address bits used for routing to specific subnets.

- *Default Gateway*—IP address of the router for the AP-80 MB/SB, which is used if the requested destination address is not on the local subnet. If you have management stations, DNS servers, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided. Otherwise, leave the address as all zeros (0.0.0.0).
- *Primary and Secondary DNS Address*—IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of IP addresses.

If you have one or more DNS servers located on the local network, type the IP addresses in the text fields provided. Otherwise, leave the addresses as all zeros (0.0.0.0).

DHCP Relay Settings

- *DHCP Relay*—Indication of whether the DHCP relay function is enabled or disabled.
- *Relay Agent Primary Server*—Server that receives DHCP requests, if DHCP Relay is enabled.
- *Relay Agent Secondary Server*—Server that receives DHCP requests, if DHCP Relay is enabled and the primary server is not available.

Telnet/SSH Settings

- *Telnet Server*—Indication of whether Telnet access to the AP-80 MB/SB is enabled or disabled.
- *SSH Server*—Indication of whether SSH access to the AP-80 MB/SB is enabled or disabled.
- *SSH Port*—Port for SSH communications (default is 22).

Speed/Duplex Settings

- *Operational speed-duplex*—Current speed and duplex settings.
- *Admin. speed-duplex*—Speed and duplex settings for the administrative interface to the AP-80 MB/SB.

In addition to setting parameters, you can view Ethernet statistics for the link by clicking Ethernet Interface Statistics Information:

☰ Ethernet Interface Statistics Information

ifInOctets	ifInUcastPkts	ifInNUcastPkts	ifInDiscards	ifInErrors	ifInUnkProtos
8373628	7019	35428	0	0	351
OutOctets	OutInUcastPkts	OutNUcastPkts	OutDiscards	OutErrors	
13183504	11725	21	0	0	

CLI Commands for TCP/IP Settings

From the global configuration mode, enter the interface configuration mode with the interface ethernet command. Use the **ip dhcp** command to enable the DHCP client, or **no ip dhcp** to disable it. To manually configure an address, specify the new IP address, subnet mask, and default gateway using the **ip address** command. To specify DNS server addresses use the **dns server** command. Then use the **show interface ethernet** command from the Exec mode to display the current IP settings.

```

Aruba Networks AP-80MB#show interface ethernet

Ethernet Interface Information
=====
IP Address           : 10.0.6.87
Subnet Mask          : 255.255.255.0
Default Gateway      : 10.0.6.1
Primary DNS          : 64.81.79.2
Secondary DNS        : 216.231.41.2
Opera. Speed-duplex : 100Base-TX Full Duplex
Admin. Speed-duplex : Auto
Admin status         : Up
Operational status   : Up
Untagged VlanId      : 1
=====
Ethernet Interface Statistics Information
=====
ifInOctets           : 47368215
ifInUcastPkts        : 720
ifInNUcastPkts       : 188319
ifInDiscards         : 0
ifInErrors           : 0
ifInUnkProtos        : 18
ifOutOctets           : 565174
ifOutUcastPkts       : 936
ifOutNUcastPkts      : 19
ifOutDiscards        : 0
ifOutErrors          : 0
=====
Ethernet RT Driver Information
=====
Speed-duplex         : 100Base-TX Full Duplex
RT Register Information
Reg 00 (0x00) Basic Mode Control (GEN_ctl)   = 0x3100
Reg 01 (0x01) Basic Mode Status (GEN_sts)    = 0x786D
Reg 02 (0x02) PHY Identifier 1 (GET_id_hi)   = 0x0000
Reg 03 (0x03) PHY Identifier 2 (GET_id_lo)   = 0x8201
Reg 04 (0x04) Auto-Neg Advertisement (AN_adv) = 0x01E1
Reg 05 (0x05) Auto-Neg Link Partner Ability = 0x45E1
Reg 06 (0x06) Auto-Neg Expansion             = 0x0001
=====
Aruba Networks AP-80MB#

```

RADIUS

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user who requires access to the network.



This guide assumes that you have already configured a RADIUS server or servers to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

Choose **RADIUS** to open the RADIUS page.

☰ RADIUS

MAC Address Format

<input checked="" type="radio"/> No Delimiter	XXXXXXXXXXXX
<input type="radio"/> Single Dash	XXXXXX-XXXXXX
<input type="radio"/> Multi-Dash	XX-XX-XX-XX-XX-XX
<input type="radio"/> Multi-Colon	XX:XX:XX:XX:XX:XX

VLAN ID Format

<input checked="" type="radio"/> Ascii
<input type="radio"/> Hex

Primary RADIUS Server Setup

RADIUS Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IP Address	0.0.0.0
Port	1812
Key	•••••
Timeout (seconds)	5
Retransmit attempts	3
Accounting Port	0
Interim Update Timeout	3600

Secondary RADIUS Server Setup

RADIUS Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IP Address	0.0.0.0
Port	1812
Key	•••••
Timeout (seconds)	5
Retransmit attempts	3
Accounting Port	0
Interim Update Timeout	3600

Set the following parameters on this page:

Primary Radius Server Setup

A primary RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security. A secondary RADIUS server may also be specified as a backup should the primary server fail or become inaccessible.

- *RADIUS Status*—Indication of whether RADIUS services are enabled or disabled.
- *IP Address*—IP address or host name of the RADIUS server.
- *Port*—UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- *Key*—Shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 255 characters)

- *Timeout*—Number of seconds the access point waits for a reply from the RADIUS server before resending a request. (Range: 1-60 seconds; Default: 5)
- *Retransmit attempts*—The number of times the access point tries to resend a request to the RADIUS server before authentication fails. (Range: 1-30; Default: 3)
- *Accounting Port*—RADIUS server port used for RADIUS accounting requests.
- *Interim Update Timeout*—The interval between transmitting accounting updates to the RADIUS server. (Range: 60-86400; Default: 3600 seconds)



For the Timeout and Retransmit attempts fields, accept the default values unless you experience problems connecting to the RADIUS server over the network.

Secondary Radius Server Setup

Configure a secondary RADIUS server to provide a backup in case the primary server fails. The access point uses the secondary server if the primary server fails or becomes inaccessible. Once the access point switches over to the secondary server, it periodically attempts to establish communication again with primary server. If communication with the primary server is re-established, the secondary server reverts to a backup role.

- *RADIUS Status*—Indication of whether RADIUS services are enabled or disabled.
- *IP Address*—IP address or host name of the RADIUS server.
- *Port*—UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- *Key*—Shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 255 characters)
- *Timeout*—Number of seconds the access point waits for a reply from the RADIUS server before resending a request. (Range: 1-60 seconds; Default: 5)
- *Retransmit attempts*—Number of times the access point tries to resend a request to the RADIUS server before authentication fails. (Range: 1-30; Default: 3)
- *Accounting Port*—RADIUS server port used for RADIUS accounting requests.
- *Interim Update Timeout*—The interval between transmittal of accounting updates to the RADIUS server. (Range: 60-86400; Default: 3600 seconds)

CLI Commands for RADIUS

From the global configuration mode, use the **radius-server address** command to specify the address of the primary or secondary RADIUS servers. (The following example configures the settings for the primary RADIUS server.) Configure the other parameters for the RADIUS server. Then use the **show radius** command from the Exec mode to display the current settings for the primary and secondary RADIUS servers.

```

Aruba Networks AP-80MB(config)#radius-server address 192.168.1.25
Aruba Networks AP-80MB(config)#radius-server port 181
Aruba Networks AP-80MB(config)#radius-server key green
Aruba Networks AP-80MB(config)#radius-server timeout 10
Aruba Networks AP-80MB(config)#radius-server retransmit 5
Aruba Networks AP-80MB(config)#exit
Aruba Networks AP-80MB#show radius

Radius Server Information
=====
IP          : 192.168.1.25
Port       : 181
Key        : *****
Retransmit : 5
Timeout    : 10
=====

Radius Secondary Server Information
=====
IP          : 0.0.0.0
Port       : 1812
Key        : *****
Retransmit : 3
Timeout    : 5
=====
Aruba Networks AP-80MB#

```

Authentication

Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point, or by using a database configured on a central RADIUS server. Alternatively, authentication can be implemented using the IEEE 802.1X network access control protocol.

The access point can also operate in an 802.1X supplicant mode. This enables the access point itself and any bridge-connected units to be authenticated with a RADIUS server using a configured MD5 user name and password. This mechanism can prevent rogue access points from gaining access to the network.

Choose **Authentication** to open the page.

Authentication

MAC Authentication : Disable

802.1X supplicant : Disable Enable

Username

Password

Local MAC Authentication :

System Default Deny Allow

MAC Authentication Settings :

MAC Address	Permission	Update
<input type="text"/>	<input type="radio"/> Deny <input checked="" type="radio"/> Allow <input type="radio"/> Delete	<input type="button" value="Update"/>

MAC Authentication Table :

Number	MAC Address	Permission

Set the following parameters on this page:

- *MAC Authentication*—Indication of whether MAC authentication is enabled or disabled. You can configure a list of the MAC addresses for wireless clients that are authorized to access the network. This provides a basic level of authentication for wireless clients attempting to gain access to the network. A database of authorized MAC addresses can be stored locally on the access point or remotely on a central RADIUS server. (Default: Local MAC)
- *802.1X Supplicant*—Indication of whether the access point can act as an 802.1X supplicant so it can be authenticated through a WDS (wireless) port with a RADIUS server on the remote network. When enabled, a unique MD5 user name and password needs to be configured for the WDS port. For an AP-80SB Slave unit, there is only one WDS port. For an AP-80MB Master unit, there are 16 WDS ports. (Default: Disabled) Enables/Disables the 802.1X supplicant function.
 - Username—MD5 user name. (Range: 1-22 characters)
 - Password— MD5 password. (Range: 1-22 characters)
- *Local MAC Authentication*—The MAC address of the associating station is compared against the local database stored on the access point. The Local MAC Authentication section enables the local database to be set up.
- *MAC Authentication Settings*—Local MAC authentication database configuration. The MAC database provides a mechanism to take certain actions based on a wireless client’s MAC address. The MAC list can be configured to allow or deny network access to specific clients. Click Update to implement the changes:
 - Deny: Blocks access for all MAC addresses except those listed in the local database as “Allow.”
 - Allow: Permits access for all MAC addresses except those listed in the local database as “Deny.”
 - Delete: Removes the MAC address from the list.



Client station MAC authentication occurs prior to the IEEE 802.1X authentication procedure configured for the access point. However, a client’s MAC address provides relatively weak user authentication, since MAC addresses can be easily captured and used by another station to break into the network. Using 802.1X provides more robust user authentication using user names and passwords or digital certificates. So, although you can configure the access point to use MAC address and 802.1X authentication together, it is better to choose one or the other, as appropriate.

CLI Commands for 802.1X Supplicant Configuration

Use the **802.1X supplicant** commands to set the Ethernet user name and password, and to enable the feature.

```
Aruba Networks AP-80MB(config)#802.1X supplicant eth_user David password DEF
Aruba Networks AP-80MB(config)#802.1X supplicant enable
Aruba Networks AP-80MB(config)#
```

CLI Commands for Local MAC Authentication

Use the **mac-authentication server** command from the global configuration mode to enable local MAC authentication. Set the default for MAC addresses not in the local table using the **address filter default** command, then enter MAC addresses in the local table using the **address filter entry**

command. To remove an entry from the table, use the **address filter delete** command. To display the current settings, use the **show authentication** command from the Exec mode.

```
Aruba Networks AP-80MB(config)#mac-authentication server local
Aruba Networks AP-80MB(config)#address filter default denied
Aruba Networks AP-80MB(config)#address filter entry 00-70-50-cc-99-1a
denied
Aruba Networks AP-80MB(config)#address filter entry 00-70-50-cc-99-1b allowed
Aruba Networks AP-80MB(config)#address filter entry 00-70-50-cc-99-1c allowed
Aruba Networks AP-80MB(config)#address filter delete 00-70-50-cc-99-1c
Aruba Networks AP-80MB(config)#exit
Aruba Networks AP-80MB#show authentication

Authentication Information
=====
MAC Authentication Server      : LOCAL
MAC Auth Session Timeout Value : 300 secs
802.1X                        : DISABLED
Broadcast Key Refresh Rate    : 5 min
Session Key Refresh Rate      : 5 min
802.1X Session Timeout Value  : 300 secs
Address Filtering             : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address          Status
-----
00-70-50-cc-99-1a   DENIED
00-70-50-cc-99-1b   ALLOWED
=====
Aruba Networks AP-80MB#
```

CLI Commands for RADIUS MAC Authentication

Use the **mac-authentication server** command from the global configuration mode to enable remote MAC authentication. Set the timeout value for re-authentication using the **mac-authentication session-timeout** command. Be sure to also configure connection settings for the RADIUS server (not shown in the following example). To display the current settings, use the **show authentication** command from the Exec mode.

```
Aruba Networks AP-80MB(config)#mac-authentication server remote
Aruba Networks AP-80MB(config)#mac-authentication session-timeout 300
Aruba Networks AP-80MB(config)#exit
Aruba Networks AP-80MB#show authentication

Authentication Information
=====
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 300 secs
802.1X                        : DISABLED
Broadcast Key Refresh Rate    : 5 min
Session Key Refresh Rate      : 5 min
802.1X Session Timeout Value  : 300 secs
Address Filtering             : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address          Status
-----
00-70-50-cc-99-1a   DENIED
00-70-50-cc-99-1b   ALLOWED
=====
Aruba Networks AP-80MB#
```


Filter Control

The AP-80 MB/SB can employ VLAN tagging support and network traffic frame filtering to control access to network resources and increase security.

Choose **Filter Control** to open the page.

Filter Control

Inter Client STAs Communication Filter :

- Disable
- Prevent intra VAP client communication
- Prevent inter and intra VAP client communication

AP Management Filter :

- Disable
- Enable (Prevent AP management via wireless client.)

Uplink Port MAC Address Filtering Status :

- Disable
- Enable

Ethernet Type Filter :

- Disable
- Enable

Local Management	ISO Designator	Status
Aironet_DDP	0x872d	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Appletalk_ARP	0x80f3	<input checked="" type="radio"/> OFF <input type="radio"/> ON
ARP	0x0806	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Banyan	0x0bad	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Berkeley_Trailer_Negotiation	0x1000	<input checked="" type="radio"/> OFF <input type="radio"/> ON
CDP	0x2000	<input checked="" type="radio"/> OFF <input type="radio"/> ON
DEC_LAT	0x6004	<input checked="" type="radio"/> OFF <input type="radio"/> ON
DEC_MOP	0x6002	<input checked="" type="radio"/> OFF <input type="radio"/> ON
DEC_MOP_Dump_Load	0x6001	<input checked="" type="radio"/> OFF <input type="radio"/> ON
DEC_XNS	0x6000	<input checked="" type="radio"/> OFF <input type="radio"/> ON
EAPOL	0x888e	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Enet_Config_Test	0x9000	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Ethertalk	0x809b	<input checked="" type="radio"/> OFF <input type="radio"/> ON
IP	0x0800	<input checked="" type="radio"/> OFF <input type="radio"/> ON
IPv6	0x86dd	<input checked="" type="radio"/> OFF <input type="radio"/> ON
LAN_Test	0x0708	<input checked="" type="radio"/> OFF <input type="radio"/> ON
NetBEUI	0xf0f0	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Novell_IPX(new)	0x8138	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Novell_IPX(old)	0x8137	<input checked="" type="radio"/> OFF <input type="radio"/> ON
PPPoE_Discovery	0x8863	<input checked="" type="radio"/> OFF <input type="radio"/> ON
PPPoE_PPP_Session	0x8864	<input checked="" type="radio"/> OFF <input type="radio"/> ON
RARP	0x8035	<input checked="" type="radio"/> OFF <input type="radio"/> ON
Telxon_TXP	0x8729	<input checked="" type="radio"/> OFF <input type="radio"/> ON
X.25_Level3	0x0805	<input checked="" type="radio"/> OFF <input type="radio"/> ON

Set the following parameters on this page:

- *Inter Client STAs Communication Filter*—Filters for communications between client stations. You can prevent intra virtual access point (VAP) client communications, prevent inter and intra VAP client communications, or allow communications by disabling the filter.
- *AP Management Filter*—Indication of whether the access point can be managed through the wireless interface.

- *Uplink Port MAC Address Filtering Status*—Prevents traffic with specified source MAC addresses from being forwarded to wireless clients through the access point. When you enable this field the following fields are displayed:
 - *MAC Address*—Specifies a MAC address to filter, in the form xx-xx-xx-xx-xx-xx.
 - *Permission*—Adds or deletes a MAC address from the filtering table. You can add a maximum of four MAC addresses to the filter table. (Default: Disabled)
- *Ethernet Type Filter*—Indication of whether filters are enabled for different types of Ethernet traffic. You can turn filtering on or off for all the protocols and applications listed on the page. Ethernet protocol types not listed in the filtering table are always forwarded by the access point.
 - *Disabled*—Ethernet protocol types are not filtered.
 - *Enabled*—Ethernet protocol types are filtered based on the configuration of protocol types in the filter table. If the status of a protocol is set to ON, the protocol is filtered from the access point.

CLI Commands for Bridge Filtering

Use the **filter ap-manage** command to restrict management access from wireless clients. To configure Ethernet protocol filtering, use the **filter ethernet-type enable** command to enable filtering and the **filter ethernet-type protocol** command to define the protocols that you want to filter. To display the current settings, use the **show filters** command from the Exec mode.

```
Aruba Networks AP-80MB(config)#filter ap-manage
Aruba Networks AP-80MB(config)#filter ethernet-type enable
Aruba Networks AP-80MB(config)#filter ethernet-type protocol ARP
Aruba Networks AP-80MB(config)#exit
Aruba Networks AP-80MB#show filters

Protocol Filter Information
=====
AP Management           :ENABLED
Ethernet Type Filter   :ENABLED

Enabled Protocol Filters
-----
Protocol: ARP           ISO: 0x0806
=====
Aruba Networks AP-80MB#
```

SNMP

You can use a network management application to manage the AP-80 MB/SB via the Simple Network Management Protocol (SNMP) from a management station. To implement SNMP management, the AP-80 MB/SB must have an IP address and subnet mask, configured either manually or dynamically. Once an IP address has been configured, appropriate SNMP communities and trap receivers should be configured.

Community names are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the AP-80 MB/SB. To communicate with the AP-80 MB/SB, a management station must first submit a valid community name for authentication. You therefore need to assign community names to specified users or user groups and set the access level.

Choose **SNMP** to open the page.

#SNMP

SNMP: Disable Enable

Location	On Track Inc.
Contact	Barbara Weinstein
Community Name (Read Only)	*****
Community Name (Read/Write)	*****

Trap Destination:

Trap Destination 1	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Trap Destination 1 IP Address	0.0.0.0
Trap Destination 1 Community Name	*****
Trap Destination 2	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Trap Destination 2 IP Address	0.0.0.0
Trap Destination 2 Community Name	*****
Trap Destination 3	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Trap Destination 3 IP Address	0.0.0.0
Trap Destination 3 Community Name	*****
Trap Destination 4	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Trap Destination 4 IP Address	0.0.0.0
Trap Destination 4 Community Name	*****

Trap Configuration:

<input checked="" type="checkbox"/> sysSystemUp	<input checked="" type="checkbox"/> dot1xMacAddrAuthFail
<input checked="" type="checkbox"/> sysSystemDown	<input checked="" type="checkbox"/> dot1xAuthNotInitiated
<input checked="" type="checkbox"/> sysRadiusServerChanged	<input checked="" type="checkbox"/> dot1xAuthSuccess
<input checked="" type="checkbox"/> sysConfigFileVersionChanged	<input checked="" type="checkbox"/> dot1xAuthFail
<input checked="" type="checkbox"/> dot11StationAssociation	<input checked="" type="checkbox"/> localMacAddrAuthSuccess
<input checked="" type="checkbox"/> dot11StationReAssociation	<input checked="" type="checkbox"/> localMacAddrAuthFail
<input checked="" type="checkbox"/> dot11StationAuthentication	<input checked="" type="checkbox"/> dot1xSuppAuthenticated
<input checked="" type="checkbox"/> dot11StationRequestFail	<input checked="" type="checkbox"/> iappStationRoamedFrom
<input checked="" type="checkbox"/> dot11InterfaceAFail	<input checked="" type="checkbox"/> iappStationRoamedTo
<input checked="" type="checkbox"/> dot11InterfaceGFail	<input checked="" type="checkbox"/> iappContextDataSent
<input checked="" type="checkbox"/> dot1xMacAddrAuthSuccess	<input checked="" type="checkbox"/> snmpServerFail
<input checked="" type="checkbox"/> wirelessExternalAntenna	<input checked="" type="checkbox"/> dot11StationDisassociate
<input checked="" type="checkbox"/> dot11StationDeauthenticate	<input checked="" type="checkbox"/> dot11StationAuthenticateFail

#SNMPv3 Configuration

Engine-ID: 80:00:07:e5:80:00:00:27:04:00:00:00:0e

User	Group	Auth Type	Passphrase	Priv Type	Passphrase	Action
New User	RO	None		None		Add
User List						

Target ID	IP Address	UDP port	SNMP user	Filter ID	Action
New Target		162			Add
Target List					

Filter ID	Filter Type	Subtree	Mask	Action
New Filter	Include		None	Add
Filter List				

Set the following parameters on this page:

SNMP

- *SNMP*—Enables or disables SNMP management access and also enables the AP-80 MB/SB to send SNMP traps (notifications). SNMP management is enabled by default.
- *Location*—Specifies the name for the location of the AP-80 MB/SB.
- *Community Name (Read Only)*—Defines the SNMP community access string that has read-only access. Authorized management stations are only able to retrieve MIB objects. (Maximum length: 23 characters, case sensitive; Default: public)
- *Community Name (Read/Write)*—Defines the SNMP community access string that has read/write access. Authorized management stations are able to both retrieve and modify MIB objects. (Maximum length: 23 characters, case sensitive; Default: private)
- *Trap Destination*—Enables or disable the trap destination.
- *Trap Destination IP Address*—Specifies the recipient of SNMP notifications. Enter the IP address or the host name. (Host Name: 1 to 20 characters)

SNMP V3

Configure values for these fields and click **Add**.

- *Engine ID*—Sets the engine identifier for the SNMPv3 agent that resides on the AP. The engine protects against message replay, delay, and redirection. It is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets. A default engine ID is automatically generated that is unique to the access point. (Range: 10 to 64 hexadecimal characters)



If the local engine ID is deleted or changed, all SNMP users will be cleared and all existing users will need to be re-configured. If it is necessary to change the default engine ID, change it first before configuring other SNMP v3 parameters.

- *SNMP Users*—Specifies information for SNMP users:
 - *User*—SNMP user.
 - *Group*—SNMP group.
 - *Auth Type*—Type of authentication.
 - *Passphrase*—Pass code for authentication.
 - *Priv Type*—Data encryption type used for the SNMP user. When DES (Data Encryption Standard) is selected, enter a key in the corresponding Passphrase field.
 - *Passphrase*—Pass code for authentication.
- *SNMP Targets*—Specifies servers as trap recipients.
 - *Target ID*—SNMP user.
 - *IP Address*—IP address of the target server.
 - *UDP port*—UDP port on the target server.
 - *SNMP user*—SNMP user on the target server.
 - *Filter ID*—Name that describes the filter.
- *SNMP Filter*—Specifies the type of SNMP filter.
 - *Filter ID*—Name that describes the filter.
 - *Filter Type*—Exclude or include.

- Subtree—Specifies the MIB subtree to be filtered. The subtree must be defined in the form “.x.x.x.x” and begin with a “.”.
- Mask—Specifies the subnet mask for the subtree.

CLI Commands for SNMP

Use the **snmp-server enable server** command from the global configuration mode to enable SNMP. To set read/write and read-only community names, use the **snmp-server community** command. The **snmp-server host** command defines a trap receiver host. To view the current SNMP settings, use the **show snmp** command.

```

Aruba Networks AP-80MB#show snmp

SNMP Information
=====
Service State           : Disable
Community (ro)         : *****
Community (rw)         : *****
Location                : Building 1
Contact                 : Amy Yee

EngineId      :80:00:07:e5:80:00:00:27:04:00:00:00:0e
EngineBoots:10

Trap Destinations:
1:      0.0.0.0, Community: *****, State: Disabled
2:      0.0.0.0, Community: *****, State: Disabled
3:      0.0.0.0, Community: *****, State: Disabled
4:      0.0.0.0, Community: *****, State: Disabled

      systemUp      Enabled      systemDown      Enabled
radiusServerChanged Enabled      configFileVersionChanged Enabled
      sntpServerFail Enabled      dot11StationAssociation Enabled
dot11StationReAssociation Enabled      dot11StationAuthentication Enabled
dot11StationRequestFail Enabled      dot1XMacAddrAuthSuccess Enabled
      dot1XMacAddrAuthFail Enabled      dot1XAuthNotInitiated Enabled
      dot1XAuthSuccess Enabled      dot1XAuthFail Enabled
localMacAddrAuthSuccess Enabled      localMacAddrAuthFail Enabled
iappStationRoamedFrom Enabled      iappStationRoamedTo Enabled
iappContextDataSent Enabled      dot1XSuppAuthenticated Enabled
wirelessExternalAntenna Enabled      dot11InterfaceAFail Enabled
      dot11InterfaceGFail Enabled

=====
Aruba Networks AP-80MB#

```

VLAN

The access point can employ VLAN tagging support to control access to network resources and increase security. VLANs separate traffic passing between the AP, associated clients, and the wired network. There can be a VLAN assigned to each associated client, a default VLAN for each VAP (Virtual Access Point) interface, and a management VLAN for the access point. The following properties apply to VLANs:

- The management VLAN is for managing the access point through remote management tools, such as the web interface, SSH, SNMP, or Telnet. The access point only accepts management traffic that is tagged with the specified management VLAN ID.
- All wireless clients associated to the access point are assigned to a VLAN. If IEEE 802.1X is being used to authenticate wireless clients, specific VLAN IDs can be configured on the RADIUS server to be assigned to each client. If a client is not assigned to a specific VLAN or if 802.1X is not used, the client is assigned to the default VLAN for the VAP interface with which it is associated. The access point only allows traffic tagged with assigned VLAN IDs or default VLAN IDs to access clients associated on each VAP interface.

- When VLAN support is enabled on the access point, traffic passed to the wired network is tagged with the appropriate VLAN ID, either an assigned client VLAN ID, default VLAN ID, or the management VLAN ID. Traffic received from the wired network must also be tagged with one of these known VLAN IDs. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.
- When VLAN support is disabled, the access point does not tag traffic passed to the wired network and ignores the VLAN tags on any received frames.



Before enabling VLAN tagging on the access point, be sure to configure the attached network switch port to support tagged VLAN frames from the access point's management VLAN ID, default VLAN IDs, and other client VLAN IDs. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

Using IEEE 802.1X and a central RADIUS server, up to 64 VLAN IDs can be mapped to specific wireless clients, allowing users to remain within the same VLAN as they move around a campus site. This feature can also be used to control access to network resources from clients, thereby improving security.

A VLAN ID (1-4094) can be assigned to a client after successful IEEE 802.1X authentication. The client VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. If a client does not have a configured VLAN ID on the RADIUS server, the access point assigns the client to the configured default VLAN ID for the VAP interface. When using IEEE 802.1X to dynamically assign VLAN IDs, the access point must have 802.1X authentication enabled and a RADIUS server configured. Wireless clients must also support 802.1X client software.

When setting up VLAN IDs for each user on the RADIUS server, be sure to use the RADIUS attributes and values as indicated in the following table. VLAN IDs on the RADIUS server can be entered as hexadecimal digits or a string. Refer to your RADIUS server software documentation for further information on RADIUS configuration.



Before enabling VLANs on the access point, you must configure the connected LAN switch port to accept tagged VLAN packets with the native VLAN ID of the AP-80 MB/SB. Otherwise, connectivity to the AP-80 MB/SB will be lost when you enable the VLAN feature.

Table 8 *RADIUS Server Values and Attributes*

Number	RADIUS Attribute	Value
64	Tunnel-Type	VLAN (13)
65	Tunnel-Medium-Type	802
81	Tunnel-Private-Group	VLANID (1 to 4094 in hexadecimal)



The specific configuration of RADIUS server software is beyond the scope of this guide. Refer to the documentation provided with the RADIUS server software.

Choose **VLAN** to open the page.

■ VLAN Configuration

Management VLAN ID :
Ethernet Untagged VLAN ID :

Set the following parameters on this page:

Management VLAN ID—Indicates the management VLAN.

Ethernet Untagged VLAN ID—Indicates the VLAN ID assigned to wireless clients that are not assigned to a specific VLAN by RADIUS server configuration. (Range: 1-64)

CLI Commands for VLAN Support

From the global configuration mode use the **management-vlanid** command to set the ID for the management VLAN and the **untagged-vlanid** command to assign the default VLAN for incoming untagged packets.

```
Aruba Networks AP-80MB(config)#management-vlanid 3  
Aruba Networks AP-80MB(if-ethernet)#untagged-vlanid 10  
Aruba Networks AP-80MB#
```

AP Management

The AP-80 MB/SB includes options to control access to the UI and limit the IP addresses that can access the devices.

Choose **AP Management** to open the page.

■ AP Management

UI Management

Telnet Access Status	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Web Access Status	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
SNMP Access Status	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable

IP Management

- Any IP** Allow any IP address to access device
- Single IP** Specify one IP address to access device
- Multiple IP** Specify multiple IP address to access device

Set the following parameters on this page:

UI Management

- *Telnet Access Status*—Indicates whether AP access using Telnet is enabled or disabled.
- *Web Access Status*—Indicates whether AP access using a web browser is enabled or disabled.
- *SNMP Access Status*—Indicates whether AP access through SNMP is enabled or disabled.

IP Management

- *Any IP*—If selected, indicates that any IP address can access the AP.
- *Single IP*—If selected, indicates that only the specified IP address can access the IP. When you select this option, an IP address entry field is presented.

- *Multiple IP*—If selected, indicates that only the specified IP subnet can access the IP. When you select this option, an IP address field and subnet mask field are presented.

Administration

The Administration page includes parameters and actions for administering the AP:

Choose **AP Management** to open the page.

Administration

Change Password

Username	<input type="text" value="admin"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

Session Timeout for WEB

Timeout (0-1800) seconds	<input type="text" value="300"/> (value 0 is for disable)
--------------------------	---

Firmware Upgrade

Current version **v2.0.2.18b04**

Local

New firmware file	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Start Upgrade"/>		

Remote

<input type="radio"/> FTP	<input checked="" type="radio"/> TFTP
New firmware file	<input type="text"/>
IP Address	<input type="text"/>
<input type="button" value="Start Upgrade"/>	

It may take several minutes to upgrade the firmware, please wait...

Configuration File Backup and Restore

Server Type	<input type="radio"/> FTP	<input checked="" type="radio"/> TFTP
Method	<input checked="" type="radio"/> Export	<input type="radio"/> Import
Target File Name	<input type="text"/>	
IP Address	<input type="text"/>	
<input type="button" value="Start Export/Import"/>		

Restore Factory Settings

Reset Access Point

Changing the Password

Management access to the web and CLI interface on the AP-80 MB/SB is controlled through a single user name and password. You can also gain additional access security by using control filters (see “Filter Control” on page 57).

To protect access to the management interface, you need to configure an Administrator’s user name and password as soon as possible. If the user name and password are not configured, then anyone having access to the AP-80 MB/SB may be able to compromise AP-80 MB/SB and network security.



Pressing the Reset button on the back of the AP-80 MB/SB for more than five seconds resets the user name and password to the factory defaults. For this reason, we recommend that you protect the AP-80 MB/SB from physical access by unauthorized persons.

Set the following password parameters:

- *Username*—The name of the user. The default name is “admin.” (Length: 3-16 characters, case sensitive.)
- *New Password*—The password for management access. (Length: 3-16 characters, case sensitive)
- *Confirm New Password*—Enter the password again for verification.

CLI Commands for User Name and Password

Use the user name and password commands from the CLI configuration mode.

```
Aruba Networks AP-80MB(config)#username bob
Aruba Networks AP-80MB(config)#password spiderman
Aruba Networks AP-80MB#
```

Setting the Session Timeout

You can configure the number of seconds after which the WebUI session times out:

- *Timeout (1-1800) second*—Specifies the amount of time after which the WebUI session times out and requires login for continued access. Enter **0** if you do not want to required a timeout.

Upgrading Firmware

You can upgrade new AP-80 MB/SB software from a local file on the management workstation, or from an FTP or TFTP server.

After upgrading new software, you must reboot the AP-80 MB/SB to implement the new code. Until a reboot occurs, the AP-80 MB/SB will continue to run the software it was using before the upgrade started. Also note that rebooting the AP-80 MB/SB with new software resets the configuration to the factory default settings.



Before upgrading your AP-80 MB/SB software, Aruba recommends that you save a copy of the current configuration file. See “copy” on page 147 for information on saving the configuration file to a TFTP or FTP server.

Before upgrading new software, verify that the AP-80 MB/SB is connected to the network and has been configured with a compatible IP address and subnet mask.

If you need to download from an FTP or TFTP server, take the following additional steps:

1. Obtain the IP address of the FTP or TFTP server where the AP-80 MB/SB software is stored.

2. If upgrading from an FTP server, be sure that you have an account configured on the server with a user name and password.



If you have upgraded system software, then you must reboot the AP-80 MB/SB to implement the new operation code.

The following parameters on the Administration page are used for firmware upgrading:

- *Current version (read only)*—Displays the runtime code version number.

New Firmware File (Local)

- *New firmware file*—Specifies the name of an image file to download from the web management station to the AP-80 MB/SB using HTTP. Use the Browse button to locate the image file locally on the management station and click **Start Upgrade** to proceed.

The new firmware file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 32 characters for files on the AP-80 MB/SB. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Firmware Upgrade Remote

- *FTP/TFTP*—Downloads an operation code image file from a specified remote FTP or TFTP server. After filling in the following fields, click Start Upgrade to proceed.
- *New firmware file*—Indicates the name of the code file on the server. The new firmware file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters or 32 characters for files on the AP-80 MB/SB. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- *IP Address*—Indicates the IP address or host name of FTP or TFTP server.
- *Username (FTP server only)*—Indicates the user ID used for login on an FTP server.
- *Password (FTP server only)*—Indicates password used for login on an FTP server.

Backing Up and Restoring the Configuration File

You can back up and restore the parameter settings configured on the AP-80 MB/SB. The following parameters on the Administration page are used for backup and restore:

- *Server Type*—Indicates whether the backup or restore involves an FTP or TFTP server. image file from a specified remote FTP or TFTP server.
- *Method*—Indicates whether the operation is for backup (Export) or restore (Import).
- *Target File Name*—Indicates the name of the image file to which the configuration will be saved or the file name from which the configuration will be restored.
- *IP Address*—Specifies the IP address of the FTP or TFTP server.

After filling in the following fields, click Start **Export/Import** to proceed.

Resetting the AP

You can reset the access point and restore factory settings. The following parameters on the Administration page are used to reset the AP:

- *Restore Factory Settings*—Click **Restore** to reset the configuration settings for the AP-80 MB/SB to the factory defaults and reboot the system. Note that all user configured information will be lost. You will have to re-enter the default user name (admin) to re-gain management access to this device.
- *Reset Access Point*—Click **Reset** to reboot the system.

CLI Commands for Downloading Software from a TFTP Server

Use the **copy tftp file** command from the Exec mode and then specify the file type, name, and IP address of the TFTP server. When the download is complete, the **dir** command can be used to check that the new file is present in the AP-80 MB/SB file system. To run the new software, use the **reset board** command to reboot the AP-80 MB/SB.

```
Aruba Networks AP-80MB#copy tftp file
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>: [1]:1
TFTP Source file name:bridge-img.bin
TFTP Server IP:192.168.1.19

Aruba Networks AP-80MB#dir
File Name                               Type   File Size
-----
dflt-img.bin                            2      1319939
bridge-img.bin                          2      1629577
syscfg                                  5       17776
syscfg_bak                             5       17776

                262144 byte(s) available

Aruba Networks AP-80MB#reset board
Reboot system now? <y/n>: y
```

CLI Commands for Resetting the AP-80 MB/SB Back to Factory Defaults

If required, the AP-80 MB/SB can be reset to factory defaults through either the system CLI or the Web User Interface.

In the CLI, the system command “reset configuration” from the Exec level prompt resets the existing configuration to factory default values. For details, see [Chapter 6, “CLI Commands.”](#)

If you do not have access to the CLI or web interface, you can perform a hardware reset using the following procedure:

1. Disconnect the network connection cable.
2. Remove the cover using an Allen wrench.
3. Reconnect the unit while the cover is off.
4. Press and hold the reset button for at least 5 seconds. The reset button is on the circuit board near the edge with the network connectors.

The unit is now reset to factory defaults.

5. Disconnect the unit and replace the cover.
6. Reconnect the cable.

The unit is now ready for use can be accessed using the web interface or CLI.

System Log

The AP-80 MB/SB can be configured to send event and error messages to a System Log server. The system clock can also be synchronized with a time server, so that all the messages sent to the Syslog server are stamped with the correct time and date.

The AP-80 MB/SB supports a logging process that can control error messages saved to memory or sent to a Syslog server. The logged messages serve as a valuable tool for isolating AP-80 MB/SB and network problems.

Choose **System Log** to open the page.

System Log

System Log Setup : Disable Enable

SNTP Server : Disable Enable

Primary Server	<input type="text" value="137.92.140.80"/>
Secondary Server	<input type="text" value="192.43.244.18"/>

Set Time Zone

Enter Time Zone
 Enable Daylight Saving From ~ To ~

AP Management

UI Management

Telnet Access Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Web Access Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
SNMP Access Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

IP Management

- Any IP** Allow any IP address to access device
- Single IP** Specify one IP address to access device
- Multiple IP** Specify multiple IP address to access device

Set the following parameters on this page:

- *System Log Setup*—Enables or disables the logging of error messages.

SNTP

- *SNTP Server*—Enables or disables use of an SNTP server for clock synchronization. Simple Network Time Protocol (SNTP) allows the AP-80 MB/SB to set its internal clock based on periodic updates from an SNTP or NTP time server. Maintaining an accurate time on the AP-80 MB/SB enables the system log to record meaningful dates and times for event entries. If the clock is not set, the AP-80 MB/SB only records the time from the factory default set at the last bootup.
The AP-80 MB/SB acts as an SNTP client, periodically sending time synchronization requests to specific time servers. You can configure up to two time server IP addresses. The AP-80 MB/SB attempts to poll each server in the configured sequence.
- *Primary Server*—Identifies the IP address of an SNTP or NTP time server that the AP-80 MB/SB attempts to poll for a time update.
- *Secondary Server*—Identifies the secondary SNTP server by IP address. The AP-80 MB/SB first attempts to update the time from the primary server; if this fails it attempts an update from the secondary server.

Set Time Zone

Use the following manual settings if you are not using SNTP:

- *Set Time Zone*—SNTP uses Coordinated Universal Time (UTC), formerly Greenwich Mean Time (GMT), based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours your time zone is located before (east) or after (west) UTC.
- *Enable Daylight Saving*—The AP-80 MB/SB provides a way to automatically adjust the system clock for Daylight Savings Time changes. To use this feature you must define the month and date to

begin and to end the change from standard time. During this period the system clock is set back or forward by one hour.

CLI Commands for System Logging

To enable logging on the AP-80 MB/SB, use the **logging on** command from the global configuration mode. The **logging level** command sets the minimum level of message to log. Use the **logging console** command to enable logging to the console. Use the **logging host** command to specify up to four Syslog servers. The CLI also allows the **logging facility-type** command to set the facility-type number to use on the Syslog server. To view the current logging settings, use the **show logging** command.

```
Aruba Networks AP-80MB(config)#logging on
Aruba Networks AP-80MB(config)#logging level alert
Aruba Networks AP-80MB(config)#logging console
Aruba Networks AP-80MB(config)#logging host 1 10.1.0.3 514
Aruba Networks AP-80MB(config)#logging facility-type 19
Aruba Networks AP-80MB(config)#exit
Aruba Networks AP-80MB#show logging

Logging Information
=====
Syslog State           : Enabled
Logging Host State    : Enabled
Logging Console State : Enabled
Server Domain name/IP : 1 10.1.0.3
Logging Level         : Error
Logging Facility Type  : 16
=====

Aruba Networks AP-80MB#
```

CLI Commands for SNTP

To enable SNTP support on the AP-80 MB/SB, from the global configuration mode specify SNTP server IP addresses using the **sntp-server ip** command, then use the **sntp-server enable** command to enable the service. Use the **sntp-server timezone** command to set the location time zone and the **sntp-server daylight-saving** command to set up a daylight saving. To view the current SNTP settings, use the **show sntp** command.

```
Aruba Networks AP-80MB(config)#sntp-server ip 10.1.0.19
Aruba Networks AP-80MB(config)#sntp-server enable
Aruba Networks AP-80MB(config)#sntp-server timezone +8
Aruba Networks AP-80MB(config)#sntp-server daylight-saving
Enter Daylight saving from which month<1-12>: 3
and which day<1-31>: 31
Enter Daylight saving end to which month<1-12>: 10
and which day<1-31>: 31
Aruba Networks AP-80MB(config)#exit
Aruba Networks AP-80MB#show sntp

SNTP Information
=====
Service State           : Enabled
SNTP (server 1) IP     : 137.92.140.80
SNTP (server 2) IP     : 192.43.244.18
Current Time           : 19 : 35, Oct 10th, 2003
Time Zone              : +8 (TAIPEI, BEIJING)
Daylight Saving       : Enabled, from Mar, 31th to Oct, 31th
=====

Aruba Networks AP-80MB#
```

CLI Commands for the System Clock

The following example shows how to manually set the system time when SNTP server support is disabled on the AP-80 MB/SB.

```
Aruba Networks AP-80MB(config)#no sntp-server enable
Aruba Networks AP-80MB(config)#sntp-server date-time
Enter Year<1970-2100>: 2003
Enter Month<1-12>: 10
Enter Day<1-31>: 10
Enter Hour<0-23>: 18
Enter Min<0-59>: 35
Aruba Networks AP-80MB(config)#
```

Wireless Distribution System (WDS)

The IEEE 802.11 standard defines a Wireless Distribution System (WDS) for connections between AP-80 MB/SBs. The AP-80 MB/SB uses WDS to forward traffic on bridge links between units. When using WDS, only AP-80 MB/SB units can associate to each other using the bridge band. A wireless client cannot associate with the access point on the AP-80 MB/SB band.

Up to six WDS bridge or repeater links (MAC addresses) per radio interface can be specified for each unit in the wireless bridge network. One unit only must be configured as the root bridge in the wireless network. The root bridge is the unit connected to the main core of the wired LAN. Other bridges need to specify one Parent link to the root bridge or to a bridge connected to the root bridge. The other five WDS links are available as “Child” links to other bridges.

Each radio interface can be set to operate in one of the following modes: (Default: AP)

- *AP (Access Point) mode*—Operates as an access point for wireless clients, providing connectivity to a wired LAN.

WDS Bridge

The VAP[1-3] will not be in service in Bridge or Root-Bridge Role.

802.11a Interface

Bridge Role AP Bridge Root-Bridge

802.11g Interface

Bridge Role AP Bridge Root-Bridge

- *Bridge mode*—Operates as a bridge to other access points. The “Parent” link to the root bridge must be configured. Up to five other “Child” links are available to other bridges.

WDS Bridge

The VAP[1-3] will not be in service in Bridge or Root-Bridge Role.

802.11a Interface

Bridge Role	<input type="radio"/> AP <input checked="" type="radio"/> Bridge <input type="radio"/> Root-Bridge
Bridge Parent	<input type="text" value="00-00-00-00-00-00"/>
Master/Slave Mode	<input checked="" type="radio"/> Master <input type="radio"/> Slave
Channel Auto Sync	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Bridge Child	1: <input type="text" value="00-00-00-00-00-00"/>
	2: <input type="text" value="00-00-00-00-00-00"/>
	3: <input type="text" value="00-00-00-00-00-00"/>
	4: <input type="text" value="00-00-00-00-00-00"/>
	5: <input type="text" value="00-00-00-00-00-00"/>
	6: <input type="text" value="00-00-00-00-00-00"/>
	7: <input type="text" value="00-00-00-00-00-00"/>
	8: <input type="text" value="00-00-00-00-00-00"/>

- *Root Bridge mode*—Operates as the root bridge in the wireless bridge network. Up to six “Child” links are available to other bridges in the network.

802.11a Interface

Bridge Role	<input type="radio"/> AP <input type="radio"/> Bridge <input checked="" type="radio"/> Root-Bridge
Bridge Child	1: <input type="text" value="00-00-00-00-00-00"/>
	2: <input type="text" value="00-00-00-00-00-00"/>
	3: <input type="text" value="00-00-00-00-00-00"/>
	4: <input type="text" value="00-00-00-00-00-00"/>
	5: <input type="text" value="00-00-00-00-00-00"/>
	6: <input type="text" value="00-00-00-00-00-00"/>
	7: <input type="text" value="00-00-00-00-00-00"/>
	8: <input type="text" value="00-00-00-00-00-00"/>

You can set the following parameters:

- *Bridge Parent*—The physical layer address of the root bridge unit or the bridge unit connected to the root bridge. (12 hexadecimal digits in the form “xx-xx-xx-xx-xx-xx”) (Bridge mode only)
- *Master/Slave Mode*—To set up a bridge link, you must configure the WDS forwarding table by specifying the Ethernet MAC address of the bridge to which you want to forward traffic.
 - *Slave bridge unit*—Specify the Ethernet MAC address of the AP-80 MB/SB unit at the opposite end of the link. (Bridge mode only)
 - *Master bridge unit*—Specify Ethernet MAC addresses of all the Slave bridge units in the network. (Bridge mode only)
- *Channel Auto Sync*—Allows a Bridge Child to automatically find the operating channel used by its Bridge Parent. (Bridge mode only)

- *Bridge Child*—The physical layer address of other bridge units for which this unit serves as the bridge parent or the root bridge. Note that the first entry under the list of child nodes is reserved for the root bridge, and can only be configured if the role is set to “Root Bridge.” (12 hexadecimal digits in the form “xx-xx-xx-xx-xx-xx”) (Bridge or Root Bridge mode)

STP

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the wireless bridge to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the root bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

Click **STP** to open the page.

Spanning Tree Protocol

Bridge	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Bridge Priority (0-65535)	<input type="text" value="32768"/>
Bridge Max Age (6-40 sec.)	<input type="text" value="20"/>
Bridge Hello Time (1-10 sec.)	<input type="text" value="2"/>
Bridge Forwarding Delay (4-30 sec.)	<input type="text" value="15"/>

802.11a Interface

Index	Link Path Cost(1-65535)	Link Port Priority(0-255)
Parent Node	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node2	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node3	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node4	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node5	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node6	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node7	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node8	<input type="text" value="19"/>	<input type="text" value="128"/>

802.11g Interface

Index	Link Path Cost(1-65535)	Link Port Priority(0-255)
Parent Node	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node2	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node3	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node4	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node5	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node6	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node7	<input type="text" value="19"/>	<input type="text" value="128"/>
Child Node8	<input type="text" value="19"/>	<input type="text" value="128"/>

Ethernet Interface

Link Path Cost(1-65535)	Link Port Priority(0-255)
<input type="text" value="19"/>	<input type="text" value="128"/>

Set the following parameters on this page:

- *Enable*—Enables/disables STP on the wireless bridge. (Default: Enabled)
- *Bridge Priority*—Used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.) (Range: 0-65535, default 32768)
- *Maximum Age*—The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (Range: 6-40, default 20 seconds)
- *Hello Time*—Interval (in seconds) at which the root device transmits a configuration message. (Range: 1-10 seconds, default 2)

- *Forward Delay*—The maximum time (in seconds) this device waits before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result. (Range: 4-30, default 15 seconds)

The following parameters are assigned separately for the 802.11a and 802.11b/g interfaces:

- *Link Path Cost*—This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) (Range: 1-10 seconds, default 19)
- *Link Port Priority*—Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Range: 0-240, in steps of 16, default 128)

The following parameter is for the Ethernet interface:

- *Link Path Cost*—This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) (Range: 1-10 seconds, default 19)

CLI Commands for STP

The following example configures spanning tree parameters for the bridge and wireless port 5.

```

Aruba Networks AP-80MB(config)#bridge stp enable
Aruba Networks AP-80MB(config)#bridge stp priority 40000
Aruba Networks AP-80MB(config)#bridge stp hello-time 5
Aruba Networks AP-80MB(config)#bridge stp max-age 38
Aruba Networks AP-80MB(config)#bridge stp forwarding-delay 12
Aruba Networks AP-80MB(config)#end
Aruba Networks AP-80MB#show bridge stp

Bridge STP Information
=====

Bridge MAC          : 00:0B:86:C3:91:93
Status              : Disabled
priority            : 32768
designated-root      : priority = 0, MAC = 00:00:00:00:00:00
root-path-cost      : 0
root-Port-no        : 0
Hold Time           :      1 Seconds
Hello Time          :      5 Seconds
Maximum Age         :     38 Seconds
Forward Delay       :     12 Seconds
bridge Hello Time   :      5 Seconds
bridge Maximum Age  :     38 Seconds
bridge Forward Delay :    12 Seconds
time-since-top-change: 772651 Seconds
topology-change-count: 0
Aruba Networks AP-80#

Aruba Networks AP-80MB#

```

RSSI

The RSSI value displayed on the RSSI page represents a signal to noise ratio. A value of 30 indicates that the power of the received signal is 30 dBm above the signal noise threshold. This value can be used to

align antennas (see “Align Antennas” on page 23) and monitor the quality of the received signal for bridge links. An RSSI value of about 30 or more indicates a strong enough signal to support the maximum data rate of 54 Mbps. Below a value of 30, the supported data rate would drop to lower rates. A value of 15 or less indicates that the signal is weak and the antennas may require realignment.

The RSSI controls allow the external connector to be disabled and the receive signal for each WDS port displayed.

Click **RSSI** to open the page.

RSSI

Auto Refresh	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Ambient Noise Floor	
Radio 11a	-96 dBm
Radio 11g	-91 dBm

802.11a Interface

RSSI Output Activate	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Refresh	<input type="button" value="refresh"/>	
RSSI Sample duration	10	
RSSI Value	Maximum	0
	Minimum	0
	Average	0
Port Number		

802.11g Interface

RSSI Output Activate	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Refresh	<input type="button" value="refresh"/>	
RSSI Sample duration	10	
RSSI Value	Maximum	0
	Minimum	0
	Average	0
Port Number		

Distance

802.11a Interface

Mode	<input checked="" type="radio"/> Normal <input type="radio"/> Turbo
11a Distance	00 KM

802.11g Interface

Mode	<input checked="" type="radio"/> Normal <input type="radio"/> Turbo
11g Distance	00 KM

Set the following parameters on this page:

- *Auto refresh*—Indication of whether the RSSI information is automatically refreshed. If auto refresh is selected, it is not necessary to click the Refresh button.
- *Ambient Noise Floor*—Ambient noise level.

The RSSI value for a selected port can be displayed and a representative voltage output can be enabled. You can set the following values for the 802.11a and 802.11g interface:

- *RSSI Output Activate*—Indication of whether RSSI voltage output on the external RSSI connector is enabled or disabled. (Default: Disabled).

- **RSSI Sample Duration**—Interval over which the RSSI is taken and averaged. (Default: 10 seconds)
- **RSSI Value**—Measured values (maximum, minimum, and average) over for the sample duration. (Default: 0 for each)
- **Port Number**—WDS port for which the maximum RSSI output voltage level is set. Ports 1-16 are available for a Master unit, only port 1 for a Slave unit. (Default: 0)

Distance

This value is used to adjust timeout values to take into account transmit delays due to link distances in the wireless bridge network. For a point-to-point link, specify the approximate distance between the two bridges. For a point-to-multipoint network, specify the distance of the Slave bridge farthest from the Master bridge.

- **Mode**—Indication of whether the 802.11a radio is operating in normal or Turbo mode. (See “Other Common Radio Settings” on page 80.)
- **Distance**—Approximate distance between antennas in a bridge link.

CLI Commands for RSSI

The following example configures the distance between antennas in a bridge link to be 2km.

```
Aruba Networks AP-80MB#config
Enter configuration commands, one per line.
Aruba Networks AP-80MB(config)#interface wireless a
Enter Wireless configuration commands, one per line.
Aruba Networks AP-80MB(if-wireless g)#rssi distance normal 2
Aruba Networks AP-80MB(if-wireless a)#rssi
Aruba Networks AP-80MB#
```

Radio Interface

The IEEE 802.11a and 802.11g interfaces include configuration options for radio signal characteristics and wireless security features. The configuration options are nearly identical, but depend on which interface is operating as the bridge band. Both interfaces and operating modes are covered in this section of the manual.

The AP-80 MB/SB can operate in the following modes:

- 802.11a in bridge mode and 802.11g in access point mode
- 802.11a in access point mode and 802.11g in bridge mode
- 802.11a and 802.11g both in access point mode (no bridging)
- 802.11a only in bridge or access point mode
- 802.11g only in bridge or access point mode

Note that 802.11g is backward compatible with 802.11b and can be configured to support both client types or restricted to 802.11g clients only. Both wireless interfaces are configured independently under the following web pages:

- Radio Interface A: 802.11a
- Radio Interface G: 802.11b/g



The radio channel settings for the wireless bridge are limited by local regulations, which determine the number of channels that are available.

Radio Settings

Open the Radio Settings page for the following radios:

Radio A (802.11a)— IEEE 802.11a interface operates within the 5 GHz band, at up to 54 Mbps in normal mode or up to 108 Mbps in Turbo mode.

Radio A (802.11g)— IEEE 802.11g interface operates within the 2.4 GHz band, at up to 54 Mbps in normal mode or up to 108 Mbps in Turbo mode.

Individual:

Default VLAN ID (1 ~ 4094) :

VAP 0	1
VAP 1	1
VAP 2	1
VAP 3	1

Hide SSID :

VAP 0	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VAP 1	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VAP 2	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VAP 3	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Authentication Timeout Interval (5-60) : (Mins)

VAP 0	60
VAP 1	60
VAP 2	60
VAP 3	60

Association Timeout Interval (5-60) : (Mins)

VAP 0	30
VAP 1	30
VAP 2	30
VAP 3	30

WPA2 PMKSA Life Time (1~1440) : (Mins)

VAP 0	720
VAP 1	720
VAP 2	720
VAP 3	720

Common:

Rogue AP :

AP Detection	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
AP Scan Interval (30-10080 min.)	720 (minutes)
AP Scan Duration (100-1000 milli sec.)	350 (milliseconds)
Scan AP Now	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Turbo Mode : Disable Static Dynamic

Radio Channel : 36 ch, 5.180 GHz

Auto Channel Select : Disable Enable

Transmit Power 100%

Maximum Supported Rate 54 Mbps

Maximum Association Client : 64

Antenna Gain Reduction : 0 dB

Antenna Control Method : Left

Antenna Location : Indoor

MIC Mode : Hardware Software

Super A : Disable Enable

Beacon Interval (20-1000) 100 TUs

Data Beacon Rate (DTIM) (1-255) 1 Beacons

Fragment Length (256-2346) 2346 Bytes

RTS Threshold (0-2347) 2347 Bytes

WMM : Disable Support Required

WMM Acknowledge Policy :

AC0 (Best Effect)	<input checked="" type="radio"/> Acknowledge <input type="radio"/> No Acknowledge
AC1 (Background)	<input checked="" type="radio"/> Acknowledge <input type="radio"/> No Acknowledge
AC2 (Video)	<input checked="" type="radio"/> Acknowledge <input type="radio"/> No Acknowledge
AC3 (Voice)	<input checked="" type="radio"/> Acknowledge <input type="radio"/> No Acknowledge

WMM BSS Parameters :

	AC0 (BestEffort)	AC1 (Background)	AC2 (Video)	AC3 (Voice)
logCwMin	4	4	3	2
logCwMax	10	10	4	3
AIFSN	3	7	2	2
TXOP Limit	0	0	94	47
Admission Control	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

WMM AP Parameters :

	AC0 (BestEffort)	AC1 (Background)	AC2 (Video)	AC3 (Voice)
logCwMin	4	4	3	2
logCwMax	6	10	4	3
AIFSN	3	7	1	1
TXOP Limit	0	0	94	47
Admission Control	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Key Type Hexadecimal For 64 Bit enter 10 digits, for 128 Bit enter 26 digits, for 152 Bit enter 32 digits
 Alphanumeric For 64 Bit enter 5 characters, for 128 Bit enter 13 characters, for 152 Bit enter 16 characters

VAP 0	VAP 1	VAP 2	VAP 3	Key Number	Shared Key Setup	Key
<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	Key 1	<input type="radio"/> 64 Bit <input checked="" type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input type="radio"/> None	*****
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Key 2	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Key 3	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Key 4	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	

The parameters for the 802.11a and 802.11g radios are presented as individual radio-specific settings and common settings. Each AP-80 MB/SB can support up to four virtual access points (VAPs):

Individual Radio Settings

Set the following parameters in this section:

- *Default VLAN ID*—Indicates the VLAN assigned to wireless clients that associate to this VAP but are not assigned to another VLAN. (Default: 1)
- *Hide SSID*—Causes the VAP interface to exclude the SSID from beacon messages, and prevents the VAP from responding to probe requests from clients that do not broadcast their SSID. (Default: Disable)
- *Authentication Timeout Interval*—Indicates the time by which the client must complete authentication before authentication times out. (Range: 5-60 minutes; Default: 60 minutes)
- *Association Timeout Interval*—Indicates the idle time interval (when no frames are sent) after which a client is disassociated from the VAP interface. (Range: 5-60 minutes; Default: 30 minutes)
- *WPA2 PMKSA Life Time*—Indicates the time interval after which a client's security associate and keys are deleted from the cache. WPA2 provides fast roaming for authenticated clients by retaining

keys and other security settings in a cache for each VAP. When clients roam back into a VAP they had previously been using, re-authentication is not required. When a WPA2 client is first authenticated, it receives a Pairwise Master Key (PMK) that is used to generate the other keys used for unicast data encryption. This key and other client information form a client Security Association (SA) that the VAP holds in a cache. When the WPA2 PMKSA lifetime expires, the security association and keys are deleted. If the client returns to an access point after the association has been deleted, it will require full re-authentication. (Range: 1-1440 minutes; Default: 720 minutes)

Rogue AP Settings

A rogue AP is an access point that is not authorized to participate in the wireless network or does not have the correct security configuration. Rogue APs can allow unauthorized access to the network or fool client stations into mistakenly associating with them and thereby blocking access to network resources.

The access point can be configured to periodically scan all radio channels and find other access points within range. A database of nearby access points is maintained where any rogue APs can be identified. During a scan, Syslog messages are sent for each access point detected.

Rogue access points can be identified by unknown BSSID (MAC address) or SSID configuration.



During the time that the access point is scanning a channel for rogue APs, wireless clients are not able to associate to the access point. It is best to avoid frequent or long duration scans unless there is a reason to believe that more intensive scanning is required to find a rogue AP.

- *AP Detection*—Enables the periodic scanning for other access points. (Default: Disable)
- *AP Scan Interval*—Sets the time between each rogue AP scan. (Range: 30 -10080 minutes; Default: 720 minutes)
- *AP Scan Duration*—Sets the length of time for each rogue AP scan. A long scan duration time will detect more access points in the area, but causes more disruption to client access. (Range: 100 -1000 milliseconds; Default: 350 milliseconds)
- *Rogue AP Authenticate*—Enables or disables RADIUS authentication. Enabling RADIUS Authentication allows the access point to discover rogue access points. With RADIUS authentication enabled, the access point checks the MAC address/ Basic Service Set Identifier (BSSID) of each access point that it finds against a RADIUS server to determine whether the access point is allowed. With RADIUS authentication disabled, the access point can detect its neighboring access points only; it cannot identify whether the access points are allowed or are rogues. If you enable RADIUS authentication, you must configure a RADIUS server for this access point (see “RADIUS” on page 51).
- *Scan AP Now*—Starts an immediate rogue AP scan on the radio interface. (Default: Disable)

Other Common Radio Settings

The following parameters apply to both radios:

- *Turbo Mode*—Configures the access point to operate in an enhanced proprietary modulation mode that offers connections of up to 108 Mbps instead of the 802.11a/g maximum of 54 Mbps. When Turbo is set to Static, the access point always uses Turbo mode. When Turbo is set to Dynamic, the access point uses Turbo mode only when no neighboring access points are active or detected. (Default: Disabled)
- *Radio Channel*—The radio channel that the AP-80 MB/SB uses to communicate with wireless clients. When multiple AP-80 MB/SBs are deployed in the same area, set the channel on neighboring AP-80 MB/SBs at least four channels apart to avoid interference with each other. For example, in the United States you can deploy up to four AP-80 MB/SBs in the same area (such as channels 36, 56, 149, 165). The channel for wireless clients is automatically set to the same as that used by the AP-80

MB/SB to which it is linked, and the available channel options depend on the Turbo Mode setting. (Default: Channel 60 for normal mode, and channel 42 for Turbo mode)

- *Auto Channel Select*—Enables the AP-80 MB/SB to automatically select an unoccupied radio channel. (Default: Enabled)
- *Transmit Power*—Adjusts the power of the radio signals transmitted from the AP-80 MB/SB. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (Options: 100%, 50%, 25%, 12%, minimum; Default: 100%)
- *Maximum Supported Rate*—The maximum data rate at which the access point transmits unicast packets on the wireless interface. The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance. (Options: 54, 48, 36, 24, 18, 12, 9, 6 Mbps; Default: 54 Mbps)
- *Maximum Association Client*—(Access point mode only) Sets the maximum number of clients that can be associated with the access point radio at the same time. (Range: 1-64 per radio; Default: 64)
- *Antenna Gain Reduction*—Specifies the attenuation that is automatically applied to the antenna signal.
- *Antenna Control Method*—Indicates the restriction on antenna use (left, right, or diversity). This setting applies only to the G radio and is grayed out for the A radio.
- *Antenna Location*—Selects the mounting location of the antenna in use. Selecting the correct location ensures that the access point only uses radio channels that are permitted in the country of operation. (Default: Indoor)
- *MIC Mode*—Sets the Message Integrity Check (MIC) mode. MIC is part of the Temporal Key Integrity Protocol (TKIP) encryption used in Wi-Fi Protected Access (WPA) security. The MIC calculation is performed in the access point for each transmitted packet and this can impact throughput and performance. The access point supports a choice of software or hardware MIC calculation. The performance of the access point can be improved by selecting the best method for the specific deployment. (Default: Software)
 - *Hardware*—Provides best performance when the number of supported clients is less than 27.
 - *Software*—Provides the best performance for a large number of clients on one radio interface. Throughput may be reduced when both 802.11a and 802.11g interfaces are supporting a high number of clients simultaneously.
- *Super A*—Determines whether the Atheros proprietary Super A performance enhancements are enabled for the AP. These enhancements include bursting, compression, and fast frames. Maximum throughput ranges between 40 to 60 Mbps for connections to Atheros-compatible clients. (Default: Disabled)
- *Beacon Interval*—Sets the rate at which beacon signals are transmitted from the AP-80 MB/SB. The beacon signals allow wireless clients to maintain contact with the AP-80 MB/SB. They may also carry power-management information. (Range: 20-1000 TUs; Default: 100 TUs)
- *Data Beacon Rate*—Sets the rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions. This parameter is also known also as the Delivery Traffic Indication Map (DTIM) interval. It indicates how often the MAC layer forwards broadcast/multicast traffic, which is necessary to wake up stations that are using Power Save mode. The default value of 2 indicates that the AP-80 MB/SB will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon. Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames. (Range: 1-255 beacons; Default: 2 beacons)

- *Fragment Length*— Configures the minimum packet size that can be fragmented when passing through the AP-80 MB/SB. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. (Range: 256-2346 bytes; Default: 2346 bytes)
- *RTS Threshold*—Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The AP-80 MB/SB sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

If the RTS threshold is set to 0, the AP-80 MB/SB always sends RTS signals. If set to 2347, the AP-80 MB/SB never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

The AP-80 MB/SBs contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 0-2347 bytes; Default: 2347 bytes)
- *Antenna Diversity*—There is no antenna diversity on Slave devices, and thus this field is inactive. There is antenna diversity on Master devices. Values are Dual, 1, and 2. Default is 1.

Wi-Fi Multimedia (WMM) Settings

Wi-Fi Multimedia Wireless (WMM) networks offer an equal opportunity for all devices to transmit data from any type of application. Although this is acceptable for most applications, multimedia applications (with audio and video) are particularly sensitive to the delay and throughput variations that result from this “equal opportunity” wireless access method. For multimedia applications to run well over a wireless network, a Quality of Service (QoS) mechanism is required to prioritize traffic types and provide an “enhanced opportunity” wireless access method.

The access point implements QoS using the Wi-Fi Multimedia (WMM) standard. Using WMM, the access point is able to prioritize traffic and optimize performance when multiple applications compete for wireless network bandwidth at the same time. WMM employs techniques that are a subset of the developing IEEE 802.11e QoS standard and it enables the access point to inter operate with both WMM-enabled clients and other devices that may lack any WMM functionality.

Set the following parameters in this section:

- *WMM*—Indicates the level of support for WMM: disabled, supported, or required. (Default: Disable)
- *Access Categories*—Specifies which of the access categories (ACs) applies. The categories correspond to traffic priority levels and are mapped to IEEE 802.1D priority tags (see [Table 9](#)). The direct mapping of the four ACs to 802.1D priorities is specifically intended to facilitate interoperability with other wired network QoS policies. While the four ACs are specified for specific types of traffic, WMM allows the priority levels to be configured to match any network-wide QoS policy. WMM also specifies a protocol that access points can use to communicate the configured traffic priority levels to QoS-enabled wireless clients.

Table 9 WMM Access Categories

Access Category	WMM Designation	Description	802.1D Tags
AC_VO (AC3)	Voice	Highest priority, minimum delay. Time-sensitive data such as VoIP (Voice over IP) calls.	7, 6

Table 9 WMM Access Categories (Continued)

Access Category	WMM Designation	Description	802.1D Tags
AC_VI (AC2)	Video	High priority, minimum delay. Time-sensitive data such as streaming video.	5, 4
AC_BE (AC0)	Best Effort	Normal priority, medium delay and throughput. Data only affected by long delays. Data from applications or devices that lack QoS capabilities.	0, 3
AC_BK (AC1)	Background	Lowest priority. Data with no delay or throughput requirements, such as bulk data transfers.	2, 1

- *logCWMin (Minimum Contention Window)*—The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than the CWMax value.
- *logCWMax (Maximum Contention Window)*—The maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax value must be greater or equal to the CWMin value.
- *AIFS (Arbitration Inter-Frame Space)*—The minimum amount of wait time before the next data transmission attempt. Specify the AIFS value in the range 0-15 microseconds.
- *TXOP Limit (Transmit Opportunity Limit)*—The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TxOpLimit. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-65535 microseconds.
- *Admission Control*—The admission control mode for the access category. When enabled, clients are blocked from using the access category. (Default: Disabled)

The remainder of the fields on this page related to WEP security and are described in “[Wired Equivalent Privacy \(WEP\)](#)” on page 87.

CLI Commands for the 802.11a and 802.11g Wireless Interfaces

From the global configuration mode, enter the **interface wireless g** or **interface wireless a** command to access the radio interface. The 802.11g radio can be forced to an 802.11g-only, 802.11b-only, or mixed 802.11b/g operating mode using the radio-mode command. You should set the desired operating mode before configuring channel settings (the default is mixed 802.11b/g operation). Select a radio channel or set selection to Auto using the channel command. Set any other radio settings as required before enabling the VAP interface (with the no shutdown command). To view the current 802.11 radio settings for the VAP interface, use the **show interface wireless g [0-3]** or **show interface wireless a [0-3]** command.

```

Aruba Networks AP-80MB(config)#interface wireless a
Aruba Networks AP-80MB(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Aruba Networks AP-80MB(if-wireless g)#radio-mode g
Aruba Networks AP-80MB(if-wireless g)#channel auto
Aruba Networks AP-80MB(if-wireless a)#transmit-power full
Aruba Networks AP-80MB(if-wireless a)#super-g
Aruba Networks AP-80MB(if-wireless g)#preamble short
Aruba Networks AP-80MB(if-wireless g)#

```

Security

A radio band set to access point mode is configured by default as an open system, which broadcasts a beacon signal including the configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the access point.

To improve wireless network security for access point operation, you have to implement two main functions:

- **Authentication:** It must be verified that clients attempting to connect to the network are authorized users.
- **Traffic Encryption:** Data passing between the access point and clients must be protected from interception and eavesdropping.

For a more secure network, the access point can implement one or a combination of the security mechanisms described in the following sections:

- [“Wired Equivalent Privacy \(WEP\)” on page 87](#)
- [“Wi-Fi Protected Access \(WPA\)” on page 91](#)
- [“802.1x” on page 94](#)
- [“Authentication” on page 54 \(for MAC address authentication\)](#)

The permitted security mechanisms depend on the level of security required, the network and management resources available, and the software support provided on wireless clients. A summary of wireless security considerations is listed in [Table 10](#).



Although a WEP static key is not needed for WEP over 802.1X, WPA over 802.1X, and WPA PSK modes, you must enable WEP encryption through the web or CLI in order to enable all types of encryption in the access point.

Table 10 *Wireless Security Considerations*

Security Mechanism	Client Support	Implementation Considerations
WEP	Built-in support on all 802.11a and 802.11g devices	Provides only weak security Requires manual key management
WEP over 802.1X	Requires 802.1X client support in system or by add-in software (support provided in Windows 2000 SP3 or later and Windows XP)	Provides dynamic key rotation for improved WEP security Requires configured RADIUS server 802.1X EAP type may require management of digital certificates for clients and server
MAC Address Filtering	Uses the MAC address of client network card	Provides only weak user authentication Management of authorized MAC addresses Can be combined with other methods for improved security Optionally configured RADIUS server
WPA over 802.1X Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	Provides robust security in WPA-only mode (i.e., WPA clients only) Offers support for legacy WEP clients, but with increased security risk (i.e., WEP authentication keys disabled) Requires configured RADIUS server 802.1X EAP type may require management of digital certificates for clients and server

Table 10 *Wireless Security Considerations*

Security Mechanism	Client Support	Implementation Considerations
WPA PSK Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	Provides good security in small networks Requires manual management of pre-shared key

The access point can simultaneously support clients using various different security mechanisms. The configuration for these security combinations are outlined in the following table. Note that MAC address authentication can be configured independently to work with all security mechanisms and is indicated separately in the table. Required RADIUS server support is also listed.

Table 11 *Security Combinations*

Client Security Combination	Configuration Summary ^a	MAC Authentication ^b	RADIUS Server ^c
No encryption and no authentication	Interface Detail Settings: Authentication: Open System Encryption: Disable 802.1x: Disable	Local, RADIUS, or Disabled	Yes
Static WEP only (with or without shared key authentication)	Enter 1 to 4 WEP keys Select a WEP transmit key for the interface Interface Detail Settings: Authentication: Shared Key or Open System Encryption: Enable 802.1x: Disable	Local, RADIUS, or Disabled	Yes
Dynamic WEP (802.1x) only	Interface Detail Settings: Authentication: Open System Encryption: Enable 802.1x: Required Set 802.1x key refresh and reauthentication rates	Local, RADIUS, or Disabled	Yes
802.1x WPA only	Interface Detail Settings: Authentication: WPA Encryption: Enable WPA Configuration: Required Cipher Suite: TKIP 802.1x: Required Set 802.1x key refresh and reauthentication rates	Local only	Yes
WPA Pre-Shared Key only	Interface Detail Settings: Authentication: WPA-PSK Encryption: Enable WPA Configuration: Required Cipher Configuration: TKIP 802.1x: Disable WPA Pre-shared Key Type: Hexadecimal or Alphanumeric Enter a WPA Pre-shared key	Local only	No

Table 11 *Security Combinations (Continued)*

Client Security Combination	Configuration Summary ^a	MAC Authentication ^b	RADIUS Server ^c
Static and dynamic (802.1x) WEP keys	Enter 1 to 4 WEP keys Select a WEP transmit key Interface Detail Settings: Authentication: Open System Encryption: Enable 802.1x: Supported Set 802.1x key refresh and reauthentication rates	Local, RADIUS, or Disabled	Yes
Dynamic WEP and 802.1x WPA	Interface Detail Settings: Authentication: WPA Encryption: Enable WPA Configuration: Supported Cipher Suite: WEP 802.1x: Required Set 802.1x key refresh and reauthentication rates	Local or Disabled	Yes
Static and dynamic (802.1x) WEP keys and 802.1x WPA	Enter 1 to 4 WEP keys Select a WEP transmit key Interface Detail Settings: Authentication: WPA Encryption: Enable WPA Configuration: Supported Cipher Suite: WEP 802.1x: Supported Set 802.1x key refresh and reauthentication rates	Local or Disabled	Yes
802.1x WPA2 only	Interface Detail Settings: Authentication: WPA2 Encryption: Enable WPA Configuration: Required Cipher Suite: AES-CCMP 802.1x: Required Set 802.1x key refresh and reauthentication rates	Local or Disabled	Yes
WPA2 Pre-Shared Key only	Interface Detail Settings: Authentication: WPA2-PSK Encryption: Enable WPA Configuration: Required Cipher Suite: AES-CCMP 802.1x: Disable WPA Pre-shared Key Type: Hexadicmal or Alphanumeric Enter a WPA Pre-shared key	Local or Disabled	No

Table 11 Security Combinations (Continued)

Client Security Combination	Configuration Summary ^a	MAC Authentication ^b	RADIUS Server ^c
802.1x WPA-WPA2 Mixed Mode	Interface Detail Settings: Authentication: WPA-WPA2-mixed Encryption: Enable WPA Configuration: Required Cipher Suite: TKIP 802.1x: Required Set 802.1x key refresh and reauthentication rates	Local or Disabled	Yes
WPA-WPA2 Mixed Mode Pre-Shared Key	Interface Detail Settings: Authentication: WPA-WPA2-PSK-mixed Encryption: Enable WPA Configuration: Required Cipher Suite: TKIP 802.1x: Disable WPA Pre-shared Key Type: Hexadimal or Alphanumeric Enter a WPA Pre-shared key	Local or disabled	No

- a. The configuration summary does not include the set up for MAC authentication.
- b. The configuration of RADIUS MAC authentication together with 802.1x WPA or WPA Pre-shared Key is not supported.
- c. A RADIUS server required only when RADIUS MAC authentication is configured.

Wired Equivalent Privacy (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

WEP is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. Unfortunately, WEP has been found to be seriously flawed and cannot be recommended for a high level of network security. For more robust wireless security, the access point provides Wi-Fi Protected Access (WPA) for improved data encryption and user authentication.

To configure WEP security, click **Radio settings** for the A or G radio and scroll to the bottom of the page:

Key Type Hexadecimal For 64 Bit enter **10** digits, for 128 Bit enter **26** digits, for 152 Bit enter **32** digits
 Alphanumeric For 64 Bit enter **5** characters, for 128 Bit enter **13** characters, for 152 Bit enter **16** characters

VAP 0	VAP 1	VAP 2	VAP 3	Key Number	Shared Key Setup	Key
<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	Key 1	<input type="radio"/> 64 Bit <input checked="" type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input type="radio"/> None	*****
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Key 2	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Key 3	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Key 4	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	

Setting up shared keys enables the basic IEEE 802.11 Wired Equivalent Privacy (WEP) on the access point to prevent unauthorized access to the network.

If you choose to use WEP shared keys instead of an open system, be sure to define at least one static WEP key for user authentication and data encryption. Also, be sure that the WEP shared keys are the The configuration settings for WEP are summarized below:

Key type—Specifies the type of WEP key.

- *Hexadecimal*—For 64-bit keys enter 10 hexadecimal digits, for 128-bit keys enter 26 digits, for 152-bit keys enter 32 digits.
- *ASCII*—For 64-bit enter 5 ASCII characters, for 128-bit enter 13 characters, for 152-bit enter 16 characters.
- *VAP*—Indicates the VAP to which each key applies.
- *Shared Key Setup*—Indicates the key length.
- *Key*—Specifies the WEP key. The Key index and type must match the index and type configured on the clients. In a mixed-mode environment with clients using static WEP keys and WPA, select WEP transmit key index 2, 3, or 4. The access point uses transmit key index 1 for the generation of dynamic keys.

To enable WEP shared keys for a VAP interface, click **Security** for the A or G radio, and then click **More** to display the security settings for the interface. Set the following parameters:

- *Authentication Type Setup*—Sets the access point to communicate as an open system that accepts network access attempts from any client, or with clients using pre-configured static shared keys. For WEP security, choose **Shared Key**. (Default: Open System)
 - **Shared Key**—Sets the access point to use WEP shared keys. If this option is selected, you must configure at least one key on the access point and all clients.
- *Encryption*—Enable or disable the access point to use data encryption (WEP, TKIP, or AES). If this option is selected when using static WEP keys, you must configure at least one key on the access point and all clients. You must enable data encryption through the web or CLI in order to enable all types of encryption (WEP, TKIP, or AES) in the access point. (Default: Disabled)

Table 12 WEP Configuration Settings

WEP Only	WEP Over 802.1X
Authentication Type: Shared Key WEP (encryption): Enable WPA clients only: Disable Multicast Cipher: WEP Shared Key: 64/128/152 Key Type - Hex: 10/26/32 characters ASCII: 5/13/16 characters Transmit Key: 1/2/3/4 (set index) 802.1X = Disabled ¹ MAC Authentication: Any setting ²	Authentication Type: Open System WEP (encryption): Enable WPA clients only: Disable Multicast Cipher: WEP Shared Key: 64/128 802.1X = Required ¹ MAC Authentication: Disabled/Local ²
1: See Authentication (page 54) 2: See Radius (page 51)	

CLI Commands for static WEP Shared Key Security

To enable WEP shared key security interface, use the **interface wireless g** or **interface wireless a** command from the CLI configuration mode to access the interface mode for the radio. Use the **key** command to define up to four WEP keys that can be used for all VAP interfaces on the radio. Then use the **vap** command to access each VAP interface to configure other security settings.

From the VAP interface configuration mode, use the **auth** command to enable WEP shared-key authentication, which enables encryption automatically. Then set one key as the transmit key for the

VAP interface using the **transmit-key** command. To view the current security settings, use the **show interface wireless g [0-3]** or **show interface wireless a [0-3]** command from the Exec mode.

```
Aruba Networks AP-80MB#config
Aruba Networks AP-80MB(config)#interface wireless g
Aruba Networks AP-80MB(if-wireless g)#key 1 128 ascii abcdeabcdeabc
Aruba Networks AP-80MB(if-wireless g)#vap 0
Aruba Networks AP-80MB(if-wireless g: VAP[0])#auth shared-key
Data Encryption is set to enabled.
Remember to set the share key using "key" command.
Aruba Networks AP-80MB(if-wireless g: VAP[0])#transmit-key 1
Aruba Networks AP-80MB(if-wireless g: VAP[0])#exit
Aruba Networks AP-80MB#show interface wireless g 0
Wireless Interface Information
=====
-----Identification-----
Description : Enterprise 802.11g Access Point
SSID : VAP_TEST_11G 0
Channel : 11 (AUTO)
Status : DISABLED
MAC Address : 00:12:cf:05:95:08
-----802.11 Parameters-----
Radio Mode : b & g mixed mode
Transmit Power : FULL (5 dBm)
Max Station Data Rate : 54Mbps
Multicast Data Rate : 5.5Mbps
Fragmentation Threshold : 2346 bytes
RTS Threshold : 2347 bytes
Beacon Interval : 100 TUs
Authentication Timeout Interval : 60 Mins
Association Timeout Interval : 30 Mins
DTIM Interval : 1 beacon
Preamble Length : SHORT-OR-LONG
Maximum Association : 64 stations
MIC Mode : Software
Super G : Disabled
VLAN ID : 1
-----Security-----
Closed System : Disabled
Multicast cipher : WEP
Unicast cipher : TKIP and AES
WPA clients : DISABLED
WPA Key Mgmt Mode : PRE SHARED KEY
WPA PSK Key Type : PASSPHRASE
WPA PSK Key : EMPTY
PMKSA Lifetime : 720 minutes
Encryption : ENABLED
Default Transmit Key : 1
Common Static Keys : Key 1: EMPTY Key 2: EMPTY
Key 3: EMPTY Key 4: EMPTY
Pre-Authentication : DISABLED
Authentication Type : SHARED
-----802.1x-----
802.1x : DISABLED
Broadcast Key Refresh Rate : 30 min
Session Key Refresh Rate : 30 min
802.1x Session Timeout Value : 0 min
Aruba Networks AP-80MB#
```



The index and length values used in the **key** command must be the same values used in the **encryption** and **transmit-key** commands.

CLI Commands for WEP over 802.1X Security

Use the **vap** command to access each VAP interface to configure the security settings. First set 802.1X to required using the **802.1x** command and set the 802.1X key refresh rates. Then, use the **auth** command to select open system authentication and the **encryption** command to enable data

encryption. To view the current security settings, use the **show interface wireless a [0-3]** or **show interface wireless g [0-3]** command (not shown in example).

```
Aruba Networks AP-80MB(config)#interface wireless g
Aruba Networks AP-80MB(if-wireless g)#vap 0
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1X required
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1X
broadcast-key-refresh-rate 5 7-67
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1X session-key-refresh-rate 5 7-68
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1X session-timeout 300
Aruba Networks AP-80MB(if-wireless g: VAP[0])#auth open-system
Aruba Networks AP-80MB(if-wireless g: VAP[0])#encryption
Aruba Networks AP-80MB(if-wireless g: VAP[0])#
Aruba Networks AP-80MB(config)#
```

Wi-Fi Protected Access (WPA)

WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks. The access point supports the WPA components and features described in this section.

IEEE 802.1X and the Extensible Authentication Protocol (EAP): WPA employs 802.1X as its basic framework for user authentication and dynamic key management. The 802.1X client and RADIUS server should use an appropriate EAP type—such as EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled TLS), or PEAP (Protected EAP)—for strongest authentication. Working together, these protocols provide “mutual authentication” between a client, the access point, and a RADIUS server that prevents users from accidentally joining a rogue network. Only when a RADIUS server has authenticated a user’s credentials will encryption keys be sent to the access point and client.



To implement WPA on wireless clients requires a WPA-enabled network card driver and 802.1X client software that supports the EAP authentication type that you want to use. Windows XP provides native WPA support, other systems require additional software.

Temporal Key Integrity Protocol (TKIP): WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys. Basically, TKIP starts with a master (temporal) key for each user session and then mathematically generates other keys to encrypt each data packet. TKIP provides further data encryption enhancements by including a message integrity check for each packet and a re-keying mechanism, which periodically changes the master key.

WPA Pre-Shared Key (PSK) Mode: For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.

Mixed WPA and WEP Client Support: WPA enables the access point to indicate its supported encryption and authentication mechanisms to clients using its beacon signal. WPA-compatible clients can likewise respond to indicate their WPA support. This enables the access point to determine which clients are using WPA security and which are using legacy WEP. The access point uses TKIP unicast data encryption keys for WPA clients and WEP unicast keys for WEP clients. The global encryption key for multicast and broadcast traffic must be the same for all clients, therefore it restricts encryption to a WEP key.

When access is opened to both WPA and WEP clients, no authentication is provided for the WEP clients through shared keys. To support authentication for WEP clients in this mixed mode configuration, you can use either MAC authentication or 802.1X authentication.

WPA2: WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption. The main differences and enhancements in WPA2 can be summarized as follows:

- **Advanced Encryption Standard (AES) Support:** WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. The AES-CCMP encryption cipher is specified as a standard requirement for WPA2. However, the computational intensive operations of AES-CCMP requires hardware support on client devices. Therefore to implement WPA2 in the network, wireless clients must be upgraded to WPA2-compliant hardware.
- **WPA2 Mixed-Mode:** WPA2 defines a transitional mode of operation for networks moving from WPA security to WPA2. WPA2 Mixed Mode allows both WPA and WPA2 clients to associate to a common SSID interface. In mixed mode, the unicast encryption cipher (TKIP or AES-CCMP) is negotiated for each client. The access point advertises its supported encryption ciphers in beacon frames and probe responses. WPA and WPA2 clients select the cipher they support and return the choice in the association request to the access point. For mixed-mode operation, the cipher used for broadcast frames is always TKIP. WEP encryption is not allowed.
- **Key Caching:** WPA2 provides fast roaming for authenticated clients by retaining keys and other security information in a cache, so that if a client roams away from an access point and then returns, re-authentication is not required. When a WPA2 client is first authenticated, it receives a Pairwise Master Key (PMK) that is used to generate other keys for unicast data encryption. This key and other client information form a Security Association that the access point names and holds in a cache.
- **Preauthentication:** Each time a client roams to another access point it has to be fully re-authenticated. This authentication process is time consuming and can disrupt applications running over the network. WPA2 includes a mechanism, known as pre-authentication, that allows clients to roam to a new access point and be quickly associated. The first time a client is authenticated to a wireless network it has to be fully authenticated. When the client is about to roam to another access point in the network, the access point sends pre-authentication messages to the new access point that include the client's security association information. Then when the client sends an association request to the new access point, the client is known to be already authenticated, so it proceeds directly to key exchange and association.

To configure WPA, click **Security** for Radio A or Radio G. Select one of the VAP interfaces by clicking **More**. Select one of the WPA options in the Authentication Setup table, and then configure the parameters displayed beneath the table.

Set the following WPA parameters:

- Encryption – You must enable data encryption in order to enable all types of encryption (WEP, TKIP, or AES) in the access point.
- Pre-Authentication – When using WPA2 over 802.1X, pre-authentication can be enabled, which allows clients to roam to a new access point and be quickly associated without performing full 802.1X authentication. (Default: Disabled)
- Authentication Setup – To use WPA or WPA2, set the access point to one of the following options. If a WPA/WPA2 mode that operates over 802.1X is selected (WPA, WPA2, or WPA-WPA2-mixed), the 802.1X settings and RADIUS server details need to be configured. Be sure you have also configured a RADIUS server on the network before enabling authentication. If a WPA/WPA2 Pre-shared Key mode is selected (WPA-PSK, WPA2-PSK, or WPA-WPA2 PSK-Mixed), be sure to specify the key string.
 - WPA: Clients using WPA over 802.1X are accepted for authentication.

- WPA-PSK: Clients using WPA with a Pre-shared Key are accepted for authentication.
- WPA2: Clients using WPA2 over 802.1X are accepted for authentication.
- WPA2-PSK: Clients using WPA2 with a Pre-shared Key are accepted for authentication.
- WPA-WPA2-mixed: Clients using WPA or WPA2 over 802.1X are accepted for authentication.
- WPA-WPA2-PSK-mixed: Clients using WPA or WPA2 with a Pre-shared Key are accepted for authentication.
- WPA Configuration – Each VAP interface can be configured to allow only WPA-enabled clients to access the network (Required), or to allow access to both WPA and WEP clients (Supported). (Default: Required)
- Cipher Suite – Selects an encryption method for the global key used for multicast and broadcast traffic, which is supported by all wireless clients.
 - WEP: WEP is used as the multicast encryption cipher. You should select WEP only when both WPA and WEP clients are supported.
 - TKIP: TKIP is used as the multicast encryption cipher.
 - AES-CCMP: AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2.
- WPA Pre-Shared Key Type – If the WPA or WPA2 pre-shared-key mode is used, all wireless clients must be configured with the same key to communicate with the access point.
 - Hexadecimal – Enter a key as a string of 64 hexadecimal numbers.
 - Alphanumeric – Enter a key as an easy-to-remember form of letters and numbers. The string must be from 8 to 63 characters and can include spaces.

Table 13 summarizes the WPA configuration settings.

Table 13 WPA Configuration Settings

WPA Pre-shared Key Only	WPA Over 802.1X
Authentication Type: Open System WEP (encryption): Enable ¹ WPA clients only: Enable WPA Mode: Pre-shared-key Multicast Cipher: WEP/TKIP/AES ² WPA PSK Type - Hex: 64 characters ASCII: 8-63 characters Shared Key: 64/128/152 802.1X = Disabled ³ MAC Authentication: Disabled/Local ⁴	Authentication Type: Open System WEP (encryption): Enable ¹ WPA clients only: Enable WPA Mode: WPA over 802.1X Multicast Cipher: WEP/TKIP/AES ² Shared Key: 64/128/152 802.1X = Required ³ MAC Authentication: Disabled/Local ⁴
1: Although WEP keys are not needed for WPA, you must enable WEP encryption through the WebUI or CLI in order to enable all types of encryption in the access point. For example, use the CLI encryption command to set Encryption = 64, 128 or 152, thus enabling encryption (i.e., all types of encryption) in the access point. 2: Do not use WEP unless the access point must support both WPA and WEP clients. 3: See Authentication (page 54) 4: See Radius (page 51)	

CLI Commands for WPA Pre-shared Key Security

From the VAP interface configuration mode, use the **auth wpa-psk** required command to enable WPA Pre-shared Key security. To enter a key value, use the **wpa-pre-shared-key** command to specify a

hexadecimal or alphanumeric key. To view the current security settings, use the **show interface wireless a [0-3]** or **show interface wireless g [0-3]** command (not shown in example).

```
Aruba Networks AP-80MB(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Aruba Networks AP-80MB(if-wireless g)#vap 0
Aruba Networks AP-80MB(if-wireless g: VAP[0])#wpa-pre-shared-key passphrase-key agoodsecret
Aruba Networks AP-80MB(if-wireless g: VAP[0])#auth wpa-psk required
Data Encryption is set to Enabled.
WPA2 Clients Mode is set to Disabled.
WPA Clients Mode is set to Required.
WPA Multicast Cipher is set to TKIP.
WPA Unicast Cipher can accept TKIP only.
WPA Authentication is set to Pre-Shared Key.
Aruba Networks AP-80MB(if-wireless g: VAP[0])#
```

CLI Commands for WPA over 802.1X Security

From the VAP interface configuration mode, use the **auth wpa required** command to select WPA over 802.1X security. Then set the 802.1X key refresh rates. To view the current security settings, use the **show interface wireless a [0-3]** or **show interface wireless g [0-3]** command (not shown in example).

```
Aruba Networks AP-80MB(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Aruba Networks AP-80MB(if-wireless g)#vap 0
Aruba Networks AP-80MB(if-wireless g: VAP[0])#auth wpa required
Data Encryption is set to Enabled.
WPA2 Clients mode is set to Disabled.
WPA Clients Mode is set to Required.
WPA Multicast Cipher is set to TKIP.
WPA Unicast Cipher can accept TKIP only.
WPA Authentication is set to 802.1X Required.
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1X broadcast-key-refresh-rate 5
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1X session-key-refresh-rate 5
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1X session-timeout 300 7-68
```

802.1x

IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the access point grants client access to the network.

The 802.1X EAP packets are also used to pass dynamic unicast session keys and static broadcast keys to wireless clients. Session keys are unique to each client and are used to encrypt and correlate traffic passing between a specific client and the access point. You can also enable broadcast key rotation, so the access point provides a dynamic broadcast key and changes it at a specified interval.

To configure 802.1x security, click **Security** for Radio A or Radio G. Select one of the VAP interfaces by clicking **More**. Select one of the WPA options in the Authentication Setup table, and then configure the parameters displayed beneath the table.



If 802.1X is enabled on the access point, then RADIUS setup must be completed (see [“RADIUS” on page 51](#)). To reach the RADIUS page, you can click the RADIUS link on the Security page.

Set the following parameters:

- *802.1x setup*—Determines the requirement for 802.1X use by clients. (Default: Disable)
 - *Disable*—The access point does not support 802.1X authentication for any wireless client. After successful wireless association with the access point, each client is allowed to access the network.
 - *Supported*—The access point supports 802.1X authentication only for clients initiating the 802.1X authentication process (i.e., the access point does not initiate 802.1X authentication). For clients initiating 802.1X, only those successfully authenticated are allowed to access the network. For those clients not initiating 802.1X, access to the network is allowed after successful wireless association with the access point. The 802.1X supported mode allows access for clients not using WPA or WPA2 security.
 - *Required*—The access point enforces 802.1X authentication for all associated wireless clients. If 802.1X authentication is not initiated by a client, the access point will initiate authentication. Only those clients successfully authenticated with 802.1X are allowed to access the network.
- *Broadcast Key Refresh Rate*—Sets the interval at which the broadcast keys are refreshed for stations using 802.1X dynamic keying. (Range: 0-1440 minutes; Default: 0 means disabled)
- *Session Key Refresh Rate*—The interval at which the access point refreshes unicast session keys for associated clients. (Range: 0-1440 minutes; Default: 0 means disabled)
- *802.1X Reauthentication Refresh Rate*: The time period after which a connected client must be re-authenticated. During the re-authentication process of verifying the client's credentials on the RADIUS server, the client remains connected the network. Only if re-authentication fails is network access blocked. (Range: 0-65535 seconds; Default: 0 means disabled)

AP Status

The AP Status window displays basic system configuration settings, as well as the settings for the wireless interfaces.

AP Status

AP System Configuration

Serial Number	0A80001590
System Up Time	3 days, 0 hours, 58 minutes, 29 seconds
Ethernet MAC Address	00-0B-86-C3-91-93
Radio A MAC Address	00-0B-86-39-19-10
Radio G MAC Address	00-0B-86-39-19-20
System Name	Aruba Networks AP-80B
Country Code	UNITED STATES
System Contact	Barbara Weinstein
IP Address	10.0.6.87
IP default-gateway	10.0.6.1
HTTP Server	ENABLED
HTTP Server Port	80
Software Version	v2.0.2.18b04
BootRom Version	v1.1.1
Hardware Version	R-14
Hardware Model	AP-80MB

AP System Configuration—The AP System Configuration table displays the basic system configuration settings:

- *Serial Number*—Serial number of the AP
- *System Up Time*—Length of time the management agent has been up.
- *Ethernet MAC Address*—The physical layer address for this device.
- *Radio A MAC Address*—The physical layer address for the A radio interface.
- *Radio G MAC Address*—The physical layer address for the G radio interface.
- *System Name*—Name assigned to this system.
- *Country Code*—Code for the country in which the access point is installed.
- *System Contact*—Administrator responsible for the system.
- *IP Address*—IP address of the management interface for this device.
- *IP Default Gateway*—IP address of the gateway router between this device and management stations that exist on other network segments.
- *HTTP Server*—Indication of whether management access via HTTP is enabled.
- *HTTP Server Port*—TCP port used by the HTTP interface.
- *Software Version*—Version number for the runtime code.
- *BootRom Version*—Version number for the boot ROM code.
- *Hardware Version*—Version number for the access point hardware.
- *Hardware Model*—Model number of the AP.

AP Wireless Configuration

The AP Wireless Configuration table displays the wireless interface settings listed below. Note that Radio A refers to the 802.11a interface and Radio G to the 802.11b/g interface.

- *Network Name (SSID)*—The service set identifier (SSID) or network name for this VAP.
- *Radio Channel*—The radio channel currently used on the AP-80 MB/SB.
- *Encryption*—The key size used for data encryption for each VAP.
- *Authentication Type*—Method of authentication for this VAP.
- *802.1X*—Indication of whether 802.1X access control for wireless clients is enabled or disabled for each VAP.

CLI Commands for Displaying System Settings

To view the current AP-80 MB/SB system settings, use the **show system** command from the Exec mode. To view the current radio interface settings, use the **show interface wireless a** command (see [page 201](#)).

```
Aruba Networks AP-80MB#show system

System Information
=====
Serial Number       : 0A80001590
System Up time     : 8 days, 22 hours, 47 minutes, 48 seconds
System Name        : Aruba Networks AP-80B
System Location    : Office
System Contact     : Contact
System Country Code : US - UNITED STATES
MAC Address        : 00-0B-86-C3-91-93
802.11a MAC Address : Default=00-0B-86-39-19-10   VAP1=00-0B-86-39-19-11
                   :                   VAP2=00-0B-86-39-19-12   VAP3=00-0B-86-39-19-13
802.11b/g MAC Address : Default=00-0B-86-39-19-20   VAP1=00-0B-86-39-19-21
                   :                   VAP2=00-0B-86-39-19-22   VAP3=00-0B-86-39-19-23
IP Address         : 10.0.6.87
Subnet Mask        : 255.255.255.0
Default Gateway    : 10.0.6.1
Management VLAN ID(AP) : 1
IAPP State        : ENABLED
DHCP Client       : DISABLED
HTTP Server       : ENABLED
HTTP Server Port  : 80
HTTP Session Timeout : 300 sec(s)
HTTPS Server      : ENABLED
HTTPS Server Port : 443
Slot Status       : Dual band(a/g)
Boot Rom Version  : v1.1.1
Software Version  : v2.0.2.18b04
SSH Server        : ENABLED
SSH Server Port   : 22
Telnet Server     : ENABLED
DHCP Relay        : ENABLED
=====

Aruba Networks AP-80MB#
```

Station Status

The Station Status window shows wireless clients currently associated with the access point.

Station Status

Interface A

802.11a VAP 0 Interface Statistics				
802.11a VAP 1 Interface Statistics				
802.11a VAP 2 Interface Statistics				
802.11a VAP 3 Interface Statistics				
Station Address	Authenticated	Associated	Forwarding Allowed	Key Type
VAP 0				
VAP 1				
VAP 2				
VAP 3				

Interface G

802.11g VAP 0 Interface Statistics				
802.11g VAP 1 Interface Statistics				
802.11g VAP 2 Interface Statistics				
802.11g VAP 3 Interface Statistics				
Station Address	Authenticated	Associated	Forwarding Allowed	Key Type
VAP 0				
VAP 1				
VAP 2				
VAP 3				

The Station Status page displays basic connection information for all associated stations. Note that this page is automatically refreshed every five seconds. The information is presented for the A and G interface.

- *Station Address*—MAC address of the remote AP-80 MB/SB.
- *Authenticated*—Indication of whether the station has been authenticated. The two basic methods of authentication supported for 802.11 wireless networks are “open system” and “shared key.” Open-system authentication accepts any client attempting to connect to the access point without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to stations before attempting authentication.
- *Associated*—Indication of whether station has been successfully associated with the access point.
- *Forwarding Allowed*—Indication of whether the station has passed authentication and is now allowed to forward traffic.
- *Key Type*
 - *Disabled*—Client is not using Wired Equivalent Privacy (WEP) encryption keys.
 - *Dynamic*—Client is using Wi-Fi Protected Access (802.1X or pre-shared key mode) or using 802.1X authentication with dynamic keying.
 - *Static*—Client is using static WEP keys for encryption.

CLI Commands for Displaying Station Information

To view status of clients currently associated with the access point, use the **show station** command from the Exec mode.

```

Aruba Networks AP-80MB#show station
Station Table Information
=====
if-wireless A VAP [0] / Default   :
802.11a Channel : 36

No 802.11a Channel Stations.

if-wireless G VAP [0]/ Default   :
802.11g Channel : 11

No 802.11g Channel Stations.

=====
Aruba Networks AP-80MB#

```

WDS-STP Status

The STP Status window shows network loop and link status information between WLANs and STP-compliant bridging devices.

STP information

Port Summary

Id	Priority	Path Cost	Status	State
1	128	19	Enable	Forwarding
10	128	19	Enable	Forwarding
11	128	19	Enable	Forwarding
12	128	19	Enable	Forwarding
13	128	19	Enable	Forwarding
14	128	19	Enable	Forwarding
15	128	19	Enable	Forwarding
16	128	19	Enable	Forwarding

The STP Status page displays basic system connection and configuration information. The following settings are displayed:

- *ID*—The bridge ID consists of two parts: the bridge priority (2 bytes), and the bridge MAC address (6 bytes). The 802.1d default bridge priority is 32768.
- *Bridge Priority*—Used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device, but if all devices have the same priority the device with the lowest MAC address becomes the root device. Range values are 0-65535, and the default value is 32768.
- *Path Cost*—Root path cost is the total cost of transmitting a frame onto a LAN through that port to the bridge root. Root path cost is assigned according to the bandwidth of the link. The slower the transmitting media, the higher the cost.
- *Status*—Status of the port (enabled or disabled)

CLI Commands for Displaying Station Information

To view aging time and Spanning Tree Protocol settings, use the **show bridge** command.

```

Aruba Networks AP-80MB#show bridge aging-time

Bridge Setting Information
=====
Aging time: 300
Aruba Networks AP-80MB

Aruba Networks AP-80MBshow bridge STP

Bridge STP Information
=====

Bridge MAC          : 00:0B:86:C3:91:93
Status              : Disabled
priority            : 32768
designated-root      : priority = 0, MAC = 00:00:00:00:00:00
root-path-cost      : 0
root-Port-no       : 0
Hold Time           : 1 Seconds
Hello Time          : 2 Seconds
Maximum Age         : 20 Seconds
Forward Delay       : 15 Seconds
bridge Hello Time   : 2 Seconds
bridge Maximum Age  : 20 Seconds
bridge Forward Delay : 15 Seconds
time-since-top-change: 343000 Seconds
topology-change-count: 0
Aruba Networks AP-80MB#

```

Event Logs

The Event Logs window shows the log messages generated by the AP-80 MB/SB and stored in memory.

Event Logs

1	Aug 16 10:13:05	Information: Get time from SNTP Server Fail
2	Aug 16 10:13:05	Information: Get time from SNTP Server Fail
3	Aug 15 22:13:05	Information: Get time from SNTP Server Fail
4	Aug 15 22:13:05	Information: Get time from SNTP Server Fail
5	Aug 15 10:13:05	Information: Get time from SNTP Server Fail
6	Aug 15 10:13:05	Information: Get time from SNTP Server Fail
7	Aug 14 22:13:05	Information: Get time from SNTP Server Fail
8	Aug 14 22:13:05	Information: Get time from SNTP Server Fail
9	Aug 14 10:13:05	Information: Sync time from SNTP Server Successfully
10	Aug 14 10:12:53	Information: Get time from SNTP Server Fail
11	Aug 13 22:12:53	Information: Get time from SNTP Server Fail
12	Aug 13 22:12:53	Information: Get time from SNTP Server Fail
13	Aug 13 18:35:33	Information: SSH task - terminated SSH session.
14	Aug 13 18:20:33	Information: SSH task - created SSH session.
15	Aug 13 10:28:03	Information: SSH task - terminated SSH session.
16	Aug 13 10:13:03	Information: SSH task - created SSH session.
17	Aug 13 10:12:54	Information: Get time from SNTP Server Successfully
18	Jan 01 00:00:00	Information: Get time from SNTP Server Fail
19	Jan 01 00:00:00	Notice: System Up
20	Jan 01 00:00:00	Information: Enable Telnet.
21	Jan 01 00:00:00	Notice: Auto Channel Scan selected 5180 MHz, channel 36

CLI Commands for Displaying the Event Logs

From the global configuration mode, use the **show logging** command.

```
Aruba Networks AP-80MB#show logging

Logging Information
=====
Syslog State           : Enabled
Logging Host State     : Enabled
Logging Console State  : Enabled
Server Domain name/IP : 192.168.1.19
Logging Level          : Alert
Logging Facility Type  : 16
=====

Aruba Networks AP-80MB#
```


Using the Command Line Interface

When accessing the management interface for the wireless bridge via a Telnet connection, the wireless bridge can be managed by entering command keywords and parameters at the prompt. Using the wireless bridge's command line interface (CLI) is very similar to entering commands on a UNIX system.

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, if the wireless bridge cannot acquire an IP address from a DHCP server, the default IP address used by the wireless bridge, 192.168.1.1, consists of a network portion (192.168.1) and a host portion (1).

To access the wireless bridge through a Telnet session, you must first set the IP address for the wireless bridge, and set the default gateway if you are managing the wireless bridge from a different IP subnet. For example:

```
Aruba Networks AP-80MB#configure
Aruba Networks AP-80MB(config)#interface ethernet
Aruba Networks AP-80MB(if-ethernet)#ip address 10.1.0.1 255.255.255.0 10.1.0.254
Aruba Networks AP-80MB(if-ethernet)#
```

After you configure the wireless bridge with an IP address, you can open a Telnet session by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI displays the `Aruba Networks AP-80MB#` prompt to show that you are using executive (Exec) access mode.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the **quit** or **exit** command.

After entering the Telnet command, the login screen opens. Log in using the username `admin` and no password.

```
Username: admin
Password:
Aruba Networks AP-80MB#
```

Entering Commands



You can open up to four sessions to the device via Telnet.

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command **show interface ethernet**, **show** and **interface** are keywords, and **ethernet** is an argument that specifies the interface type.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Aruba Networks AP-80MB(config)#username smith
```

Minimum Abbreviation

The CLI accepts a minimum number of characters that uniquely identify a command. For example, the command **configure** can be entered as **con**. If an entry is ambiguous, the system prompts for further input.

Command Completion

If you terminate input with a Tab key, the CLI prints the remaining characters of a partial keyword up to the point of ambiguity. For example, typing **con** followed by a tab results in printing the command **configure**.

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by following a command with the **?** character to list keywords or parameters.

Showing Commands

If you enter a **?** at the command prompt, the system displays the first level of keywords for the current configuration mode (Exec, Global Configuration, or Interface). You can also display a list of valid keywords for a specific command. For example, the command **show ?** displays a list of possible show commands:

```
Aruba Networks AP-80MB#show ?
  authentication      Show Authentication parameters
  bootfile            Show bootfile name
  bridge              Show bridge table
  filters             Show filters
  hardware            Show hardware version
  history             Display the session history
  interface           Show interface information
  line                TTY line information
  logging             Show the logging buffers
  memory-allocation  Show memory allocation
  radius              Show radius server
```


snmp	Show snmp statistics
sntp	Show sntp statistics
station	Show 802.11 station table
system	Show system information
version	Show system version
wds	Show wds table

The command **show interface ?** displays the following information:

```
Aruba Networks AP-80MB#show interface ?
  ethernet Show Ethernet interface
  wireless Show wireless interface
  <cr>
Aruba Networks AP-80MB#show interface
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example **s?** shows all the keywords starting with **s**.

```
Aruba Networks AP-80MB#show s?
snmp      sntp      station system
Aruba Networks AP-80MB#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword **no** to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command logs system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Use the **show history** command to display a longer list of recently-executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark **?** at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table.

Table 14 *Command Modes and Classes*

Class	Mode
Exec	Privileged
Configuration	Global Interface-ethernet Interface-wireless

Exec Commands

When you open a new console session on the wireless bridge, the system enters Exec command mode. Only a limited number of the commands are available in this mode. You can access all other commands only from the configuration mode. To access Exec mode, open a new console session with the user name **admin**. The command prompt displays as “Aruba Networks AP-80MB#” for Exec mode.

```
Username: admin
Password: [system login password]
Aruba Networks AP-80MB#
```

Configuration Commands

Configuration commands are used to modify wireless bridge settings. These commands modify the running configuration and are saved in memory.

The configuration commands are organized into three different modes:

- **Global Configuration**—These commands modify the system level configuration, and include commands such as **username** and **password**.
- **Interface-Ethernet Configuration**—These commands modify the Ethernet port configuration, and include command such as **dns** and **ip**.
- **Interface-Wireless Configuration**—These commands modify the wireless port configuration, and include command such as **channel** and **encryption**.

To enter the Global Configuration mode, enter the command **configure** in Exec mode. The system prompt changes to “Aruba Networks AP-80MB(config)#” which gives you access privilege to all Global Configuration commands.

```
Aruba Networks AP-80MB#configure
Aruba Networks AP-80MB(config)#
```

To enter Interface mode, you must enter the **interface ethernet** or **interface wireless a** command while in Global Configuration mode. The system prompt changes to “Aruba Networks AP-80MB(if-ethernet)#,” or “Aruba Networks AP-80MB(if-wireless a)” indicating that you have access privileges to the associated commands. You can use the **end** command to return to the Exec mode.

```
Aruba Networks AP-80MB(config)#interface ethernet
Aruba Networks AP-80MB(if-ethernet)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the ? character to display a list of possible matches. You can also use the following editing keystrokes for command line processing:

Table 15 *Command Line Keystrokes*

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates a task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes from cursor to the end of the command line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Shows the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor backward one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Table 16 *System Command Groups*

Command Group	Description
General Commands	Includes basic commands for entering configuration mode, restarting the system, or quitting the CLI
System Management Commands	Controls user name, password, browser management options, and a variety of other system information
System Logging Commands	Configures system logging parameters
System Clock Commands	Configures SNTP and system clock settings

Table 16 System Command Groups (Continued)

Command Group	Description
DHCP Relay Commands	Configures settings to sending DHCP address requests to a DHCP server
SNMP Commands	Configures community access strings and trap managers
Flash/File Commands	Manages code image or wireless bridge configuration files
RADIUS Client Commands	Configures the RADIUS client used with 802.1x authentication
802.1x Authentication Commands	Configures IEEE 802.1x port access control and address filtering
MAC Address Authentication Commands	Configures MAC authentication on the access point
Filtering Commands	Controls filters for access to the management interface from wireless nodes, and filters traffic using specific Ethernet protocol types
WDS Bridge Commands	Sets the operation mode for each access point interface and configures Wireless Distribution System (WDS) forwarding table settings
Ethernet Interface Commands	Configures connection parameters for the Ethernet interface
Wireless Interface Commands	Configures connection parameters for the wireless interface
Rogue AP Detection Commands	Configure settings to detect access points that are not authorized to participate in the wireless network or that do not have the correct security configuration
Link Integrity Commands	Configures link check to a host device on the wired network
IAPP Commands	Enables roaming between multi-vendor access points
VLAN Commands	Configures VLAN membership
WMM Commands	Configures VLAN support

The access mode shown in the following tables is indicated by these abbreviations: **GC** (Global Configuration), **IC-E** (Ethernet Interface Configuration), and **IC-W** (Wireless Interface Configuration).

General Commands

The general commands are used to interact with the CLI, contact other systems, and display history and console port settings.

Table 17 System General Commands and Functions

Command	Function	Mode
configure	Activates global configuration mode	Exec
end	Returns to the previous configuration mode	GC, IC
exit	Returns to Exec mode, or exits the CLI	any
ping	Sends ICMP echo request packets to another node on the network	Exec
reset	Restarts the system	Exec

Table 17 System General Commands and Functions (Continued)

Command	Function	Mode
<code>show history</code>	Shows the command history buffer	Exec
<code>show line</code>	Shows the configuration settings for the console port	Exec

configure

This command activates Global Configuration mode. You must enter this mode to modify most of the settings on the wireless bridge. You must also enter Global Configuration mode prior to enabling the context modes for Interface Configuration. See [“Using the Command Line Interface” on page 103](#).

Default Setting

None

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#configure
Aruba Networks AP-80MB(config)#
```

end

This command returns to the previous configuration mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration

Example

This example shows how to return to the Configuration mode from the Interface Configuration mode:

```
Aruba Networks AP-80MB(if-ethernet)#end
Aruba Networks AP-80MB(config)#
```

exit

This command returns to the Exec mode or exits the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Exec mode from the Interface Configuration mode, and then quit the CLI session:

```
Aruba Networks AP-80MB(if-ethernet)#exit
Aruba Networks AP-80MB#exit
CLI session with the wireless bridge is now closed
Username:
```

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

```
ping <host_name> | <ip_address>
```

- *host_name* - Alias of the host
- *ip_address* - IP address of the host

Default Setting

None

Command Mode

Exec

Command Usage

Use the ping command to see if another site on the network can be reached.

The following are some results of the ping command:

- *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
- *Destination does not respond* - If the host does not respond, a timeout appears in ten seconds.
- *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
- *Network or host unreachable* - The gateway found no corresponding entry in the route table. Press Esc to stop pinging.

Example

This command sends packets to address **10.1.0.19**:

```
Aruba Networks AP-80MB#ping 10.1.0.19
192.168.1.19 is alive
```

reset

This command restarts the system or restores the factory default settings.

Syntax

```
reset {board | configuration}
```

- **board** - Reboots the system
- **configuration** - Resets the configuration settings to the factory defaults, and then reboots the system

Default Setting

None

Command Mode

Exec

Command Usage

When the system is restarted, it always runs the Power-On Self-Test.

Example 1

This example shows how to reset the system:

```
Aruba Networks AP-80MB#reset board
Reboot system now? <y/n>: y
```

Example 2

This example shows how to restore the factory default settings:

```
Aruba Networks AP-80MB#reset configuration
Reset to Factory Defaults now? <y/n>: y
Restoring factory defaults, please wait...
Factory defaults are set.
```

show history

This command shows the contents of the command history buffer.

Syntax

```
show history
```

Command Mode

Exec

Command Usage

The history buffer size is fixed at 10 commands.

Use the up or down arrow keys to scroll through the commands in the history buffer.

Example

This example lists the contents of the command history buffer:

```
Aruba Networks AP-80MBshow history
History Command
```

```

=====
show history
ping 10.0.0.0
show history
=====
Aruba Networks AP-80MB

```

show line

This command displays the console port's configuration settings.

Syntax

```
show line
```

Command Mode

Exec

Example

```

Aruba Networks AP-80MBshow line
Console Line Information
=====
databits   : 8
parity     : none
speed      : 9600
stop bits  : 1
=====

```

System Management Commands

These commands are used to configure the user name, password, browser management options, and a variety of other system information.

Table 18 System Management Commands and Functions

Command	Function	Mode
<i>Country Setting</i>		
country	Sets the wireless bridge country code for correct radio operation	Exec
<i>Device Designation</i>		
prompt	Customizes the command line prompt	GC
system name	Specifies the host name for the wireless bridge	GC
snmp-server contact	Sets the system contact string	GC
snmp-server location	Sets the system location string	GC
<i>Management Access</i>		
APmgmtIP	Specifies an IP address or range of addresses allowed access to the management interface	GC
APmgmtUI	Enables or disables SNMP, Telnet or web management access	GC

Table 18 System Management Commands and Functions (Continued)

Command	Function	Mode
<code>ip ssh-server enable</code>	Enables the Secure Shell server	IC-E
<code>ip ssh-server port</code>	Sets the Secure Shell port	IC-E
<code>ip telnet-server enable</code>	Enables the Telnet server	IC-E
<code>password</code>	Specifies the password for management access	GC
<code>show apmanagement</code>	Shows the AP management configuration	EXEC
<code>username</code>	Configures the user name for management access	GC
<i>Web Server</i>		
<code>ip http port</code>	Specifies the port to be used by the web browser interface	GC
<code>ip http server</code>	Allows the wireless bridge to be monitored or configured from a browser	GC
<code>ip http session-timeout</code>	Sets the timeout for the web browser interface	GC
<code>ip https port</code>	Specifies the UDP port number used for a secure HTTP connection to the access point's Web interface	GC
<code>ip https server</code>	Enables the secure HTTP server on the access point	GC
<i>System Status</i>		
<code>show hardware</code>	Displays the access point's hardware version	Exec
<code>show system</code>	Displays system information	Exec
<code>show version</code>	Displays version information for the system	Exec

country

This command configures the wireless bridge's country code, which identifies the country of operation and sets the authorized radio channels.

Syntax

country <country_code>

- *country_code* - A two character code that identifies the country of operation. See the following table for a full list of codes.

Table 19 Country Command Codes

Country	Code	Country	Code	Country	Code	Country	Code
Albania	AL	Dominican Republic	DO	Kuwait	KW	Romania	RO
Algeria	DZ	Ecuador	EC	Latvia	LV	Russia	RU
Argentina	AR	Egypt	EG	Lebanon	LB	Saudi Arabia	SA
Armenia	AM	Estonia	EE	Liechtenstein	LI	Singapore	SG
Australia	AU	Finland	FI	Lithuania	LT	Slovak Republic	SK

Table 19 Country Command Codes (Continued)

Country	Code	Country	Code	Country	Code	Country	Code
Austria	AT	France	FR	Luxembourg	LU	Slovenia	SI
Azerbaijan	AZ	Georgia	GE	Macao	MO	South Africa	ZA
Bahrain	BH	Germany	DE	Macedonia	MK	Spain	ES
Belarus	BY	Greece	GR	Malaysia	MY	Sweden	SE
Belgium	BE	Guatemala	GT	Mexico	MX	Switzerland	CH
Belize	BZ	Hong Kong	HK	Monaco	MC	Syria	SY
Bolivia	BO	Hungary	HU	Morocco	MA	Taiwan	TW
Brazil	BR	Iceland	IS	Netherlands	NL	Thailand	TH
Brunei Darussalam	BN	India	IN	New Zealand	NZ	Turkey	TR
Bulgaria	BG	Indonesia	ID	Norway	NO	Ukraine	UA
Canada	CA	Iran	IR	Oman	OM	United Arab Emirates	AE
Chile	CL	Ireland	IE	Pakistan	PK	United Kingdom	GB
China	CN	Israel	IL	Panama	PA	United States	US
Colombia	CO	Italy	IT	Peru	PE	Uruguay	UY
Costa Rica	CR	Japan	JP	Philippines	PH	Venezuela	VE
Croatia	HR	Jordan	JO	Poland	PL	Vietnam	VN
Cyprus	CY	Kazakhstan	KZ	Portugal	PT		
Czech Republic	CZ	North Korea	KP	Puerto Rico	PR		
Denmark	DK	Korea Republic	KR	Qatar	QA		
Albania	AL	Dominican Republic	DO	Kuwait	KW	Romania	RO

Default Setting

US - for units sold in the United States

99 (no country set) - for units sold in other countries

Command Mode

Exec

Command Usage

If you purchased an wireless bridge outside of the United States, the country code must be set before radio functions are enabled.

The available Country Code settings can be displayed by using the **country ?** command.

Example

This example sets the country code to **US**.

```
Aruba Networks AP-80MB#country us
```

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

```
prompt <string>  
no prompt
```

- *string* - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

Aruba Networks AP-80MB

Command Mode

Global Configuration

Example

This commands sets the prompt to **RD2**:

```
Aruba Networks AP-80MB(config)#prompt RD2  
RD2(config)#
```

system name

This command specifies or modifies the system name for this device. Use the **no** form to restore the default system name.

Syntax

```
system name <name>  
no system name
```

- *name* - The name of this host (maximum length: 32 characters)

Default Setting

Outdoor Bridge

Command Mode

Global Configuration

Example

This command sets the system name to **bridge-link**:

```
Aruba Networks AP-80MB(config)#system name bridge-link  
bridge-link(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

```
snmp-server contact <string>  
no snmp-server contact
```

- *string* - String that describes the system contact (maximum length: 255 characters)

Default Setting

Contact

Command Mode

Global Configuration

Example

This example sets the system contact to **Paul**.

```
Aruba Networks AP-80MB(config)#snmp-server contact Paul
```

Related Commands

snmp-server location (6-116)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

```
snmp-server location <text>  
no snmp-server location
```

- *text* - String that describes the system location (maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

This example sets the SNMP system location to building-1.

```
Aruba Networks AP-80MB(config)#snmp-server location building-1
```

Related Commands

snmp-server contact (6-115)

APmgmtIP

This command specifies the client IP addresses that are allowed to have management access to the access point through various protocols. Secure Web (HTTPS) connections are not affected by the UI Management or IP Management settings.

Syntax

```
APmgmtIP <multiple IP_address subnet mask | single IP_address | any>
```

- **multiple** - IP addresses within a specifiable range allowed.
- **single** - individual IP address allowed.
- **any** - all IP addresses allowed
- *IP_address* - IP addresses to the SNMP, web and Telnet groups.
- *subnet_mask* - Specifies a range of IP addresses allowed management access.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- If anyone tries to access a management interface on the access point from an invalid address, the unit will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the access point will not accept overlapping address ranges. When entering addresses for different groups, the access point will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Aruba Networks AP-80MB(config)#apmgmtip multiple 192.168.1.50 255.255.255.0
Aruba Networks AP-80MB(config)#
```

APmgmtUI

This command enables and disables management access to the access point through SNMP, Telnet and web interfaces.



Secure Web (HTTPS) connections are not affected by the UI Management or IP Management settings.

Syntax

```
APmgmtUI {[SNMP | Telnet | Web] enable | disable}
```

- **SNMP** - Specifies SNMP management access.
- **Telnet** - Specifies Telnet management access.
- **Web** - Specifies web based management access.
- **enable/disable** - Enables or disables the selected management access method.

Default Setting

All enabled

Command Mode

Global Configuration

Example

This example restricts management access to the indicated addresses.

```
Aruba Networks AP-80MB(config)#apmgmtui SNMP enable
Aruba Networks AP-80MB(config)#
```

ip ssh-server enable

This command enables the Secure Shell (SSH) server. Use the no form to disable the server.

Syntax

```
ip ssh-server enable
no ip ssh-server
```

Default Setting

Interface enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The access point supports Secure Shell version 2.0 only.
- After boot up, the SSH server needs about two minutes to generate host encryption keys. The SSH server is disabled while the keys are being generated.

Example

This example enables the SSH server.

```
Aruba Networks AP-80MB(if-ethernet)#ip ssh-server enable
Aruba Networks AP-80MB(if-ethernet)#
```

ip ssh-server port

This command sets the Secure Shell server port. Use the no form to disable the server.

Syntax

```
ip ssh-server port <port-number>
```

- *port-number*—The UDP port used by the SSH server. (Range: 1-65535)

Default Setting

22

Command Mode

Interface Configuration (Ethernet)

Example

This example enables the SSH server and sets the port to **1124**.

```
Aruba Networks AP-80MB(if-ethernet)#ip ssh-server enable
Aruba Networks AP-80MB(if-ethernet)#
Aruba Networks AP-80MB(if-ethernet)#ip ssh-server port 1124
Aruba Networks AP-80MB(if-ethernet)#
```

ip telnet-server enable

This command enables the Telnet server. Use the no form to disable the server.

Syntax

```
ip telnet-server enable
no ip telnet-server
```

Default Setting

Interface enabled

Command Mode

Interface Configuration (Ethernet)

Example

This example enables the Telnet server.

```
Aruba Networks AP-80MB(if-ethernet)#ip telnet-server enable
Aruba Networks AP-80MB(if-ethernet)#
```

password

Sets the password for access to the CLI and web interface. After initially logging onto the system, you should set the password. Remember to record it in a safe place. Use the **no** form to reset the default password.

Syntax

```
password <password>  
no password
```

- *password* - Password for management access (length: 3-16 characters, case sensitive)

Default Setting

null

Command Mode

Global Configuration

Example

This example sets the administrative password to **adminpwd**.

```
Aruba Networks AP-80MB(config)#password adminpwd
```

show apmanagement

This command shows the AP management configuration, including the IP addresses of management stations allowed to access the access point, as well as the interface protocols which are open to management access.

Syntax

```
show apmanagement
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show apmanagement  
Management AP Information  
=====  
AP Management IP Mode: Any IP  
Telnet UI: Enable  
WEB UI : Enable  
SNMP UI : Enable  
=====  
Aruba Networks AP-80MB#
```

username

This command configures the user name for management access.

Syntax

```
username <name>
```

- *name* - The name of the user (length: 3-16 characters, case sensitive)

Default Setting

admin

Command Mode

Global Configuration

Example

This example sets the administrative user name to **bob**.

```
Aruba Networks AP-80MB(config)#username bob
```

ip http port

This command specifies the TCP port number used by the web interface. Use the **no** form to use the default port.

Syntax

```
ip http port <port-number>  
no ip http port
```

- *port-number*—The TCP port to be used by the browser interface (range: 1024-65535)

Default Setting

80

Command Mode

Global Configuration

Example

This example sets the port for the web interface to **1143**.

```
Aruba Networks AP-80MB(config)#ip http port 1143
```

Related Commands

```
ip http server (6-122)
```

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

```
ip http server
no ip http server
```

Default Setting

Enabled

Command Mode

Global Configuration

Example

This example enables the HTTP server.

```
Aruba Networks AP-80MB(config)#ip http server
```

Related Commands

ip http port (6-121)

ip http session-timeout

This command sets the time limit for an idle web interface session.

Syntax

```
ip http session-timeout <time>
```

- *time* - Sets the web interface session timeout. (Range: 0 - 1800 seconds, 0 means disabled)

Default Setting

300

Command Mode

Global Configuration

Example

This example sets the session timeout to **600** seconds (10 minutes).

```
Aruba Networks AP-80MB(config)#ip http session-timeout 600
Aruba Networks AP-80MB(config)#
```

Related Commands

ip http port (7-17)

ip https port

Use this command to specify the UDP port number used for HTTPS/SSL connection to the access point's Web interface. Use the no form to restore the default port.

Syntax

```
ip https port <port_number>
no ip https port
```

- *port_number* – The UDP port used for HTTPS/SSL. (Range: 80, 1024-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- To avoid using common reserved TCP port numbers below 1024, the configurable range is restricted to 443 and between 1024 and 65535.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:

```
https://device:port_number
```

Example

This example sets the HTTPS port to **1234**.

```
Aruba Networks AP-80MB(config)#ip https port 1234
Aruba Networks AP-80MB(config)#
```

ip https server

Use this command to enable the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the access point's Web interface. Use the no form to disable this function.

Syntax

```
ip https server
no ip https server
```

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently.
- If you enable HTTPS, you must indicate this in the URL:

```
https://device:port_number]
```

- When you start HTTPS, the connection is established in this way:
 - The client authenticates the server using the server's digital certificate.
 - The client and server negotiate a set of security protocols to use for the connection.
 - The client and server generate session keys for encrypting and decrypting data.
 - The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for Internet Explorer 5.x.

Example

This example enables the HTTPS server.

```
Aruba Networks AP-80MB(config)#ip https server
Aruba Networks AP-80MB(config)#
```

show hardware

This command displays the system hardware version.

Syntax

```
show hardware
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show hardware
Hardware Version Information
=====
Hardware version R01
=====
Aruba Networks AP-80MB#
```

show system

This command displays basic system configuration settings.

Default Setting

None

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show system
System Information
=====
Serial Number       : 0000000000
System Up time     : 0 days, 0 hours, 17 minutes, 2 seconds
System Name        : Dual Band Outdoor AP
System Location    :
```

```

System Contact      : Contact
System Country Code : TW - TAIWAN
MAC Address         : 00-03-7F-E0-06-EA
IP Address          : 192.168.1.1
Subnet Mask         : 255.255.255.0
Default Gateway     : 0.0.0.0
VLAN State          : DISABLED
Native VLAN ID      : 1
IAPP State          : ENABLED
DHCP Client         : ENABLED
HTTP Server         : ENABLED
HTTP Server Port    : 80
Slot Status         : Dual band(a/g)
Software Version    : v1.1.2.1B05
=====
Aruba Networks AP-80MB#

```

show version

This command displays the software version for the system.

Syntax

```
show version
```

Command Mode

Exec

Example

```

Aruba Networks AP-80MB#show version
Version v1.1.2.1B05

```

System Logging Commands

These commands are used to configure system logging on the wireless bridge.

Table 20 System Logging Commands

Command	Function	Mode
<code>logging clear</code>	Clears all log entries in access point memory	GC
<code>logging console</code>	Initiates logging of error messages to the console	GC
<code>logging facility-type</code>	Sets the facility type for remote logging of syslog messages	GC
<code>logging host</code>	Adds a syslog server host IP address that will receive logging messages	GC
<code>logging level</code>	Defines the minimum severity level for event logging	GC
<code>logging on</code>	Controls logging of error messages	GC
<code>show event-log</code>	Displays all the log entries in access point memory	Exec
<code>show logging</code>	Displays the state of logging	Exec

logging clear

This command clears all log messages stored in the access point's memory.

Syntax

```
logging clear
```

Command Mode

Global Configuration

Example

This example clears all log messages.

```
Aruba Networks AP-80MB(config)#logging clear
Aruba Networks AP-80MB(config)#
```

logging console

This command initiates logging of error messages to the console. Use the **no** form to disable logging to the console.

Syntax

```
logging console
no logging console
```

Default Setting

Disabled

Command Mode

Global Configuration

Example

This example starts sending error messages to the system console.

```
Aruba Networks AP-80MB(config)#logging console
```

logging facility-type

This command sets the facility type for remote logging of syslog messages.

Syntax

```
logging facility-type <type>
```

- *type* - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service (range: 16-23)

Default Setting

16

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the wireless bridge. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

This example sets the facility type for remote logging to **19**.

```
Aruba Networks AP-80MB(config)#logging facility 19
```

logging host

This command specifies a syslog server host that will receive logging messages. Use the **no** form to remove syslog server host.

Syntax

```
logging host <host_name> | <host_ip_address>  
no logging host
```

- *host_name* - The name of a syslog server (range: 1-20 characters)
- *host_ip_address* - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Example

This example assigns **10.1.0.3** as the host to receive log messages.

```
Aruba Networks AP-80MB(config)#logging host 10.1.0.3
```

logging level

This command sets the minimum severity level for event logging.

Syntax

```
logging level {Emergency | Alert | Critical | Error | Warning | Notice |  
Informational | Debug}
```

- **Emergency** - System unusable
- **Alert** - Immediate action needed
- **Critical** - Serious conditions (for example, memory allocation, or free memory error - resource exhausted)
- **Error** - Conditions that interfere with system operation (for example, invalid input, default used)
- **Warning** - Conditions about unexpected behavior or responses (for example, return false, unexpected return)
- **Notice** - Conditions that are normal but noteworthy, such as cold start

- **Informational** - Messages that contain useful information
- **Debug** - Messages that may help in troubleshooting

Default Setting

Error

Command Mode

Global Configuration

Command Usage

Messages sent include the selected level down to the Emergency level.

Example

This example sets the minimum log level to **alert**.

```
Aruba Networks AP-80MB(config)#logging level alert
```

logging on

This command controls logging of error messages (sending debug or error messages to memory). The **no** form disables the logging process.

Syntax

```
logging on  
no logging on
```

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to memory. You can use the **logging level** command to control the type of error messages that are stored in memory.

Example

This example enables error message logging.

```
Aruba Networks AP-80MB(config)#logging on
```

show event-log

This command displays log messages stored in the access point's memory.

Syntax

```
show event-log
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show event-log
Mar 09 11:57:55 Information: 802.11g:11g Radio Interface Enabled
Mar 09 11:57:55 Information: 802.11g:Radio channel updated to 8
Mar 09 11:57:34 Information: 802.11g:11g Radio Interface Enabled
Mar 09 11:57:18 Information: 802.11g:11g Radio Interface Enabled
Mar 09 11:56:35 Information: 802.11a:11a Radio Interface Enabled
Mar 09 11:55:52 Information: SSH task: Set SSH server port to 22
Mar 09 11:55:52 Information: SSH task: Enable SSH server.
Mar 09 11:55:52 Information: Enable Telnet.
Mar 09 11:55:40 Information: 802.11a:11a Radio Interface Disabled
Mar 09 11:55:40 Information: 802.11a:Transmit Power set to QUARTER
Press <n> next. <p> previous. <a> abort. <y> continue to end :
Aruba Networks AP-80MB#configure
Enter configuration commands, one per line. End with CTRL/Z
Aruba Networks AP-80MB(config)#
```

show logging

This command displays the logging configuration.

Syntax

```
show logging
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show logging

Logging Information
=====
Syslog State           : Disabled
Logging Host State     : Enabled
Logging Console State  : Disabled
Server Domain name/IP : none
Logging Level          : Error
Logging Facility Type  : 16
=====
```

System Clock Commands

These commands are used to configure SNTP and system clock settings on the wireless bridge.

Table 21 System Clock Commands and Functions

Command	Function	Mode
<code>sntp-server date-time</code>	Manually sets the system date and time	GC
<code>sntp-server daylight-saving</code>	Sets the start and end dates for daylight savings time	GC
<code>sntp-server enable</code>	Accepts time from the specified time servers	GC

Table 21 System Clock Commands and Functions (Continued)

Command	Function	Mode
<code>sntp-server ip</code>	Specifies one or more time servers	GC
<code>sntp-server timezone</code>	Sets the time zone for the wireless bridge's internal clock	GC
<code>show sntp</code>	Shows current SNTP configuration settings	Exec

sntp-server date-time

This command sets the system clock. When you enter the command, the system prompts you to enter values.

Syntax

```
sntp-server date-time
```

Default Setting

00:14:00, January 1, 1970

Command Mode

Global Configuration

Example

This example sets the system clock to **17:37 June 19, 2007**.

```
Aruba Networks AP-80MB(config)#sntp-server date-time
Enter Year<1970-2100>: 2007
Enter Month<1-12>: 6
Enter Day<1-31>: 19
Enter Hour<0-23>: 17
Enter Min<0-59>: 37
Aruba Networks AP-80MB(config)#
```

Related Commands

`sntp-server enable` (6-131)

sntp-server daylight-saving

This command sets the start and end dates for daylight savings time. Use the **no** form to disable daylight savings time. When you enter the command, the system prompts you to enter values.

Syntax

```
sntp-server daylight-saving
no sntp-server daylight-saving
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The command sets the system clock back one hour during the specified period.

Example

This example sets daylight savings time to be used from July 1st to September 1st.

```
Aruba Networks AP-80MB(config)#sntp-server daylight-saving
Enter Daylight saving from which month<1-12>: 6
and which day<1-31>: 1
Enter Daylight saving end to which month<1-12>: 9
and which day<1-31>: 1
Aruba Networks AP-80MB(config)#
```

sntp-server enable

This command enables SNTP client requests for time synchronization with NTP or SNTP time servers specified by the **sntp-server ip** command. Use the **no** form to disable SNTP client requests.

Syntax

```
sntp-server enable
no sntp-server enable
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the wireless bridge only records the time starting from the factory default set at the last bootup (for example, 00:14:00, January 1, 2005).

Example

This example enables the SNTP server.

```
Aruba Networks AP-80MB(config)#sntp-server enable
```

Related Commands

sntp-server ip (6-132)
show sntp (6-133)

sntp-server ip

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

```
sntp-server ip {1 | 2 | <ip>}
```

- **1** - First time server
- **2** - Second time server
- *ip* - IP address of an time server (NTP or SNTP)

Default Setting

137.92.140.80
192.43.244.18

Command Mode

Global Configuration

Command Usage

When SNTP client mode is enabled using the `sntp-server enable` command, the `sntp-server ip` command specifies the time servers from which the wireless bridge polls for time updates. The wireless bridge polls the time servers in the order specified until a response is received.

Example

This example sets the SNTP server IP address to **10.1.0.19**.

```
Aruba Networks AP-80MB(config)#sntp-server ip 10.1.0.19
```

Related Commands

`sntp-server enable` (6-131)
`show sntp` (6-133)

sntp-server timezone

This command sets the time zone for the wireless bridge's internal clock.

Syntax

```
sntp-server timezone <hours>
```

- *hours* - Number of hours before/after UTC (range: -12 to +12 hours)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To

display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

This example sets the time zone to 5 hours before UTC (U.S. Eastern time zone).

```
Aruba Networks AP-80MB(config)#ntp-server timezone -5
```

show ntp

This command displays the current time and configuration settings for the SNTP client.

Syntax

```
show ntp
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show ntp

SNTP Information
=====
Service State      : Enabled
SNTP (server 1) IP : 137.92.140.80
SNTP (server 2) IP : 192.43.244.18
Current Time       : 08 : 04, Jun 20th, 2003
Time Zone          : +8 (TAIPEI, BEIJING)
Daylight Saving    : Enabled, from Jun, 1st to Sep, 1st
=====
```

DHCP Relay Commands

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients that broadcast a request. To receive the broadcast request, the DHCP server would normally have to be on the same subnet as the client. However, when the access point's DHCP relay agent is enabled, received client requests can be forwarded directly by the access point to a known DHCP server on another subnet. Responses from the DHCP server are returned to the access point, which then broadcasts them back to clients.

Table 22 DHCP Commands and Functions

Command	Function	Mode
dhcp-relay	Configures the primary and secondary DHCP server addresses	GC
dhcp-relay enable	Enables the access point's DHCP relay agent	GC
show dhcp-relay	Displays the current DHCP relay configuration	Exec

dhcp-relay

This command configures the primary and secondary DHCP server addresses.

Syntax

```
dhcp-relay {primary | secondary} <ip_address>
```

- **primary** - The primary DHCP server.
- **secondary** - The secondary DHCP server.
- *ip_address* - IP address of the server.

Default Setting

Primary and secondary: 0.0.0.0

Command Mode

Global Configuration

Example

This example sets the DHCP primary server IP address to **192.168.1.10**.

```
Aruba Networks AP-80MB(config)#dhcp-relay primary 192.168.1.10
Aruba Networks AP-80MB(config)#
```

dhcp-relay enable

This command enables the access point's DHCP relay agent. Use the no form to disable the agent.

Syntax

```
[no] dhcp-relay enable
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

For the DHCP relay agent to function, the primary DHCP server must be configured using the dhcp-relay primary command. A secondary DHCP server does not need to be configured, but it is recommended.

If there is no response from the primary DHCP server, and a secondary server has been configured, the agent will then attempt to send DHCP requests to the secondary server.

Example

This example enables DHCP relay.

```
Aruba Networks AP-80MB(config)#dhcp-relay enable
Aruba Networks AP-80MB(config)#
```

show dhcp-relay

This command displays the current DHCP relay configuration.

Syntax

```
show dhcp-relay
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show dhcp-relay
DHCP Relay : ENABLED
Primary DHCP Server : 192.168.1.10
Secondary DHCP Server : 0.0.0.0
Aruba Networks AP-80MB#
```

SNMP Commands

Controls access to this wireless bridge from management stations using the Simple Network Management Protocol (SNMP), as well as the hosts that will receive trap messages.

Table 23 *SNMP Commands and Functions*

Command	Function	Mode
<code>snmp-server contact</code>	Sets the system contact string	GC
<code>snmp-server community</code>	Sets up the community access string to permit access to SNMP commands	GC
<code>snmp-server enable server</code>	Enables SNMP service and traps	GC
<code>snmp-server engine-id</code>	Sets the engine ID for SNMP v3	GC
<code>snmp-server filter</code>	Configures SNMP v3 notification filters	GC
<code>snmp-server filter-assignments</code>	Assigns SNMP v3 notification filters to targets	GC
<code>snmp-server host</code>	Specifies the recipient of an SNMP notification operation	GC
<code>show snmp groups</code>	Configures SNMP v3 notification targets	GC
<code>snmp-server location</code>	Sets the system location string	GC
<code>snmp-server trap</code>	Enables specific SNMP notifications	GC
<code>snmp-server user</code>	Sets the name of the SNMP v3 user	GC
<code>show snmp</code>	Displays the status of SNMP communications	Exec
<code>show snmp filter</code>	Displays the SNMP v3 notification filters	Exec
<code>show snmp filter-assignments</code>	Displays the SNMP v3 notification filter assignments	Exec
<code>show snmp groups</code>	Displays the pre-defined SNMP v3 groups	Exec
<code>show snmp group-assignments</code>	Displays the assignment of users to SNMP v3 groups	Exec
<code>show snmp target</code>	Displays the SNMP v3 notification targets	Exec

Table 23 *SNMP Commands and Functions (Continued)*

Command	Function	Mode
<code>show snmp users</code>	Displays SNMP v3 user settings	Exec

snmp-server community

This command defines the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

```
snmp-server community <string> {ro | rw}
no snmp-server community <string>
```

- *string* - Community string that functions as a password, permitting access to the SNMP protocol. (maximum length: 23 characters, case sensitive).
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- **public** - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

If you enter a community string without the **ro** or **rw** option, the default is read only.

Example

This example sets the SNMP read/write community string to **alpha**.

```
Aruba Networks AP-80MB(config)#snmp-server community alpha rw
```

snmp-server enable server

This command enables SNMP management access and also enables this device to send SNMP traps (notifications). Use the **no** form to disable SNMP service and trap messages.

Syntax

```
snmp-server enable server
no snmp-server enable server
```

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- This command enables both authentication failure notifications and link-up-down notifications.
- The `snmp-server host` command specifies the host device that receives SNMP notifications.

Example

This example enables the SNMP server and configures the server to send SNMP traps.

```
Aruba Networks AP-80MB(config)#snmp-server enable server
```

Related Commands

`snmp-server host` (6-139)

snmp-server engine-id

This command is used for SNMP v3. It is used to uniquely identify the access point among all access points in the network. Use the `no` form to delete the engine ID.

Syntax

```
snmp-server engine-id <engine-id>  
no snmp-server <engine-id>
```

- *engine-id* - Enter engine-id in hexadecimal (5-32 characters).

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- This command is used in conjunction with the `snmp-server user` command.
- Entering this command invalidates all engine IDs that have been previously configured.
- If the engineID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users

Example

This example assigns the AP-80 MB/SB ID to be **1a:2b:3c:4d:00:ff**, as needed for SNMP.

```
Aruba Networks AP-80MB(config)#snmp-server engine-id 1a:2b:3c:4d:00:ff  
Aruba Networks AP-80MB(config)#
```

snmp-server filter

This command configures SNMP v3 notification filters. Use the `no` form to delete an SNMP v3 filter or remove a subtree from a filter.

Syntax

```
snmp-server filter <filter-id> {include | exclude} <subtree> [mask <mask>]  
no snmp-server filter <filter-id> [subtree]
```

- *filter-id* - A user-defined name that identifies an SNMP v3 notification filter. (Maximum length: 32 characters)
- **include** - Defines a filter type that includes objects in the MIB subtree.
- **exclude** - Defines a filter type that excludes objects in the MIB subtree.
- *subtree* - The identifier for the MIB subtree that is to be filtered. The value must be preceded by a period (.).
- *mask* - An optional hexadecimal value bit mask to define objects in the MIB subtree.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- The access point allows up to 10 notification filters to be created. Each filter can be defined by up to 20 MIB subtree ID entries.
- Use the command more than once with the same filter ID to build a filter that includes or excludes multiple MIB objects. Note that the filter entries are applied in the sequence that they are defined.
- The MIB subtree must be defined in the form “.1.3.6.1” and always start with a “.”.
- The mask is a hexadecimal value with each bit masking the corresponding ID in the MIB subtree. A “1” in the mask indicates an exact match and a “0” indicates a “wild card.” For example, a mask value of 0xFFBF provides a bit mask “1111 1111 1011 1111.” If applied to the subtree 1.3.6.1.2.1.2.2.1.1.23, the zero corresponds to the 10th subtree ID. When there are more subtree IDs than bits in the mask, the mask is padded with ones.

Example

This example defines the **trapfilter** notification with MIB subtree identifier .1.

```
Aruba Networks AP-80MB(config)#snmp-server filter trapfilter include .1  
Aruba Networks AP-80MB(config)#snmp-server filter trapfilter exclude  
.1.3.6.1.2.1.2.2.1.1.23
```

snmp-server filter-assignments

This command assigns SNMP v3 notification filters to targets. Use the no form to remove an SNMP v3 filter assignment.

Syntax

```
snmp-server filter-assignments <target-id> <filter-id>  
no snmp-server filter-assignments <target-id>
```

- *target-id* - A user-defined name that identifies a receiver of SNMP notifications. (Maximum length: 32 characters)
- *filter-id* - A user-defined name that identifies an SNMP v3 notification filter. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Example

This example assigns the notification filter **trapfilter** to the **mytraps** receiver.

```
Aruba Networks AP-80MB(config)#snmp-server filter-assignments mytraps trapfilter
Aruba Networks AP-80MB(config)#exit
Aruba Networks AP-80MB#show snmp target
Host ID : mytraps
User : chris
IP Address : 192.168.1.33
UDP Port : 162
=====
Aruba Networks AP-80MB#show snmp filter-assignments
HostID FilterID
mytraps trapfilter
Aruba Networks AP-80MB(config)#
```

snmp-server host

This command specifies the recipient of an SNMP notification. Use the **no** form to remove the specified host.

Syntax

```
snmp-server host {<host_ip_address> | <host_name> <community-string>}
no snmp-server host
```

- *host_ip_address* - IP of the host (the targeted recipient)
- *host_name* - Name of the host (range: 1-20 characters)
- *community-string* - Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command (maximum length: 23 characters).

Default Setting

Host Address: None

Community String: public

Command Mode

Global Configuration

Command Usage

The **snmp-server host** command is used in conjunction with the **snmp-server enable server** command to enable SNMP notifications.

Example

This example sets the SNMP notification recipient to IP address **10.1.19.23**, with community string **batman**.

```
Aruba Networks AP-80MB(config)#snmp-server host 10.1.19.23 batman
```

Related Commands

snmp-server enable server (6-136)

snmp-server targets

This command configures SNMP v3 notification targets. Use the no form to delete an SNMP v3 target.

Syntax

```
snmp-server targets <target-id> <ip-addr> <sec-name> [version {3}] [udp-port  
{port-number}] [notification-type TRAP]  
no snmp-server targets <target-id>
```

- *target-id* - A user-defined name that identifies a receiver of SNMP notifications. (Maximum length: 32 characters)
- *ip-addr* - Specifies the IP address of the management station to receive notifications.
- *sec-name* - The defined SNMP v3 user name that is to receive notifications.
- *version* - The SNMP version of notifications. Currently only version 3 is supported in this command.
- **udp-port** - The UDP port that is used on the receiving management station for notifications.
- **notification-type** - The type of notification that is sent. Currently only TRAP is supported.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- The access point supports up to 10 SNMP v3 target IDs.
- The SNMP v3 user name that is specified in the target must first be configured using the snmp-server user command.

Example

This example assigns the notification target **mytraps** to IP address **192.168.1.33** and user **chris**.

```
Aruba Networks AP-80MB(config)#snmp-server targets mytraps 192.168.1.33 chris  
Aruba Networks AP-80MB(config)#
```

snmp-server trap

This command enables the access point to send specific SNMP traps (notifications). Use the no form to disable specific trap messages.

Syntax

```
snmp-server trap <trap>  
no snmp-server trap <trap>
```

- *trap* - One of the following SNMP trap messages:

- dot11InterfaceAGFail - The 802.11a or 802.11g interface has failed.
- dot11InterfaceBFail - The 802.11b interface has failed.
- dot11StationAssociation - A client station has successfully associated with the access point.
- dot11StationAuthentication - A client station has been successfully authenticated.
- dot11StationReAssociation - A client station has successfully re-associated with the access point.
- dot11StationRequestFail - A client station has failed association, re-association, or authentication.
- dot1xAuthFail - A 802.1X client station has failed RADIUS authentication.
- dot1xAuthNotInitiated - A client station did not initiate 802.1X authentication.
- dot1xAuthSuccess - A 802.1X client station has been successfully authenticated by the RADIUS server.
- dot1xMacAddrAuthFail - A client station has failed MAC address authentication with the RADIUS server.
- dot1xMacAddrAuthSuccess - A client station has successfully authenticated its MAC address with the RADIUS server.
- iappContextDataSent - A client station's Context Data has been sent to another access point with which the station has associated.
- iappStationRoamedFrom - A client station has roamed from another access point (identified by its IP address).
- iappStationRoamedTo - A client station has roamed to another access point (identified by its IP address).
- localMacAddrAuthFail - A client station has failed authentication with the local MAC address database on the access point.
- localMacAddrAuthSuccess - A client station has successfully authenticated its MAC address with the local database on the access point.
- snmpServerFail - The access point has failed to set the time from the configured SNTP server.
- sysConfigFileVersionChanged - The access point's configuration file has been changed.
- sysRadiusServerChanged - The access point has changed from the primary RADIUS server to the secondary, or from the secondary to the primary.
- sysSystemDown - The access point is about to shutdown and reboot.
- sysSystemUp - The access point is up and running.

Default Setting

All traps enabled

Command Mode

Global Configuration

Command Usage

This command is used in conjunction with the `snmp-server host` and `snmp-server enable-server` commands to enable SNMP notifications.

Example

This example enables the access point to send the trap **dot11StationAssociation**.

```
Aruba Networks AP-80MB(config)#no snmp-server trap dot11StationAssociation
Aruba Networks AP-80MB(config)#
```

snmp-server user

This command configures the SNMP v3 users that are allowed to manage the access point. Use the no form to delete an SNMP v3 user.

Syntax

```
snmp-server user <user-name>
```

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Up to 10 SNMPv3 users can be configured on the access point.
- The SNMP engine ID is used to compute the authentication/privacy digests from the pass phrase. You should therefore configure the engine ID with the snmp-server engine-id command before using this configuration command.
- The access point enables SNMP v3 users to be assigned to three pre-defined groups. Other groups cannot be defined. The available groups are:
 - RO - A read-only group using no authentication and no data encryption. Users in this group use no security, either authentication or encryption, in SNMP messages they send to the agent. This is the same as SNMP v1 or SNMP v2c.
 - RWAAuth - A read/write group using authentication, but no data encryption. Users in this group send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.
 - RWPriv - A read/write group using authentication and data encryption. Users in this group send SNMP messages that use an MD5 key/password for authentication and a DES key/password for encryption. Both the MD5 and DES key/passwords must be defined.

The command prompts for the following information to configure an SNMP v3 user:

- user-name - A user-defined string for the SNMP user. (32 characters maximum)
- group-name - The name of the SNMP group to which the user is assigned (32 characters maximum). There are three pre-defined groups: RO, RWAAuth, or RWPriv.
- auth-proto - The authentication type used for user authentication: md5 or none.
- auth-passphrase - The user password required when authentication is used (8 – 32 characters).
- priv-proto - The encryption type used for SNMP data encryption: des or none.
- priv-passphrase - The user password required when data encryption is used (8 – 32 characters).
- Users must be assigned to groups that have the same security levels. If a user who has “AuthPriv” security (uses authentication and encryption) is assigned to a read-only (RO) group, the user will not be able to access the database. An AuthPriv user must be assigned to the RWPriv group with the AuthPriv security level.
- To configure a user for the RWAAuth group, you must include the auth-proto and auth-passphrase keywords.
- To configure a user for the RWPriv group, you must include the auth-proto, auth-passphrase, priv-proto, and priv-passphrase keywords.

Example

This example sets parameters for an SNMP user. When you enter this command, the system prompts you to enter values.

```
Aruba Networks AP-80MB(config)#snmp-server user
User Name<1-32> :chris
Group Name<1-32> :RWPriv
Authtype(md5,<cr>none):md5
Passphrase<8-32>:a good secret
Privacy(des,<cr>none) :des
Passphrase<8-32>:a very good secret
Aruba Networks AP-80MB(config)#
```

show snmp

This command displays the SNMP configuration settings.

Syntax

```
show snmp
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show snmp

SNMP Information
=====
Service State   : Enable
Community (ro)  : *****
Community (rw)  : *****
Location        : WC-19
Contact         : Paul
Traps           : Enabled
Host Name/IP    : 10.1.19.23
Trap Community  : *****
=====
```

show snmp filter

This command displays the SNMP v3 notification filter settings.

Syntax

```
show snmp filter <filter-id>
```

- *filter-id* - A user-defined name that identifies an SNMP v3 notification filter. (Maximum length: 32 characters)

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show snmp group-assignments
GroupName :RWPriv
UserName :chris
Aruba Networks AP-80MB#
Aruba Networks AP-80MB#
```

show snmp filter-assignments

This command displays the SNMP v3 notification filter assignments.

Syntax

```
show snmp filter-assignments
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show snmp filter-assignments
HostID FilterID
mytraps trapfilter
Aruba Networks AP-80MB#
```

show snmp groups

This command displays the SNMP v3 pre-defined groups.

Syntax

```
show snmp groups
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show snmp groups
GroupName :RO
SecurityModel :USM
SecurityLevel :NoAuthNoPriv
GroupName :RWAuth
SecurityModel :USM
SecurityLevel :AuthNoPriv
GroupName :RWPriv
SecurityModel :USM
SecurityLevel :AuthPriv
Aruba Networks AP-80MB#
```

show snmp group-assignments

This command displays the SNMP v3 user group assignments.

Syntax

```
show snmp group-assignments
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show snmp group-assignments
GroupName :RWPriv
UserName :chris
Aruba Networks AP-80MB#
Aruba Networks AP-80MB#
```

show snmp target

This command displays the SNMP v3 notification target settings.

Syntax

```
show snmp target
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show snmp target
Host ID : mytraps
User : chris
IP Address : 192.168.1.33
UDP Port : 162
=====
Aruba Networks AP-80MB#
```

show snmp users

This command displays the SNMP v3 users and settings.

Syntax

```
show snmp users
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show snmp users
=====
UserName :chris
```

```

GroupName :RWPriv
AuthType :MD5
Passphrase:*****
PrivType :DES
Passphrase:*****
=====
Aruba Networks AP-80MB#

```

Flash/File Commands

These commands are used to manage the system code or configuration files.

Table 24 *Flash/File Commands and Function*

Command	Function	Mode
<code>bootfile</code>	Specifies the file or image used to start up the system	Exec
<code>copy</code>	Copies a code image or configuration between flash memory and a FTP/TFTP server	Exec
<code>delete</code>	Deletes a file or code image	Exec
<code>dir</code>	Displays a list of files in flash memory	Exec
<code>show bootfile</code>	Displays the name of the current operation code file that booted the system	

bootfile

This command specifies the image used to start up the system.

Syntax

```
bootfile <filename>
```

- *filename* - Name of the image file

Default Setting

None

Command Mode

Exec

Command Usage

The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 32 characters. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”) If the file contains an error, it cannot be set as the default file.

Example

This example sets the boot image to **bridge-img.bin**.

```
Aruba Networks AP-80MB#bootfile bridge-img.bin
```

copy

This command copies a boot file, code image, or configuration file between the wireless bridge's flash memory and an FTP/TFTP server. When you save the configuration settings to a file on an FTP/TFTP server, that file can later be downloaded to the wireless bridge to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

Syntax

```
copy {ftp | tftp file}
copy config {ftp | tftp}
```

- **ftp** - Keyword that allows you to copy to/from an FTP server
- **tftp** - Keyword that allows you to copy to/from a TFTP server
- **file** - Keyword that allows you to copy to/from a flash memory file
- **config** - Keyword that allows you to upload the configuration file from flash memory.

Default Setting

None

Command Mode

Exec

Command Usage

- The system prompts for data required to complete the copy command.
- Only a configuration file can be uploaded to an FTP/TFTP server, but every type of file can be downloaded to the wireless bridge.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters or 32 characters for files on the wireless bridge. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the flash memory, the wireless bridge supports only two operation code files.
- The system configuration file must be named **syscfg** in all copy commands.

Example

This example shows uploads configuration settings to a file on the TFTP server.

```
Aruba Networks AP-80MB#copy config tftp
TFTP Source file name:syscfg
TFTP Server IP:192.168.1.19
```

This example downloads a configuration file.

```
Aruba Networks AP-80MB#copy tftp file
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>: [1]:2
TFTP Source file name:syscfg
TFTP Server IP:192.168.1.19
```

delete

This command deletes a file or image.

Syntax

```
delete <filename>
```

- *filename* - Name of the configuration file or image name

Default Setting

None

Command Mode

Exec



Beware of deleting application images from flash memory. At least one application image is required in order to boot the wireless bridge. If there are multiple image files in flash memory, and the one used to boot the wireless bridge is deleted, be sure you first use the **bootfile** command to update the application image file booted at startup before you reboot the wireless bridge.

Example

This example deletes the **test.cfg** configuration file from flash memory.

```
Aruba Networks AP-80MB#delete test.cfg
Are you sure you wish to delete this file? <y/n>: y
```

Related Commands

bootfile (6-146)

dir (6-148)

dir

This command displays a list of files in flash memory.

Command Mode

Exec

Command Usage

File information is shown below.

Table 25 *dir* Command Column Descriptions

Column Heading	Description
File Name	The name of the file.
Type	(2) Operation Code and (5) Configuration file
File Size	The length of the file in bytes.

Example

This example displays all file information.

```
Aruba Networks AP-80MB#dir

apimg1          765652
zz-img.bin      1309756
dflt-img.bin    1177004
ap3xart.sys     641540
syscfg_bak     26928
syscfg          26928
apcfg           2932
zz-imgf.bin     1177004
apcfg.bak       2932

2502656 bytes free
```

show bootfile

This command displays the name of the current operation code file that booted the system.

Syntax

```
show bootfile
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MBshow bootfile
Bootfile Information
=====
Bootfile : dflt-img.bin
=====
Aruba Networks AP-80MBshow bootfile ?
```

RADIUS Client Commands

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access for RADIUS-aware devices to the network. An authentication server contains a database of credentials, such as users names and passwords, for each wireless client that requires access to the access point.

Table 26 RADIUS Client Commands and Functions

Command	Function	Mode
<code>radius-server address</code>	Specifies the RADIUS server	GC
<code>radius-server enable</code>	Sets the RADIUS encryption key	GC
<code>radius-server key</code>	Sets the RADIUS encryption key	GC
<code>radius-server port</code>	Sets the RADIUS server network port	GC

Table 26 RADIUS Client Commands and Functions (Continued)

Command	Function	Mode
<code>radius-server port-accounting</code>	Sets the RADIUS Accounting server network port	GC
<code>radius-server radius-mac-format</code>	Sets the format for specifying MAC addresses on the RADIUS server	GC
<code>radius-server retransmit</code>	Sets the number of retries	GC
<code>radius-server timeout</code>	Sets the interval between sending authentication requests	GC
<code>radius-server timeout-interim</code>	Sets the interval between transmitting accounting updates to the RADIUS server	GC
<code>radius-server vlan-format</code>	Sets the format for specifying VLAN IDs on the RADIUS server	GC
<code>show radius</code>	Shows the current RADIUS settings	Exec

radius-server address

This command specifies the primary and secondary RADIUS servers.

Syntax

```
radius-server address [secondary] {<host_ip_address> | <host_name>}
```

- **secondary** - Secondary server
- *host_ip_address* - IP address of server
- *host_name* - Host name of server (range: 1-20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

This example sets the primary RADIUS server IP address to **192.168.1.25**.

```
Aruba Networks AP-80MB(config)#radius-server address 192.168.1.25
```

radius-server enable

This command enables RADIUS features.

Syntax

```
radius-server enable  
no radius-server
```

Default Setting

Disabled

Command Mode

Global Configuration

Example

This example disables the RADIUS server functionality.

```
Aruba Networks AP-80MB(config)#no radius-server
```

radius-server key

This command sets the RADIUS encryption key.

Syntax

```
radius-server [secondary] key <key_string>
```

- **secondary** - Secondary server
- *key_string* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string (maximum length: 20 characters).

Default Setting

DEFAULT

Command Mode

Global Configuration

Example

This example sets the RADIUS encryption key for the secondary server to **green**.

```
Aruba Networks AP-80MB(config)#radius-server secondary key green
```

radius-server port

This command sets the RADIUS server network port.

Syntax

```
radius-server [secondary] port <port_number>
```

- **secondary** - Secondary server
- *port_number* - RADIUS server UDP port used for authentication messages (range: 1024-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

This example sets the primary RADIUS server port to **181**.

```
Aruba Networks AP-80MB(config)#radius-server port 181
```

radius-server port-accounting

This command sets the RADIUS Accounting server network port.

Syntax

```
radius-server [secondary] port-accounting <port_number>
```

- **secondary** - Secondary server. If secondary is not specified, then the access point assumes you are configuring the primary RADIUS server.
- *port_number* - RADIUS Accounting server UDP port used for accounting messages. (Range: 0 or 1024-65535)

Default Setting

0 (disabled)

Command Mode

Global Configuration

Command Usage

When the RADIUS Accounting server UDP port is specified, a RADIUS accounting session is automatically started for each user that is successfully authenticated to the access point.

Example

This example sets the accounting port for the primary RADIUS server to **1813**.

```
Aruba Networks AP-80MB(config)#radius-server port-accounting 1813
Aruba Networks AP-80MB(config)#
```

radius-server radius-mac-format

This command sets the format for specifying MAC addresses on the RADIUS server.

Syntax

```
radius-server radius-mac-format {multi-colon | multi-dash | no-delimiter |
single-dash}
```

- **multi-colon** - Enter MAC addresses in the form xx:xx:xx:xx:xx:xx.
- **multi-dash** - Enter MAC addresses in the form xx-xx-xx-xx-xx-xx.
- **no-delimiter** - Enter MAC addresses in the form xxxxxxxxxxxx.
- **single-dash** - Enter MAC addresses in the form xxxxxx-xxxxxx.

Default Setting

No delimiter

Command Mode

Global Configuration

Example

This example sets the MAC address format for the primary RADIUS server to **multi-dash**.

```
Aruba Networks AP-80MB(config)#radius-server radius-mac-format multi-dash
Aruba Networks AP-80MB(config)#
```

radius-server retransmit

This command sets the number of retries.

Syntax

```
radius-server [secondary] retransmit <number_of_retries>
```

- **secondary** - Secondary server
- *number_of_retries* - Number of times the access point tries to authenticate logon access via the RADIUS server (range: 1 - 30)

Default Setting

3

Command Mode

Global Configuration

Example

This example sets the number of retries for the secondary RADIUS server to **5**.

```
Aruba Networks AP-80MB(config)#radius-server secondary retransmit 5
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server.

Syntax

```
radius-server [secondary] timeout <number_of_seconds>
```

- **secondary** - Secondary server
- *number_of_seconds* - Number of seconds the access point waits for a reply before resending a request (range: 1-60)

Default Setting

5

Command Mode

Global Configuration

Example

This example sets timeout for the primary RADIUS server to **10** seconds.

```
Aruba Networks AP-80MB(config)#radius-server timeout 10
```

radius-server timeout-interim

This command sets the interval between transmitting accounting updates to the RADIUS server.

Syntax

```
radius-server [secondary] timeout-interim <number_of_seconds>
```

- **secondary** - Secondary server.
- *number_of_seconds* - Number of seconds the access point waits between transmitting accounting updates. (Range: 60-86400)

Default Setting

3600

Command Mode

Global Configuration

Command Usage

- The access point sends periodic accounting updates after every interim period until the user logs off and a “stop” message is sent.

Example

This example sets the interval between transmitting accounting updates to the primary RADIUS server to **500** seconds.

```
Aruba Networks AP-80MB(config)#radius-server timeout-interim 500
Aruba Networks AP-80MB(config)#
```

radius-server vlan-format

This command sets the format for specifying VLAN IDs on the RADIUS server.

Syntax

```
radius-server [secondary] vlan-format {hex | ascii}
```

- **secondary** - Secondary server.
- **hex** - Enter VLAN IDs as a hexadecimal number.
- **ascii** - Enter VLAN IDs as an ASCII string.

Default Setting

Hex

Command Mode

Global Configuration

Example

This example sets the format for VLAN IDs on the primary RADIUS server to ASCII.

```
Aruba Networks AP-80MB(config)#radius-server vlan-format ascii
Aruba Networks AP-80MB(config)#
```

show radius

This command displays the current settings for the RADIUS server.

Syntax

```
show radius
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show radius
```

```
Radius Server Information
=====
IP                : 192.168.1.25
Port              : 181
Key               : *****
Retransmit       : 5
Timeout          : 10
=====
```

```
Radius Secondary Server Information
=====
IP                : 0.0.0.0
Port              : 1812
Key               : *****
Retransmit       : 3
Timeout          : 5
=====
```

802.1x Authentication Commands

The access point supports IEEE 802.1x access control for wireless clients. This control feature prevents unauthorized access to the network by requiring a 802.1x client application to submit user credentials for authentication. Client authentication is then verified via by a RADIUS server using Extensible Authentication Protocol (EAP) before the access point grants client access to the network.

Client MAC addresses can also be used for authentication on the access point. For local MAC authentication, first define the default filtering policy using the address filter default command. Then enter the MAC addresses to be filtered, indicating if they are allowed or denied. For RADIUS MAC authentication, the MAC addresses and filtering policy must be configured on the RADIUS server.

Table 27 Authentication Commands and Functions

Command	Function	Mode
802.1x broadcast-key-refresh-rate	Sets the interval at which the primary broadcast keys are refreshed for stations using 802.1x dynamic keying	IC-W VAP
802.1x session-key-refresh-rate	Sets the interval at which unicast session keys are refreshed for associated stations using dynamic keying	IC-W VAP
802.1x session-timeout	Sets the timeout after which a connected client must be re-authenticated	IC-W VAP

Table 27 Authentication Commands and Functions (Continued)

Command	Function	Mode
802.1x supported	Configures 802.1x as disabled, supported, or required	IC-W VAP
802.1x supplicant	Sets the supplicant user name and password for the access point and enables the feature	GC
show authentication	Shows all 802.1X authentication settings, as well as the address filter table	Exec

802.1x broadcast-key-refresh-rate

This command sets the interval at which the broadcast keys are refreshed for stations using 802.1x dynamic keying.

Syntax

802.1x broadcast-key-refresh-rate <rate>

- *rate* - The interval at which the access point rotates broadcast keys (range: 0 - 1440 minutes)

Default Setting

0 (Disabled)

Command Mode

Interface Configuration (Wireless) VAP

Command Usage

- The access point uses Extensible Authentication Protocol Over LANs (EAPOL) packets to pass dynamic unicast session and broadcast keys to wireless clients. The 802.1x **broadcast-key-refresh-rate** command specifies the interval after which the broadcast keys are changed. The **802.1x session-key-refresh-rate** command specifies the interval after which unicast session keys are changed.
- Dynamic broadcast key rotation allows the access point to generate a random group key and periodically update all key-management capable wireless clients.

Example

This example sets the 802.1x broadcast interval to **5** minutes.

```
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1x broadcast-key-refresh-rate 5
```

802.1x session-key-refresh-rate

This command sets the interval at which unicast session keys are refreshed for associated stations using dynamic keying.

Syntax

802.1x session-key-refresh-rate <rate>

- *rate* - The interval at which the access point refreshes a session key (range: 0 - 1440 minutes)

Default Setting

0 (Disabled)

Command Mode

Interface Configuration (Wireless) VAP

Command Usage

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Example

This example sets the refresh rate for unicast keys to **5** minutes.

```
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1x session-key-refresh-rate 5
```

802.1x session-timeout

This command sets the time period after which a connected client must be re-authenticated. Use the **no** form to disable 802.1x re-authentication.

Syntax

```
802.1x session-timeout <seconds>  
no 802.1x session-timeout
```

- *seconds* - The number of seconds (range: 0-65535)

Default

0 (Disabled)

Command Mode

Interface Configuration (Wireless) VAP

Example

This example sets the session timeout to **5** minutes.

```
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1x session-timeout 300
```

802.1x supported

This command configures 802.1x as optionally supported or as required for wireless clients. Use the **no** form to disable 802.1x support.

Syntax

```
802.1x {supported | required}  
no 802.1x
```

- **supported** - Authenticates clients that initiate the 802.1x authentication process. Uses standard 802.11 authentication for all others.
- **required** - Requires 802.1x authentication for all clients.

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless) VAP

Command Usage

- When 802.1x is disabled, the access point does not support 802.1x authentication for any station. After successful 802.11 association, each client is allowed to access the network.
- When 802.1x is supported, the access point supports 802.1x authentication only for clients initiating the 802.1x authentication process (the access point does NOT initiate 802.1x authentication). For stations initiating 802.1x, only those stations successfully authenticated are allowed to access the network. For those stations not initiating 802.1x, access to the network is allowed after successful 802.11 association.
- When 802.1x is required, the access point enforces 802.1x authentication for all 802.11 associated stations. If 802.1x authentication is not initiated by the station, the access point initiates authentication. Only those stations successfully authenticated with 802.1x are allowed to access the network.
- 802.1x does not apply to the 10/100Base-TX port.

Example

This example specifies that 802.1x is supported, but not required.

```
Aruba Networks AP-80MB(if-wireless g: VAP[0])#802.1x supported
```

802.1x supplicant

This command sets the user name and password used for authentication of the access point when operating as a 802.1x supplicant and enables supplicant authentication. Use the **no** form to disable the feature.

Syntax

```
802.1x supplicant eth_password <password>
802.1x supplicant eth_user <username>
802.1x supplicant wds_password <port> <password>
802.1x supplicant wds_user <port> <username>
802.1x supplicant {eth | wds <port>}
no 802.1x supplicant {eth | wds <port>}
```

- **eth_password** - Specifies a password for authentication using the Ethernet port (range: 1-32 alphanumeric characters)
- **eth_user** - Specifies a username for authentication using the Ethernet port (range: 1-32 alphanumeric characters)
- **wds_password** - Specifies a password for authentication using the specified WDS port (range: 1-32 alphanumeric characters)
- **wds_user** - Specifies a username for authentication using the specified WDS port (range: 1-32 alphanumeric characters)
- **eth** - Enables 802.1X supplicant authentication using the Ethernet port
- **wds** - Enables 802.1X supplicant authentication using the specified WDS port
- *port* - Specifies a WDS port number (range: 1-16 Master; 1 Slave)

Default

Disabled

Command Mode

Global Configuration

Command Usage

- Ethernet and WDS user names and passwords must be set before enabling the 802.1x supplicant feature for the specified port.
- The access point currently only supports EAP-MD5 CHAP for 802.1x supplicant authentication.

Example

This example sets the user name and password for WDS port 1.

```
Aruba Networks AP-80MB(config)#802.1x supplicant wds_user 1 David
Aruba Networks AP-80MB(config)#802.1x supplicant wds_password 1 ABC
Aruba Networks AP-80MB(config)#802.1x supplicant wds 1
```

show authentication

This command shows all 802.1x authentication settings, as well as the address filter table.

Syntax

```
show authentication
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show authentication

Authentication Information
=====
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 1 secs
802.1x                        : SUPPORTED
Broadcast Key Refresh Rate    : 5 min
Session Key Refresh Rate      : 5 min
802.1x Session Timeout Value  : 300 secs
Address Filtering             : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address          Status
-----
00-70-50-cc-99-1a   DENIED
00-70-50-cc-99-1b   ALLOWED
=====
```

MAC Address Authentication Commands

These commands define MAC authentication on the access point. For local MAC authentication, first define the default filtering policy using the address filter default command. Then enter the MAC addresses to be filtered, indicating if they are allowed or denied. For RADIUS MAC authentication, the MAC addresses and filtering policy must be configured on the RADIUS server.

Table 28 Authentication Commands and Functions

Command	Function	Mode
<code>address filter default</code>	Sets filtering to allow or deny listed addresses	GC
<code>address filter delete</code>	Removes a MAC address from the filter table	GC
<code>address filter entry</code>	Enters a MAC address in the filter table	GC
<code>mac-authentication server</code>	Sets address filtering to be performed with local or remote options	GC
<code>mac-authentication session-timeout</code>	Sets the interval at which associated clients will be re-authenticated with the RADIUS server authentication database	GC
<code>show authentication</code>	Shows all 802.1X authentication settings, as well as the address filter table	Exec

address filter default

This command sets filtering to allow or deny listed MAC addresses.

Syntax

```
address filter default {allowed | denied}
```

- **allowed** - Only MAC addresses entered as **denied** in the address filtering table are denied.
- **denied** - Only MAC addresses entered as **allowed** in the address filtering table are allowed.

Default

allowed

Command Mode

Global Configuration

Example

This example configures the system to deny listed MAC addresses.

```
Aruba Networks AP-80MB(config)#address filter default denied
```

Related Commands

`address filter entry` (6-161)

address filter delete

This command deletes a MAC address from the filter table.

Syntax

```
address filter delete <mac-address>
```

- *mac-address* - Physical address of client. (Enter six pairs of hexadecimal digits separated by hyphens.)

Default

None

Command Mode

Global Configuration

Example

This example deletes the MAC address **00-70-50-cc-99-1b** from the filter table.

```
Aruba Networks AP-80MB(config)#address filter delete 00-70-50-cc-99-1b
```

address filter entry

This command enters a MAC address in the filter table.

Syntax

```
address filter entry <mac-address> {allowed | denied}
```

- *mac-address* - Physical address of client. (Enter six pairs of hexadecimal digits separated by hyphens; for example, 00-90-D1-12-AB-89.)
- **allowed** - Entry is allowed access.
- **denied** - Entry is denied access.

Default

None

Command Mode

Global Configuration

Command Mode

- The access point supports up to 1024 MAC addresses.
- An entry in the address table may be allowed or denied access depending on the global setting configured for the **address entry default** command.

Example

This command enters the MAC address **00-70-50-cc-99-1a** into the filter table and specifies that the address is allowed.

```
Aruba Networks AP-80MB(config)#address filter entry 00-70-50-cc-99-1a allowed
```

Related Commands

address filter default (6-160)

mac-authentication server

This command sets the MAC authentication server to be local or remote.

Syntax

```
mac-authentication server {local | remote}
```

- **local** - Authenticate the MAC address of wireless clients with the local authentication database during 802.11 association.
- **remote** - Authenticate the MAC address of wireless clients with the RADIUS server during 802.1x authentication.

Default

local

Command Mode

Global Configuration

Example

This example sets MAC

This examples sets the MAC authentication server to be remote.

```
Aruba Networks AP-80MB(config)#mac-authentication server remote
```

Related Commands

address filter entry (6-161)

radius-server address (6-150)

mac-authentication session-timeout

This command sets the interval at which associated clients will be re-authenticated with the RADIUS server authentication database. Use the **no** form to disable reauthentication.

Syntax

```
mac-authentication session-timeout <seconds>
```

- *seconds* - Re-authentication interval (range: 0-65535)

Default

0 (disabled)

Command Mode

Global Configuration

Example

This example sets the MAC authentication timeout to **1** second.

```
Aruba Networks AP-80MB(config)#mac-authentication session-timeout 1
Aruba Networks AP-80MB(config)#
```

Filtering Commands

The commands described in this section are used to control access to the management interface from the wireless interface and filter traffic using specific Ethernet protocol types.

Table 29 *Filtering Commands and Functions*

Command	Function	Mode
<code>filter local-bridge</code>	Disables communication between wireless clients	GC
<code>filter ap-manage</code>	Prevents access to the management interface over the wireless bridge link	GC
<code>filter uplink enable</code>	Ethernet port MAC address filtering	GC
<code>filter uplink</code>	Adds or deletes a MAC address from the filtering table	GC
<code>filter ethernet-type enable</code>	Checks the Ethernet type for all incoming and outgoing Ethernet packets against the protocol filtering table	GC
<code>filter ethernet-type protocol</code>	Sets a filter for a specific Ethernet type	GC
<code>show filters</code>	Shows the filter options and protocol entries in the filter table.	

filter local-bridge

This command disables communication between wireless clients. Use the **no** form to disable this filtering.

Syntax

```
filter local-bridge {all-VAP | intra-VAP}
no filter local-bridge
```

- **all-VAP** - When enabled, clients cannot establish wireless communications with any other client, either those associated to the same VAP interface or any other VAP interface.
- **intra-VAP** - When enabled, clients associated with a specific VAP interface cannot establish wireless communications with each other. Clients can communicate with clients associated to other VAP interfaces.

Default

Disabled

Command Mode

Global Configuration

Command Usage

This command can disable wireless-to-wireless communications between clients via the access point. However, it does not affect communications between wireless clients and the wired network.

Example

This example disables intra-VAP communications between wireless clients.

```
Aruba Networks AP-80MB(config)#filter local-bridge intra-VAP
```

filter ap-manage

This command prevents access to wireless bridge management from the wireless interface. Use the **no** form to disable this filtering.

Syntax

```
filter ap-manage
no filter ap-manage
```

Default

Disabled

Command Mode

Global Configuration

Example

This example prevents access to wireless bridge management from the wireless interface.

```
Aruba Networks AP-80MB(config)#filter ap-manage
```

filter uplink enable

This command enables filtering of MAC addresses from the Ethernet port.

Syntax

```
[no] filter uplink enable
```

Default

Disabled

Command Mode

Global Configuration

Example

```
Aruba Networks AP-80MB(config)#filter uplink enable
Aruba Networks AP-80MB(config)#
```

filter uplink

This command adds or deletes MAC addresses from the uplink filtering table.

Syntax

```
filter uplink {add | delete} <MAC-address>
```

- *MAC-address* - Specifies a MAC address in the form xx-xx-xx-xx-xx-xx. A maximum of four addresses can be added to the filtering table.

Default

Disabled

Command Mode

Global Configuration

Example

This example adds the MAC address **00-12-34-56-78-9a** to the uplink filtering table.

```
Aruba Networks AP-80MB(config)#filter uplink add 00-12-34-56-78-9a
Aruba Networks AP-80MB(config)#
```

filter ethernet-type enable

This command checks the Ethernet type on all incoming and outgoing Ethernet packets against the protocol filtering table. Use the **no** form to disable this feature.

Syntax

```
filter ethernet-type enable
no filter ethernet-type enable
```

Default

Disabled

Command Mode

Global Configuration

Command Usage

This command is used in conjunction with the `filter ethernet-type protocol` command to determine which Ethernet protocol types are to be filtered.

Example

This example enables the Ethernet type.

```
Aruba Networks AP-80MB(config)#filter ethernet-type enable
```

Related Commands

`filter ethernet-type protocol` (6-165)

filter ethernet-type protocol

This command sets a filter for a specific Ethernet type. Use the **no** form to disable filtering for a specific Ethernet type.

Syntax

```
filter ethernet-type protocol <protocol>
no filter ethernet-type protocol <protocol>
```

- *protocol* - An Ethernet protocol type. (Options: ARP, RARP, Berkeley-Trailer-Negotiation, LAN-Test, X25-Level-3, Banyan, CDP, DEC XNS, DEC-MOP-Dump-Load, DEC-MOP, DEC-LAT, Ethertalk, Appletalk-ARP, Novell-IPX(old), Novell-IPX(new), EAPOL, Telxon-TXP, Aironet-DDP, Enet-Config-Test)

Default

None

Command Mode

Global Configuration

Command Usage

Use the **filter ethernet-type enable** command to enable filtering for Ethernet types specified in the filtering table, or the no **filter ethernet-type enable** command to disable all filtering based on the filtering table.

Example

This example sets a filter for the ARP protocol.

```
Aruba Networks AP-80MB(config)#filter ethernet-type protocol ARP
```

Related Commands

filter ethernet-type enable (6-165)

show filters

This command shows the filter options and protocol entries in the filter table.

Syntax

```
show filters
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show filters
```

```
Protocol Filter Information
=====
AP Management           :ENABLED
Ethernet Type Filter   :ENABLED

Enabled Protocol Filters
-----
Protocol: ARP                               ISO: 0x0806
=====
```

WDS Bridge Commands

The commands described in this section are used to set the operation mode for each access point interface and configure Wireless Distribution System (WDS) forwarding table settings.

Table 30 WDS Bridge Commands

Command	Function	Mode
<code>bridge mode</code>	Selects master or slave mode	IC-W
<code>bridge role (WDS)</code>	Selects the bridge operation mode for a radio interface	IC-W
<code>bridge channel-auto-sync</code>	Automatically finds the parent bridge operating channel	IC-W
<code>bridge-link parent</code>	Configures the MAC addresses of the parent bridge node	IC-W
<code>bridge-link child</code>	Configures MAC addresses of connected child bridge nodes	IC-W
<code>bridge dynamic-entry age-time</code>	Sets the aging time for dynamic entries in the WDS forwarding table	GC
<code>show bridge aging-time</code>	Displays the current WDS forwarding table aging time	Exec
<code>show bridge filter-entry</code>	Displays current entries in the bridge MAC address table	Exec
<code>show bridge link</code>	Displays current bridge settings for specified interfaces	Exec

bridge mode

This command selects between Master and Slave mode.

Syntax

```
bridge mode {master | slave}
```

- **master** - Operates as a master enabling up to five slave links.
- **slave** - Operates as a slave with only one link to the master.

Default Setting

WA6202A: Slave

WA6202AM: Master

Command Mode

Interface Configuration (Wireless)

Example

```
Aruba Networks AP-80MB(if-wireless g)#bridge mode master
Aruba Networks AP-80MB(if-wireless g)#
```

bridge role (WDS)

This command selects the bridge operation mode for the radio interface.

Syntax

```
bridge role {ap | repeater | bridge | root-bridge}
```

- **ap** - Operates only as an access point for wireless clients.
- **repeater** - Operates as a wireless repeater, extending the range for remote wireless clients and connecting them to the root bridge. The Parent link to the root bridge must be configured. In this mode, traffic is not forwarded to the Ethernet port from the radio interface.
- **bridge** - Operates as a bridge to other access points also in bridge mode.
- **root-bridge** - Operates as the root bridge in the wireless bridge network.

Default Setting

AP

Command Mode

Interface Configuration (Wireless)

Command Usage

- When the bridge role is set to repeater, the Parent link to the root bridge must be configured. When the access point is operating in this mode, traffic is not forwarded to the Ethernet port from the radio interface.
- Up to four WDS bridge links (MAC addresses) per radio interface can be specified for each unit in the wireless bridge network. One unit only must be configured as the root bridge in the wireless network. The root bridge is the unit connected to the main core of the wired LAN. Other bridges need to specify one Parent link to the root bridge or to a bridge connected to the root bridge. The other seven WDS links are available as Child links to other bridges.
- The bridge link on the radio interface always uses the default VAP interface. In any bridge mode, VAP interfaces 1 to 7 are not available for use.

Example

```
Aruba Networks AP-80MB(if-wireless g)#bridge role ap
Aruba Networks AP-80MB(if-wireless g)#
```

bridge channel-auto-sync

This command allows a child bridge to automatically find the operating channel of its parent bridge.

Syntax

```
bridge channel-auto-sync {enable | disable}
```

- **enable** - The bridge will automatically search and find the operating channel of its parent.
- **disable** - The bridge must have the operating channel manually set to the operating channel of its parent bridge.

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless)

Example

```
Aruba Networks AP-80MB(if-wireless g)#bridge channel-auto-sync enable
Aruba Networks AP-80MB(if-wireless g)#
```

bridge-link parent

This command configures the MAC address of the parent bridge node.

Syntax

```
bridge-link parent <mac-address>
```

- *mac-address* - The wireless MAC address of the parent bridge unit. (12 hexadecimal digits in the form “xx-xx-xx-xx-xx-xx”).

Default Setting

None

Command Mode

Interface Configuration (Wireless)

Command Usage

Every bridge (except the root bridge) in the wireless bridge network must specify the MAC address of the parent bridge that is linked to the root bridge, or the root bridge itself.

Example

```
Aruba Networks AP-80MB(if-wireless a)#bridge-link parent 00-08-2d-69-3a-51
Aruba Networks AP-80MB(if-wireless a)#
```

bridge-link child

This command configures the MAC addresses of child bridge nodes.

Syntax

```
bridge-link child <index> <mac-address>
```

- *index* - The link index number of the child node. (Range: 1 - 6)
- *mac-address* - The wireless MAC address of a child bridge unit (12 hexadecimal digits in the form xx-xx-xx-xx-xx-xx).

Default Setting

None

Command Mode

Interface Configuration (Wireless)

Command Usage

- In root bridge mode, up to six child bridge links can be specified using link

index numbers 1 to 6.

- In bridge mode, up to five child links can be specified using link index numbers 2 to 6. Index number 1 is reserved for the parent link, which must be set using the bridge parent command.

Example

```
Aruba Networks AP-80MB(if-wireless a)#bridge-link child 2 00-08-3e-84-bc-6d
Aruba Networks AP-80MB(if-wireless a)#
```

bridge dynamic-entry age-time

This command sets the time for aging out dynamic entries in the WDS forwarding table.

Syntax

```
bridge dynamic-entry age-time <seconds>
```

- *seconds* - The time to age out an address entry. (Range: 10-10000 seconds).

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

If the MAC address of an entry in the address table is not seen on the associated interface for longer than the aging time, the entry is discarded.

Example

```
Aruba Networks AP-80MB(config)#bridge dynamic-entry age-time 100
Aruba Networks AP-80MB(config)#
```

show bridge aging-time

This command displays the current WDS forwarding table aging time setting.

Syntax

```
show bridge aging-time
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#bridge dynamic-entry age-time 100
Aruba Networks AP-80MB#
Aruba Networks AP-80MB#show bridge aging-time
Aging time: 300
Aruba Networks AP-80MB#
```

show bridge filter-entry

This command displays current entries in the WDS forwarding table.

Syntax

```
show bridge filter-entry
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#bridge filter-entry
=====
                          Bridge MAC Addr Table   Maximum Entries::512
-----
|      MAC      | Port | Fwd_type| VlanID|origin life|remain Life| Type |
| 01-80-C2-00-00-00 | 255 | 5      | 0     |300      |300      | Static |
| 01-80-C2-00-00-03 | 255 | 5      | 0     |300      |300      | Static |
| 00-0B-86-39-19-10 | 2    | 0      | 0     |300      |300      | Static |
| 00-A0-CC-E6-A0-11 | 1    | 3      | 1     |300      |215     | Dynamic |
| 00-0B-86-39-19-11 | 3    | 0      | 0     |300      |300      | Static |
| 00-0B-86-39-19-12 | 4    | 0      | 0     |300      |300      | Static |
0-----
Entries in used::25
=====
Aruba Networks AP-80MB#
```

show bridge link

This command displays WDS bridge link and spanning tree settings for specified interfaces.

Syntax

```
show bridge link {ethernet | wireless {a | g} [index]}
```

- **ethernet** - Specifies the Ethernet interface.
- **wireless** - Specifies a wireless interface:
 - **a** - The 802.11a radio interface.
 - **g** - The 802.11g radio interface.
- *index* - The index number of a bridge link. (Range: 1 - 6)

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show bridge link ethernet
Bridge Port/Link Information (Ethernet)
=====

Port-No           : 1
status            : Enabled
state             : Forwarding
priority          : 128
```

```

path cost          : 19
message age Timer  : Inactive
message age        : 0
designated-root    : priority = 0, MAC = 00:00:00:00:00:00
designated-cost    : 0
designated-bridge  : priority = 0, MAC = 00:00:00:00:00:00
designated-port    : priority = 0, port No = 0
forward-transitions : 0
Aruba Networks AP-80MB#show bridge link wireless g

```

```

Interface Wireless G WDS Information
=====
AP Role:   AP
Parent:    NONE
Child:     NONE
Aruba Networks AP-80#show bridge link wireless a

```

```

Interface Wireless A WDS Information
=====
AP Role:   AP
Parent:    NONE
Child:     NONE
Aruba Networks AP-80MB#show bridge link wireless a 1

```

```

Bridge Port/Link Information (Wireless A 1)
=====

Port-No          : 10
status           : Enabled
state            : Forwarding
priority         : 128
path cost        : 19
message age Timer : Inactive
message age      : 0
designated-root   : priority = 0, MAC = 00:00:00:00:00:00
designated-cost   : 0
designated-bridge : priority = 0, MAC = 00:00:00:00:00:00
designated-port   : priority = 0, port No = 0
forward-transitions : 0
Aruba Networks AP-80MB#

```

Spanning Tree Commands

The commands described in this section are used to set the MAC address table aging time and spanning tree parameters for both the Ethernet and wireless interfaces.

Table 31 *Bridge Commands and Functions*

Command	Function	Mode
<code>bridge dynamic-entry</code>	Sets the aging time for the address table	GC
<code>bridge stp enable</code>	Enables the spanning tree protocol for the bridge	GC
<code>bridge stp forwarding-delay</code>	Configures the spanning tree bridge forward time	GC
<code>bridge stp hello-time</code>	Configures the spanning tree bridge hello time	GC
<code>bridge stp max-age</code>	Configures the spanning tree bridge maximum age	GC

Table 31 *Bridge Commands and Functions (Continued)*

Command	Function	Mode
<code>bridge stp priority</code>	Configures the spanning tree bridge priority	GC
<code>show bridge aging-time</code>	Displays aging time for dynamic entries	Exec
<code>show bridge filter-entry</code>	Displays MAC address entries in the filter database	Exec
<code>show bridge link</code>	Displays parameters of each wireless interface or Ethernet port	Exec
<code>show bridge stp</code>	Displays spanning tree parameters	Exec

bridge dynamic-entry

This command sets dynamic bridge parameters.

Syntax

```
bridge dynamic-entry age-time <seconds>
```

- *seconds* - The time to age out an address entry. (Range: 10-10000 seconds)

Default

Ethernet: 100

802.11a wireless: 1800

Command Mode

Global Configuration

Example

This example sets the aging time to **1000** seconds.

```
Aruba Networks AP-80MB(config)#bridge dynamic-entry age-time 1000
```

bridge stp enable

Use this command to enable the Spanning Tree Protocol globally for the wireless bridge. Use the **no** form to disable it.

Syntax

```
bridge stp enable  
no bridge enable
```

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the wireless bridge to interact with

other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example enables STP for the wireless bridge.

```
Aruba Networks AP-80MB(config)#bridge stp enable
```

bridge stp forwarding-delay

Use this command to configure the spanning tree bridge forward time globally for the wireless bridge. Use the **no** form to restore the default.

Syntax

```
bridge stp forwarding-delay <seconds>  
no bridge stp forwarding-delay
```

- *seconds* - Time in seconds (range: 4 - 30 seconds). The minimum value is the higher of 4 or $[(\text{max-age} / 2) + 1]$.

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device waits before changing states (discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

This example sets the forwarding delay to **15** seconds.

```
Aruba Networks AP-80MB(config)#bridge stp forwarding-delay 15
```

bridge stp hello-time

Use this command to configure the spanning tree bridge hello time globally for the wireless bridge. Use the **no** form to restore the default.

Syntax

```
bridge stp hello-time <time>  
no bridge stp hello-time
```

- *time* - Time in seconds (range: 1-10 seconds). The maximum value is the lower of 10 or $[(\text{max-age} / 2) - 1]$.

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

This example sets the time interval to **5** seconds.

```
Aruba Networks AP-80MB(config)#bridge stp hello-time 5
```

bridge stp max-age

Use this command to configure the spanning tree bridge maximum age globally for the wireless bridge. Use the **no** form to restore the default.

Syntax

```
bridge stp max-age <seconds>  
no bridge stp max-age
```

- *seconds* - Time in seconds (range: 6-40 seconds). The minimum value is the higher of 6 or [2 x (hello-time + 1)]. The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

This example sets the maximum age to **40** seconds.

```
Aruba Networks AP-80MB(config)#bridge stp max-age 40
```

bridge stp priority

Use this command to configure the spanning tree priority globally for the wireless bridge. Use the **no** form to restore the default.

Syntax

```
bridge stp priority <priority>
no bridge stp priority
```

- *priority* - Priority of the bridge (range: 0 - 65535)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address then becomes the root device.

Example

This example sets the priority to 40000.

```
Aruba Networks AP-80MB(config)#bridge stp priority 40000
```

show bridge aging-time

This command displays aging time for dynamic entries.

Syntax

```
show bridge aging-time
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MBshow bridge aging-time
```

```
Bridge Setting Information
```

```
=====
```

```
Aging time: 100
```

```
Aruba Networks AP-80MB
```

show bridge filter-entry

This command displays the MAC entries in the filter database.

Syntax

```
show bridge filter-entry
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MBshow bridge filter-entry
```

```
=====
                        Bridge MAC Addr Table   Maximum Entries::512
-----
|      MAC      | Port | Fwd_type| VlanID|origin life|remain Life| Type |
|-----|-----|-----|-----|-----|-----|-----|
| 01-80-C2-00-00-00 | 255 | 5       | 0     | 100   | 300   | Static |
| 01-80-C2-00-00-03 | 255 | 5       | 0     | 100   | 300   | Static |
| 00-0B-86-39-19-10 | 2    | 0       | 0     | 100   | 300   | Static |
| 00-A0-CC-E6-A0-11 | 1    | 3       | 1     | 100   | 20    | Dynamic |
| 00-0B-86-39-19-11 | 3    | 0       | 0     | 100   | 300   | Static |
| 00-0B-86-39-19-12 | 4    | 0       | 0     | 100   | 300   | Static |
| 00-0B-86-39-19-13 | 5    | 0       | 0     | 100   | 300   | Static |
| 00-0B-86-39-19-20 | 6    | 0       | 0     | 100   | 300   | Static |
| 00-17-F2-52-71-21 | 1    | 3       | 1     | 100   | 20    | Dynamic |
| 00-0B-86-39-19-21 | 7    | 0       | 0     | 100   | 300   | Static |
| 00-0B-86-39-19-22 | 8    | 0       | 0     | 100   | 300   | Static |
| 00-0B-86-39-19-23 | 9    | 0       | 0     | 100   | 300   | Static |
| 00-87-21-94-D3-28 | 1    | 3       | 1     | 100   | 90    | Dynamic |
| 00-14-A5-EA-6D-42 | 1    | 3       | 1     | 100   | 100   | Dynamic |
| 00-03-93-C0-60-6A | 1    | 3       | 1     | 100   | 60    | Dynamic |
| 00-03-93-BB-03-6C | 1    | 3       | 1     | 100   | 60    | Dynamic |
| 00-E0-98-4E-E3-74 | 1    | 3       | 1     | 100   | 100   | Dynamic |
| 00-11-2F-54-BA-78 | 1    | 3       | 1     | 100   | 55    | Dynamic |
| 00-12-17-B8-FE-90 | 1    | 3       | 1     | 100   | 95    | Dynamic |
| 00-0B-86-C3-91-93 | 1    | 0       | 1     | 100   | 300   | Static |
| 00-50-8B-93-8F-BA | 1    | 3       | 1     | 100   | 35    | Dynamic |
| 00-17-F2-04-15-C6 | 1    | 3       | 1     | 100   | 80    | Dynamic |
| FF-FF-FF-FF-FF-FF | 255  | 4       | 0     | 100   | 300   | Static |
-----
Entries in used::23
=====
Aruba Networks AP-80MB
```

show bridge link

This command displays the parameters of each wireless interface or Ethernet port.

Syntax

```
show bridge link ethernet
show bridge link wireless {a | g} [<index>]
```

- *index* - The index that identifies the bridge link: 1 for the root bridge role and 2-8 for the master bridge role.

Command Mode

Exec

Example

```
Aruba Networks AP-80MBshow bridge link ethernet

Bridge Port/Link Information (Ethernet)
=====

Port-No           : 1
status            : Enabled
state             : Forwarding
priority          : 128
path cost         : 19
message age Timer : Inactive
message age       : 11165
designated-root    : priority = 32768, MAC = 00:0B:86:C3:91:93
designated-cost    : 0
designated-bridge  : priority = 32768, MAC = 00:0B:86:C3:91:93
designated-port    : priority = 128, port No = 1
forward-transitions : 1
Aruba Networks AP-80MB
```

```
Aruba Networks AP-80MBshow bridge link wireless g

Interface Wireless G WDS Information
=====
AP Role:    AP
Parent:     NONE
Child:      NONE
Aruba Networks AP-80MB
```

show bridge stp

This command displays spanning tree parameters.

Syntax

```
show bridge stp
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MBshow bridge stp

Bridge STP Information
=====

Bridge MAC           : 00:0B:86:C3:91:93
Status               : Enabled
```

```

priority                : 32768
designated-root          : priority = 32768, MAC = 00:0B:86:C3:91:93
root-path-cost          : 0
root-Port-no            : 0
Hold Time                :      1 Seconds
Hello Time               :      8 Seconds
Maximum Age              :     20 Seconds
Forward Delay            :     10 Seconds
bridge Hello Time        :      8 Seconds
bridge Maximum Age       :     20 Seconds
bridge Forward Delay     :     10 Seconds
time-since-top-change    : 11493 Seconds
topology-change-count    : 25
Aruba Networks AP-80MB

```

Ethernet Interface Commands

The commands described in this section configure connection parameters for the Ethernet interface.

Table 32 *Ethernet Interface Commands and Function*

Command	Function	Mode
<code>dns</code>	Specifies the primary name server	IC-E
<code>interface ethernet</code>	Enters Ethernet interface configuration mode	GC
<code>ip address</code>	Sets the IP address for the Ethernet interface	IC-E
<code>ip dhcp</code>	Submits a DHCP request for an IP address	IC-E
<code>speed-duplex</code>	Configures speed and duplex on the Ethernet interface	IC-E
<code>shutdown</code>	Disables the Ethernet interface	IC-E
<code>show interface ethernet</code>	Shows the status for the Ethernet interface	Exec

dns

This command specifies the address for the primary or secondary domain name server to be used for name-to-address resolution.

Syntax

```

dns primary-server <server-address>
dns secondary-server <server-address>

```

- **primary-server** - Primary server used for name resolution
- **secondary-server** - Secondary server used for name resolution
- *server-address* - IP address of domain-name server.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

The primary and secondary name servers are queried in sequence.

Example

This example specifies two domain-name servers.

```
Aruba Networks AP-80MB(if-ethernet)#dns primary-server 192.168.1.55
Aruba Networks AP-80MB(if-ethernet)#dns secondary-server 10.1.0.55
```

Related Commands

show interface ethernet (6-183)

interface ethernet

This command enters Ethernet interface configuration mode.

Syntax

```
interface ethernet
```

Default Setting

None

Command Mode

Global Configuration

Example

To specify the 10/100Base-TX network interface, enter the following command:

```
Aruba Networks AP-80MB(config)#interface ethernet
Aruba Networks AP-80MB(if-ethernet)#
```

ip address

This command sets the IP address for the (10/100Base-TX) Ethernet interface. Use the **no** form to restore the default IP address.

Syntax

```
ip address <ip-address> <netmask> <gateway>
no ip address
```

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- *gateway* - IP address of the default gateway

Default Setting

IP address: 192.168.1.1
Netmask: 255.255.255.0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- DHCP is enabled by default. To manually configure a new IP address, you must first disable the DHCP client with the **no ip dhcp** command.
- You must assign an IP address to this device to gain management access over the network or to connect the wireless bridge to existing IP subnets. You can manually configure a specific IP address using this command, or direct the device to obtain an address from a DHCP server using the **ip dhcp** command. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format is not accepted by the configuration program.

Example

This example sets the IP address **192.167.1.2** and network mask **255.255.255.0**.

```
Aruba Networks AP-80MB(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
Aruba Networks AP-80MB(if-ethernet)#ip address 192.168.1.2 255.255.255.0
192.168.1.253
```

Related Commands

ip dhcp (6-181)

ip dhcp

This command enables the access point to obtain an IP address from a DHCP server. Use the **no** form to restore the default IP address.

Syntax

```
ip dhcp
no ip dhcp
```

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must assign an IP address to this device to gain management access over the network or to connect the wireless bridge to existing IP subnets. You can manually configure a specific IP address using the **ip address** command, or direct the device to obtain an address from a DHCP server using this command.
- When you use this command, the wireless bridge begins broadcasting DHCP client requests. The current IP address (default or manually configured address) continues to be effective until a DHCP reply is received. Requests are broadcast periodically by this device in an effort to learn its IP address. (DHCP values can include the IP address, subnet mask, and default gateway.)

Example

This example enables the access point to obtain an IP address from a DHCP server.

```
Aruba Networks AP-80MB(config)#interface ethernet
```

```
Enter Ethernet configuration commands, one per line.
Aruba Networks AP-80MB(if-ethernet)#ip dhcp
```

Related Commands

ip address (6-180)

speed-duplex

This command configures the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

```
speed-duplex {auto | 10MH | 10MF | 100MF | 100MH}
```

- auto - autonegotiate speed and duplex mode
- 10MH - Forces 10 Mbps, half-duplex operation
- 10MF - Forces 10 Mbps, full-duplex operation
- 100MH - Forces 100 Mbps, half-duplex operation
- 100MF - Forces 100 Mbps, full-duplex operation

Default Setting

Auto-negotiation is enabled by default.

Command Mode

Interface Configuration (Ethernet)

Command Usage

If autonegotiation is disabled, the speed and duplex mode must be configured to match the setting of the attached device.

Example

The following example configures the Ethernet port to 100 Mbps, full-duplex operation.

```
Aruba Networks AP-80MB(if-ethernet)#speed-duplex 100mf
Aruba Networks AP-80MB(if-ethernet)#
```

shutdown

This command disables the Ethernet interface. To restart a disabled interface, use the **no** form.

Syntax

```
shutdown
no shutdown
```

Default Setting

Interface enabled-

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command allows you to disable the Ethernet port due to abnormal behavior (for example, excessive collisions), and re-enable it after the problem has been resolved. You may also want to disable the Ethernet port for security reasons.

Example

The following example disables the Ethernet port.

```
Aruba Networks AP-80MB(if-ethernet)#shutdown
```

show interface ethernet

This command displays the status for the Ethernet interface.

Syntax

```
show interface [ethernet]
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show interface ethernet
Ethernet Interface Information
=====
IP Address           : 192.168.1.1
Subnet Mask          : 255.255.255.0
Default Gateway     : 192.168.1.253
Primary DNS         : 192.168.1.55
Secondary DNS       : 10.1.0.55
Admin status        : Up
Operational status  : Up
=====
```

Wireless Interface Commands

The commands described in this section configure connection parameters for the wireless interface.hy7

Table 33 *Wireless Interface Commands and Functions*

Command	Function	Mode
ant-gain-reduction	Sets the reduction in antenna gain	IC-W
antenna	Sets antenna location and diversity	IC-W
assoc-timeout-interval	Sets the timeout interval for client association	IC-W VAP
auth-timeout-value	Sets the timeout for authentication requests	IC-W VAP
auth	Defines authentication settings	IC-W VAP
beacon-interval	Configures the rate at which beacon signals are transmitted from the wireless bridge	IC-W

Table 33 *Wireless Interface Commands and Functions (Continued)*

Command	Function	Mode
bridge	Configures the rate at which beacon signals are transmitted from the wireless bridge	IC-W
channel	Configures the radio channel	IC-W
cipher-suite	Defines the cipher algorithm used for broadcasting and multicasting when using Wi-Fi Protected Access (WPA) security	IC-W VAP
description	Adds a description to the wireless interface	IC-W VAP
dtim-period	Configures the rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions	IC-W
encryption	Defines whether or not WEP or AES encryption is used to provide privacy for wireless communications	IC-W VAP
fragmentation-length	Configures the minimum packet size that can be fragmented	IC-W
hide-ssid	Suppresses the SSID in beacons	IC-W VAP
interface wireless	Enters wireless interface configuration mode	GC
key	Sets the keys used for WEP and AES encryption	IC-W
max-association	Configures the maximum number of clients that can be associated with the access point radio at the same time	IC-W VAP
MIC_mode	Configures the minimum packet size that can be fragmented	IC-W
multicast-data-rate	Sets the keys used for WEP or AES encryption	IC-W
preamble	Sets the preamble length	IC-W
pmksa-lifetime	Sets the lifetime PMK security associations	IC-W VAP
pre-authentication	Enables WPA2 pre-authentication for fast roaming	IC-W VAP
protection-method	Sets the packet size threshold at which an RTS must be sent to the receiving station prior to the sending station starting communications	IC-W VAP
radio-mode	Configures the maximum data rate for transmitting unicast packets on the wireless interface	IC-W VAP
rssi		IC-W
rts-threshold	Sets the packet size threshold at which an RTS must be sent to the receiving station prior to the sending station starting communications	IC-W
speed	Configures the maximum data rate for transmitting unicast packets on the wireless interface	IC-W
shutdown	Disables the wireless interface	IC-W
show interface wireless	Shows the status for the wireless interface	Exec
show station	Shows the wireless clients associated with the access point	Exec
ssid	Configures the service set identifier	IC-W VAP

Table 33 *Wireless Interface Commands and Functions (Continued)*

Command	Function	Mode
<code>super-g</code> or <code>super-a</code>	Sets parameters for the Atheros proprietary Super G performance enhancements	IC-W
<code>transmit-key</code>	Sets the keys used for WEP or AES encryption	IC-W VAP
<code>transmit-power</code>	Adjusts the power of the radio signals transmitted from the wireless bridge	IC-W
<code>turbo</code>	Configures the 802.11a radio to use a faster proprietary modulation mode	IC-W
<code>vap</code>	Provides access to the VAP interface configuration mode	IC-W

ant-gain-reduction

This command configures the antenna gain reduction.

Syntax

```
ant-gain-reduction <dB>
```

- *dB* - Amount of antenna gain reduction (0-29db)

Default Setting

0

Command Mode

Interface Configuration (Wireless)

Example

This example sets the antenna gain reduction to 10dB.

```
Aruba Networks AP-80MB(if-wireless g)#ant-gain-reduction 10
Aruba Networks AP-80MB(if-wireless g)#
```

antenna

This command sets antenna location and diversity.

Syntax

```
antenna control {diversity | left | right}
antenna location {indoor | outdoor}
```

- **left/right/diversity** - Radio used for output.
- **indoor/outdoor** - Physical location of the AP-80 MB/SB.

Default Setting

Diversity (applies only to the G radio, outdoor)

Command Mode

Interface Configuration (Wireless)

Command Usage

This command allows you to select a specific receive antenna or to allow the access point to choose the receive antenna in response to ambient noise conditions.

Example

This example sets antenna diversity for the 802.11g radio.

```
Aruba Networks AP-80MB(if-wireless g)#antenna control diversity
Aruba Networks AP-80MB(if-wireless g)#
```

assoc-timeout-interval

This command sets the timeout interval for client association.

Syntax

```
assoc-timeout-interval <value>
```

- *value* - Time interval (minutes)

Default Setting

30

Command Mode

Interface Configuration (Wireless) VAP

Command Usage

This command determines how soon clients lose association if no traffic passes between the client and the access point.

Example

This example sets the association timeout for the 802.11g radio to 10 minutes.

```
Aruba Networks AP-80MB(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Aruba Networks AP-80MB(if-wireless g)#vap 0
Aruba Networks AP-80MB(if-wireless g: VAP[0])#assoc-timeout-interval 10
Aruba Networks AP-80MB(if-wireless g: VAP[0])#
```

auth-timeout-value

This command sets the authentication timeout interval.

Syntax

```
auth-timeout-value <value>
```

- *value* - Time interval (minutes)

Default Setting

60

Command Mode

Interface Configuration (Wireless) VAP

Command Usage

This command determines how soon client authentication times out if no traffic passes between the client and the access point.

Example

This example sets the authentication timeout for the 802.11a radio to 10 minutes.

```
Aruba Networks AP-80MB(config)#interface wireless a
Enter Wireless configuration commands, one per line.
Aruba Networks AP-80MB(if-wireless a)#vap 0
Aruba Networks AP-80MB(if-wireless a: VAP[0])#auth-timeout-value 10
Aruba Networks AP-80MB(if-wireless a: VAP[0])#
```

auth

This command defines the 802.11 authentication type allowed by the access point.

Syntax

```
authentication open-system | shared-key
wpa required | supported
wpa-psk required | supported
wpa-wpa2-mixed required | supported
wpa-wpa2-psk-mixed required | supported
wpa2 required | supported
wpa2-psk required | supported
```

- **open-system** - Authentication open.
- **shared-key** - Authentication shared.
- **required** - Supports only clients using WPA.
- **supported** - Support clients with or without WPA.
- **wpa, wpa-psk, wpa-wpa2-mixed, wpa-wpa2-psk-mixed, wpa2, wpa2-psk** - WPA authentication type (WPA1 or WPA2, or mixed).

Default Setting

open-system

Command Mode

Interface Configuration (Wireless) VAP

Command Usage

- Wi-Fi Protected Access (WPA) provides improved data encryption, which was weak in WEP, and user authentication, which was largely missing in WEP. WPA uses the following security mechanisms.
- Enhanced Data Encryption through TKIP—WPA uses Temporal Key Integrity Protocol (TKIP). TKIP provides data encryption enhancements including per-packet key hashing (i.e., changing the

encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.

- Enterprise-level User Authentication via 802.1x and EAP—To strengthen user authentication, WPA uses 802.1x and the Extensible Authentication Protocol (EAP). Used together, these protocols provide strong user authentication via a central RADIUS authentication server that authenticates each user on the network before they join it. WPA also employs “mutual authentication” to prevent a wireless client from accidentally joining a rogue network.
- When the WPA mode is set to “dynamic,” clients are authenticated using 802.1x via a RADIUS server. Each client has to be WPA-enabled or support 802.1x client software. A RADIUS server must also be configured and be available in the wired network.
- When the WPA mode is set to pre-shared-key, the key must first be generated and distributed to all wireless clients before they can successfully associate with the access point.
- Shared key authentication can only be used when WEP is enabled with the **encryption** command, and at least one static WEP key has been defined with the **key** command.
- When using WPA or 802.1x for authentication and dynamic keying, the access point must be set to **open**.

Example

This example sets the authentication type for the 802.11g radio to WPA.

```
Aruba Networks AP-80MB(if-wireless g: VAP[0])# auth wpa required
Data Encryption is set to Enabled.
WPA2 Clients mode is set to Disabled.
WPA Clients Mode is set to Required.
WPA Multicast Cipher is set to TKIP.
WPA Unicast Cipher can accept TKIP only.
WPA Authentication is set to 802.1X Required.
Aruba Networks AP-80MB(if-wireless g: VAP[0])#
```

beacon-interval

This command configures the rate at which beacon signals are transmitted from the wireless bridge.

Syntax

```
beacon-interval <interval>
```

- *interval* - The rate for transmitting beacon signals (range: 20-1000 milliseconds)

Default Setting

100

Command Mode

Interface Configuration (Wireless)

Command Usage

The beacon signals allow remote bridges to maintain contact with the local wireless bridge. They may also carry power-management information.

Example

This example sets the beacon interval to 120 milliseconds.

```
Aruba Networks AP-80MB(if-wireless a)#beacon-interval 150
```

bridge

This command sets bridge parameters.

Syntax

```
bridge channel-auto-sync {enable | disable}
bridge mode {master | slave}
bridge role {ap | bridge | root-bridge}
```

- **channel-auto-sync** - channel automatically changed to make a wireless connection.
- **mode** - Master or slave mode
- **role** - ap, bridge, or root-bridge mode

Default Setting

AP

Command Mode

Interface Configuration (Wireless)

Example

This example sets the bridge mode to **master**.

```
Aruba Networks AP-80MB(if-wireless g)#bridge mode master
Aruba Networks AP-80MB(if-wireless g)#
```

channel

This command configures the radio channel through which the local wireless bridge communicates with remote bridges.

Syntax

```
channel {<channel> | auto}
```

- **channel** - Manually sets the radio channel used for communications with remote bridges (range: 802.11a - 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165 for normal mode, and 42, 50, 58, 152, 160 for turbo mode; 802.1g - 1 to 14)
- **auto** - Automatically selects an unoccupied channel (if available). Otherwise, the lowest channel is selected.

Default Setting

11 (auto)

Command Mode

Interface Configuration (Wireless)

Command Usage

The available channel settings are limited by local regulations, which determine the number of channels that are available.

Example

This example sets the 802.11a channel to **36**.

```
Aruba Networks AP-80MB(if-wireless a)#channel 36
```

cipher-suite

This command defines the cipher algorithm used for broadcasting and multicasting when using Wi-Fi Protected Access (WPA) security.

Syntax

```
multicast-cipher {AES | TKIP | WEP}
```

- **AES** - Advanced Encryption Standard
- **TKIP** - Temporal Key Integrity Protocol
- **WEP** - Wired Equivalent Privacy

Default Setting

WEP

Command Mode

Interface Configuration (Wireless) VAP

Command Usage

- WPA enables the access point to support different unicast encryption keys for each client. However, the global encryption key for multicast and broadcast traffic must be the same for all clients. This command sets the encryption type that is supported by all clients.
- If any clients supported by the access point are not WPA enabled, the multicast-cipher algorithm must be set to WEP.
- WEP is the first generation security protocol used to encrypt data crossing the wireless medium using a fairly short key. Communicating devices must use the same WEP key to encrypt and decrypt radio signals. WEP has many security flaws, and is not recommended for transmitting highly sensitive data.
- TKIP provides data encryption enhancements including per-packet key hashing (i.e., changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.
- TKIP defends against attacks on WEP in which the unencrypted initialization vector in encrypted packets is used to calculate the WEP key. TKIP changes the encryption key on each packet, and rotates not just the unicast keys, but the broadcast keys as well. TKIP is a replacement for WEP that removes the predictability that intruders relied on to determine the WEP key.
- AES has been designated by the National Institute of Standards and Technology as the successor to the Data Encryption Standard (DES) encryption algorithm, and will be used by the U.S. government for encrypting all sensitive, nonclassified information. Because of its strength, and resistance to attack, AES is also being incorporated as part of the 802.11 standard.

Example

This example sets the multicast cipher to TKIP.

```
Aruba Networks AP-80MB(if-wireless g: VAP[0]):#multicast-cipher TKIP
```

description

This command adds a description to the wireless interface. Use the **no** form to remove the description.

Syntax

```
description <string>  
no description
```

- *string* - Comment or a description for this interface (range: 1-80 characters)

Default Setting

Enterprise 802.11g Access Point

Command Mode

Interface Configuration (Wireless) VAP

Example

This example sets the description RD-AP#3 for the 802.11a radio, VAP 0.

```
Aruba Networks AP-80MB(config)#interface wireless a  
Aruba Networks AP-80MB(if-wireless g: VAP[0])#description RD-AP#3
```

dtim-period

This command configures the interval during which remote bridges in sleep mode must wake up to receive broadcast/multicast transmissions.

Syntax

```
dtim-period <interval>
```

- *interval* - Interval between the beacon frames that transmit broadcast or multicast traffic (range: 1-255 beacon frames)

Default Setting

1

Command Mode

Interface Configuration (Wireless)

Command Usage

- The Delivery Traffic Indication Map (DTIM) packet interval value indicates how often the MAC layer forwards broadcast/multicast traffic. This parameter is necessary to wake up remote bridges that are using Power Save mode.
- The DTIM is the interval between two synchronous frames with broadcast/multicast information. The default value of 2 indicates that the wireless bridge will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon.
- Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing remote bridges in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by remote bridges in Power Save mode, but delays the transmission of broadcast/multicast frames.

Example

This example sets the DTIM period to 100 beacon frames.

```
Aruba Networks AP-80MB(if-wireless a)#dtim-period 100
```

encryption

This command defines whether WEP or AES encryption is used to provide privacy for wireless communications. Use the **no** form to disable encryption.

Syntax

```
encryption {wep <key-length> | wdsaes alphanumeric | hex}  
no encryption
```

- **wep** - The keyword that enables WEP encryption.
- *key-length* - Size of encryption key. (Options: 64, 128, or 152 bits)
- **wdsaes** - The keyword that enables 128-bit AES encryption.
- **alphanumeric** - Specifies an encryption key entered as an alphanumeric string.
- **hex** - Specifies an encryption key entered as hexadecimal digits.

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

- Wired Equivalent Privacy (WEP) and Advanced Encryption Standard (AES) are implemented in this device to prevent unauthorized access to your network. For more secure data transmissions, enable WEP or AES encryption with this command, and set at least one key with the **key** command.
- AES has been designated by the National Institute of Standards and Technology as the successor to the Data Encryption Standard (DES) encryption algorithm, and will be used by the U.S. government for encrypting all sensitive, nonclassified information. Because of its strength, and resistance to attack, AES is also being incorporated as part of the 802.11 standard.
- The WEP settings must be the same on all bridges in your wireless network.
- The WEP encryption length specified in the **encryption** command and the **key** command must match.
- The AES keys must match for each wireless bridge link pair.
- The AES key type value entered using the **key** command must be the same as the type specified in the **encryption** command.
- Note that encryption protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

Example

This example sets encryption to 128-bit WEP.

```
Aruba Networks AP-80MB(if-wireless a)#encryption wep 128
```

Related Commands

transmit-key (6-203)

fragmentation-length

This command configures the minimum packet size that can be fragmented when passing through the wireless bridge.

Syntax

```
fragmentation-length <length>
```

- *length* - Minimum packet size for which fragmentation is allowed. (Range: 256-2346 bytes)

Default Setting

2346

Command Mode

Interface Configuration (Wireless)

Command Usage

- If the packet size is smaller than the preset Fragment size, the packet will not be segmented.
- Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames.

Example

This example sets the fragmentation length to 512 bytes.

```
Aruba Networks AP-80MB(if-wireless a)#fragmentation-length 512
```

hide-ssid

This command suppression broadcast of the SSID in beacons.

Syntax

```
hide-ssid  
no hide-ssid
```

Default Setting

disabled

Command Mode

Interface Configuration (Wireless) VAP

Example

This example allows SSID broadcast in beacons.

```
Aruba Networks AP-80MB(if-wireless a)#no hide-ssid
```

interface wireless

This command enters wireless interface configuration mode.

Syntax

```
interface wireless {a | g}
```

- **a** - 802.11a radio interface
- **g** - 802.11g radio interface

Default Setting

None

Command Mode

Global Configuration

Example

This example enters configuration mode for the 802.11a radio.

```
Aruba Networks AP-80MB(config)#interface wireless a
Aruba Networks AP-80MB(if-wireless a)#
```

key

This command sets the keys used for WEP and AES encryption. Use the **no** form to delete a configured key.

Syntax

```
key {wep <index> <size> <type> <wep-value> | wdsaes <port-id> <aes-value>}
no key {wep <index> | wdsaes}
```

- **wep** - The keyword that specifies a WEP encryption key.
 - index* - Key index. (Range: 1-4)
 - size* - Key size. (Options: 64, 128, or 152 bits)
 - type* - Input format. (Options: ASCII, HEX)
 - wep-value* - The WEP key string. For ASCII input, use 5/13/16 alphanumeric characters for 64/128/152 bit keys. For HEX input, use 10/26/32 hexadecimal digits for 64/128/152 bit keys.
- **wdsaes** - The keyword that specifies an AES encryption key
 - port-id* - The ID for the wireless port on the bridge. For Slave units, the ID is 1. For Master units, the ID can be from 1 to 16.
 - aes-value* - The AES key string. For alphanumeric input, use 8 to 31 characters. For hexadecimal input, use exactly 32 digits.

Default Setting

None

Command Mode

Interface Configuration (Wireless)

Command Usage

- To enable WEP encryption, use the **encryption** command to specify the key type and length, and use the **key** command to configure at least one key.

- To enable AES encryption, use the **encryption** command to specify the key type, and use the **key** command to configure a key for each wireless port.
- If WEP is enabled, all units in the wireless bridge network must be configured with the same keys.
- The WEP key length specified in the **encryption** command and the **key** command must match.
- The WEP key index, length and type configured on the local wireless bridge must match those configured on other wireless bridges.
- If AES is enabled, each wireless bridge link in the network must be configured to use the same AES key.
- The AES key type value entered using the **key** command must be the same as the type specified in the **encryption** command.

Example

This example sets WEP keys.

```
Aruba Networks AP-80MB(if-wireless a)#key wep 1 64 ascii 12345
Aruba Networks AP-80MB(if-wireless a)#key wep 2 64 ascii abcde
```

Related Commands

encryption (6-192)

max-association

This command configures the maximum number of clients that can be associated with the access point at the same time.

Syntax

```
max-association <count>
```

- *count* - Maximum number of associated stations (range: 0-64)

Default Setting

64

Command Mode

Interface Configuration (Wireless) VAP

Example

This example sets the maximum number of clients to 32.

```
AP(if-wireless g)#max-association 32
```

MIC_mode

This command sets the Message Integrity Check (MIC) mode.

Syntax

```
MIC-mode {hardware | software}
```

- **hardware** - hardware mode
- **software** - software mode

Default Setting

hardware

Command Mode

Interface Configuration (Wireless)

Example

This example sets the MIC mode to **hardware** for the 802.11g radio.

```
Aruba Networks AP-80MB(if-wireless g)#mic_mode hardware
Aruba Networks AP-80MB(if-wireless g)#
```

multicast-data-rate

This command sets the data rate for multicast messages.

Syntax

```
multicast-data-rate <rate>
```

- *rate* - The rate for transmitting beacon signals (Mbps)

Default Setting

5.5

Command Mode

Interface Configuration (Wireless)

Example

This example sets the multicast data rate to **1** Mbps.

```
Aruba Networks AP-80MB(if-wireless g)#multicast-data-rate 1
Aruba Networks AP-80MB(if-wireless g)#
```

preamble

This command sets the RF preamble option.

Syntax

```
preamble {short | short-or-long}
```

- **short** - short preamble supported
- **short-or-long** - either short or long preamble supported

Default Setting

short-or-long

Command Mode

Interface Configuration (Wireless)

Command Usage

- If all clients and access points in the network support the short preamble, then configuring that option can improve network throughput.
- If not all clients support the short preamble, configure the short-or-long option.

Example

This example sets the RF preamble to **short** for the 802.11a radio.

```
Aruba Networks AP-80MB(if-wireless a)#preamble short
Aruba Networks AP-80MB(if-wireless a)#
```

pmksa-lifetime

This command sets the time for aging out cached WPA2 Pairwise Master Key Security Association (PMKSA) information for fast roaming.

Syntax

```
pmksa-lifetime <minutes>
```

- **minutes** - The time for aging out PMKSA information. (Range: 0 - 14400 minutes)

Default Setting

720 minutes

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- WPA2 provides fast roaming for authenticated clients by retaining keys and other security information in a cache, so that if a client roams away from an access point and then returns reauthentication is not required.
- When a WPA2 client is first authenticated, it receives a Pairwise Master Key (PMK) that is used to generate other keys for unicast data encryption. This key and other client information form a Security Association that the access point names and holds in a cache. The lifetime of this security association can be configured with this command. When the lifetime expires, the client security association and keys are deleted from the cache. If the client returns to the access point, it requires full reauthentication.
- The access point can store up to 256 entries in the PMKSA cache.

Example

```
Aruba Networks AP-80MB(if-wireless g: VAP[0])#wpa-pre-shared-key ASCII
agoodsecret
Aruba Networks AP-80MB(if-wireless g: VAP[0])#
```

pre-authentication

This command enables WPA2 pre-authentication for fast secure roaming.

Syntax

```
pre-authentication {enable | disable}
```

- **enable** - Enables pre-authentication for the VAP interface.
- **disable** - Disables pre-authentication for the VAP interface.

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- Each time a client roams to another access point it has to be fully re-authenticated. This authentication process is time consuming and can disrupt applications running over the network. WPA2 includes a mechanism, known as pre-authentication, that allows clients to roam to a new access point and be quickly associated. The first time a client is authenticated to a wireless network it has to be fully authenticated. When the client is about to roam to another access point in the network, the access point sends pre-authentication messages to the new access point that include the client's security association information. Then when the client sends an association request to the new access point the client is known to be already authenticated, so it proceeds directly to key exchange and association.
- To support pre-authentication, both clients and access points in the network must be WPA2 enabled.
- Pre-authentication requires all access points in the network to be on the same IP subnet.

Example

```
Aruba Networks AP-80MB(if-wireless g: VAP[0])#wpa-pre-shared-key ASCII  
agoodsecret  
Aruba Networks AP-80MB(if-wireless g: VAP[0])#
```

protection-method

This command sets the RTS (Request to Send) or CTS (Clear to Send) protection method.

Syntax

```
protection method {CTS-only | RTS-only}
```

- **CTS-only** - clear to send only
- **RTS-only** - request to send only

Default Setting

CTS-only

Command Mode

Interface Configuration (Wireless)

Example

This command sets the protection method to CTS only for the 802.11g radio.

```
Aruba Networks AP-80MB(if-wireless g)#protection method CTS-only
Aruba Networks AP-80MB(if-wireless g)#
```

radio-mode

This command sets the 802.11 radio mode for the b/g radio.

Syntax

```
radio-mode b | g | b+g
```

Default Setting

b+g

Example

This example sets the 802.11b/g radio mode to b.

```
Aruba Networks AP-80MB(if-wireless g)#radio-mode b
Aruba Networks AP-80MB(if-wireless g)#
```

rssi

This command defines parameters for Received Signal Strength Indicator (RSSI).

Syntax

```
rssi outputactive {enable | disable}
rssi {distance [normal | turbo] <distance> | port <port> | sample-duration
<duration> }
```

- **outputactive enable/disable** - RSSI output generation enabled or disabled.
- *distance* - The distance (Km) over which to measure RSSI in normal or turbo mode.
- *port* - the AP-80 MB/SB port for RSSI output.
- *sample-duration* - The period (seconds) over which each RSSI sample is taken.

Default Setting

Disable

Command Mode

Interface Configuration (Wireless)

Example

This example sets the sample duration for RSSI to **10** seconds.

```
AP(if-wireless a)#rssi sample-duration 10
AP(if-wireless a)#
```

rts-threshold

This command sets the packet size threshold at which a Request to Send (RTS) signal must be sent to the receiving remote bridge prior to the sending bridge starting communications.

Syntax

```
rts-threshold <threshold>
```

- *threshold* - Threshold packet size for which to send an RTS (range: 0-2347 bytes)

Default Setting

2347

Command Mode

Interface Configuration (Wireless)

Command Usage

- If the threshold is set to 0, the wireless bridge always sends RTS signals. If set to 2347, the wireless bridge never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.
- The wireless bridge sends RTS frames to a receiving remote bridge to negotiate the sending of a data frame. After receiving an RTS frame, the remote bridge sends a CTS frame to notify the local bridge that it can start sending data.
- Wireless bridges contending for the wireless medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node” problem.

Example

This example sets the RTS threshold to **256** bytes.

```
Aruba Networks AP-80MB(if-wireless a)#rts-threshold 256
```

speed

This command configures the maximum data rate for transmitting unicast packets on the wireless interface.

Syntax

```
speed <speed>
```

- *speed* - Maximum access speed allowed for remote bridges (options: 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps; 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps)

Default Setting

54 Mbps

Command Mode

Interface Configuration (Wireless)

Command Usage

The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance.

Example

This example sets the maximum data rate for unicast packets from the 802.11a radio to **6** Mbps.

```
Aruba Networks AP-80MB(if-wireless a)#speed 6
```

shutdown

This command disables the wireless interface. Use the **no** form to restart the interface.

Syntax

```
shutdown
no shutdown
```

Default Setting

Interface enabled

Command Mode

Interface Configuration (Wireless)

Example

This example disables the 802.11a interface.

```
Aruba Networks AP-80MB(if-wireless a)#shutdown
```

show interface wireless

This command displays the status for the wireless interface.

Syntax

```
show interface wireless a | g
```

- **a** - 802.11a radio interface
- **g** - 802.11g radio interface

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show interface wireless a
```

```
Wireless Interface Information
=====
-----Identification-----
Description                : Enterprise 802.11a Access Point
Service Type               : WDS Bridge
SSID                      : DualBandOutdoor
Turbo Mode                 : OFF
Channel                   : 36
Status                    : Enable
-----802.11 Parameters-----
Transmit Power             : FULL (15 dBm)
Max Station Data Rate     : 54Mbps
```

```

Fragmentation Threshold      : 2346 bytes
RTS Threshold                : 2347 bytes
Beacon Interval              : 100 TUs
DTIM Interval                : 2 beacons
Maximum Association          : 64 stations
-----Security-----
Encryption                   : 128-BIT AES ENCRYPTION
AES Key type                 : Alphanumeric
=====

```

show station

This command shows the wireless clients associated with the access point.

Syntax

```
show station
```

Command Mode

Exec

Example

```

Aruba Networks AP-80MB#show station

Station Table Information
=====
802.11a Channel : 56

No 802.11a Channel Stations.
802.11g Channel : 11
802.11g Channel Station Table
Station Address   : 00-04-E2-41-C2-9D VLAN ID: 0
Authenticated Associated Forwarding KeyType
TRUE             TRUE      TRUE      NONE
Counters:pkts   Tx    /    Rx    bytes Tx    /    Rx
                  4/      0      1440/      0
Time:Associated LastAssoc LastDisAssoc LastAuth
          143854         0         0         0
=====

```

ssid

This command configures the service set identifier (SSID).

Syntax

```
ssid <string>
```

- *string* - The name of a basic service set supported by the access point (range: 1 - 32 characters)

Default Setting

Aruba_VAP_G 0

Command Mode

Interface Configuration (Wireless) VAP

Command Usage

Clients that want to connect to the wireless network via an access point must set their SSIDs to the same as that of the access point.

Example

This example sets the SSID to **RD-AP#3** for the 802.11g interface.

```
AP(if-wireless g)#ssid RD-AP#3
```

super-g or super-a

This command sets parameters for the Atheros proprietary Super G performance enhancements. Enhancements include bursting, compression, fast frames and dynamic turbo. Maximum throughput ranges from 40 to 60 Mbps for connections to Atheros compatible clients,

Syntax

```
super-g  
super-a
```

Default Setting

disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

Example

This example enables the Super G enhancements.

```
Aruba Networks AP-80MB(if-wireless g)#super-g
```

transmit-key

This command sets the index of the WEP key to be used for encrypting data frames broadcast or multicast from the wireless bridge.

Syntax

```
transmit-key <index>
```

- *index* - Key index (range: 1-4)

Default Setting

1

Command Mode

Interface Configuration (Wireless)

Command Usage

If you use WEP key encryption, the wireless bridge uses the transmit key to encrypt multicast and broadcast data signals that it sends to other nodes. Other keys can be used for decryption of data from other nodes.

Example

This example sets the transmit key index to **2**.

```
Aruba Networks AP-80MB(if-wireless a)#transmit-key 2
```

transmit-power

This command adjusts the power of the radio signals transmitted from the wireless bridge.

Syntax

```
transmit-power <signal-strength>
```

- *signal-strength* - Signal strength transmitted from the wireless bridge (options: full, half, quarter, eighth, min)

Default Setting

full

Command Mode

Interface Configuration (Wireless)

Command Usage

- The “min” option indicates minimum power.
- The longer the transmission distance, the higher the transmission power required. Power selection is not just a trade off between coverage area and maximum data rates. You also have to ensure that high strength signals do not interfere with the operation of other radio devices in your area.

Example

This example sets the transmit power to half of the available power.

```
Aruba Networks AP-80MB(if-wireless a)#transmit-power half
```

turbo

This command sets the wireless bridge to an enhanced mode (not regulated in IEEE 802.11a) that provides a higher data rate of up to 108 Mbps.

Syntax

```
turbo {dynamic | static}
```

- **dynamic** - Access point uses Turbo mode only when no neighboring access points are active or detected.
- **static** - Access point always uses Turbo mode.

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless - 802.11a)

Command Usage

- The normal 802.11a wireless operation mode provides connections up to 54 Mbps. Turbo Mode is an enhanced mode (not regulated in IEEE 802.11a) that provides a higher data rate of up to 108 Mbps. Enabling Turbo Mode allows the wireless bridge to provide connections up to 108 Mbps.
- Choose the dynamic option to use Turbo mode only when no neighboring access points are active or detected, or choose static to always use Turbo mode.

Example

This example sets the wireless bridge to turbo mode.

```
Aruba Networks AP-80MB(if-wireless a)#turbo
```

vap

This command provides access to the VAP (Virtual Access Point) interface configuration mode.

Syntax

```
vap <vap-id>
```

- *vap-id* - The number that identifies the VAP interface. (Options: 0-3)

Default Setting

None

Command Mode

Interface Configuration (Wireless)

Example

This example provides access to VAP 0 for the 802.11g radio.

```
Aruba Networks AP-80MB(config)#interface wireless g
Aruba Networks AP-80MB(if-wireless g)#vap 0
Aruba Networks AP-80MB(if-wireless g: VAP[0])#
```

Rogue AP Detection Commands

A “rogue AP” is either an access point that is not authorized to participate in the wireless network, or an access point that does not have the correct security configuration. Rogue APs can potentially allow unauthorized users access to the network. Alternatively, client stations may mistakenly associate to a rogue AP and be prevented from accessing network resources. Rogue APs may also cause radio interference and degrade the wireless LAN performance.

The access point can be configured to periodically scan all radio channels and find other access points within range. A database of nearby access points is maintained where any rogue APs can be identified.

Table 34 *Rogue AP Detection Commands*

Command	Function	Mode
<code>rogue-ap authenticate</code>	Enables identification of all access points	GC
<code>rogue-ap duration</code>	Sets the duration that all channels are scanned	GC
<code>rogue-ap enable</code>	Enables the periodic detection of other nearby access points	GC
<code>rogue-ap interval</code>	Sets the time between each scan	GC
<code>rogue-ap scan</code>	Forces an immediate scan of all radio channels	GC
<code>show rogue-ap</code>	Shows the current database of detected access points	Exec

rogue-ap authenticate

This command forces the unit to authenticate all access points on the network. Use the `no` form to disable this function.

Syntax

```
rogue-ap authenticate
no rogue-ap authenticate
```

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

Enabling authentication in conjunction with a database of approved access points stored on a RADIUS server allows the access point to discover rogue APs. With authentication enabled and a configure RADIUS server, the access point checks the MAC address/Basic Service Set Identifier (BSSID) of each access point that it finds against a RADIUS server to determine whether the access point is allowed. With authentication disabled, the access point can identify its neighboring access points only; it cannot identify whether the access points are allowed or are rogues. If you enable authentication, you should also configure a RADIUS server for this access point (see [“RADIUS Client Commands” on page 149](#)).

Example

This example disables the requirement that all access points must be authenticated to associate to the 802.11g interface.

```
Aruba Networks AP-80MB(if-wireless g)#no rogue-ap authenticate
Aruba Networks AP-80MB(if-wireless g)#
```

rogue-ap duration

This command sets the scan duration for detecting access points.

Syntax

```
rogue-ap duration <milliseconds>
```

- *milliseconds* - The duration of the scan. (Range: 100-1000 milliseconds)

Default Setting

350 milliseconds

Command Mode

Interface Configuration (Wireless)

Command Usage

- During a scan, client access may be disrupted and new clients may not be able to associate to the access point. If clients experience severe disruption, reduce the scan duration time.
- A long scan duration time will detect more access points in the area, but causes more disruption to client access.

Example

This example sets the scan duration to **200** milliseconds for the 802.11g interface.

```
Aruba Networks AP-80MB(if-wireless g)#rogue-ap duration 200
Aruba Networks AP-80MB(if-wireless g)#
```

Related Commands

rogue-ap interval (7-117)

rogue-ap enable

This command enables the periodic detection of nearby access points. Use the no form to disable periodic detection.

Syntax

```
[no] rogue-ap enable
```

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

- While the access point scans a channel for rogue APs, wireless clients will not be able to connect to the access point. Therefore, avoid frequent scanning or scans of a long duration unless there is a reason to believe that more intensive scanning is required to find a rogue AP.

A “rogue AP” is either an access point that is not authorized to participate in the wireless network, or an access point that does not have the correct security configuration. Rogue access points can be

identified by unknown BSSID (MAC address) or SSID configuration. A database of nearby access points should therefore be maintained on a RADIUS server, allowing any rogue APs to be identified.

The rogue AP database can be viewed using the **show rogue-ap** command.

- The access point sends Syslog messages for each detected access point during a rogue AP scan.

Example

This example enables rogue AP detection for the 802.11g interface.

```
Aruba Networks AP-80MB(if-wireless g)#rogue-ap enable
configure either syslog or trap or both to receive the rogue APs detected.
Aruba Networks AP-80MB(if-wireless g)#
```

rogue-ap interval

This command sets the interval at which to scan for access points.

Syntax

```
rogue-ap interval <minutes>
```

- *minutes* - The interval between consecutive scans. (Range: 30-10080 minutes)

Default Setting

720 minutes

Command Mode

Interface Configuration (Wireless)

Command Usage

This command sets the interval at which scans occur. Frequent scanning will more readily detect other access points, but will cause more disruption to client access.

Example

This example sets the scan interval to **120** minutes for the 802.11a interface.

```
Aruba Networks AP-80MB(if-wireless a)#rogue-ap interval 120
Aruba Networks AP-80MB(if-wireless a)#
```

Related Commands

rogue-ap duration (7-117)

rogue-ap scan

This command starts an immediate scan for access points on the radio interface.

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

While the access point scans a channel for rogue APs, wireless clients will not be able to connect to the access point. Therefore, avoid frequent scanning or scans of a long duration unless there is a reason to believe that more intensive scanning is required to find a rogue AP.

Example

This example performs a rogue AP scan.

```
Aruba Networks AP-80MB(if-wireless g)#rogue-ap scan
Aruba Networks AP-80MB(if-wireless g)#rogueApDetect Completed (Radio G) : 9 APs
detected
rogueAPDetect (Radio G): refreshing ap database now
Aruba Networks AP-80MB(if-wireless g)#
```

show rogue-ap

This command displays the current rogue AP database.

Syntax

```
show rogue-ap
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show rogue-ap
802.11a Channel : Rogue AP Status
AP Address(BSSID) SSID Channel(MHz) RSSI Type Privacy RSN
=====
802.11g Channel : Rogue AP Status
AP Address(BSSID) SSID Channel(MHz) RSSI Type Privacy RSN
=====
00-04-e2-2a-37-23 WLAN1AP 11(2462 MHz) 17 ESS 0 0
00-04-e2-2a-37-3d ANY 7(2442 MHz) 42 ESS 0 0
00-04-e2-2a-37-49 WLAN1AP 9(2452 MHz) 42 ESS 0 0
00-90-d1-08-9d-a7 WLAN1AP 1(2412 MHz) 12 ESS 0 0
00-30-f1-fb-31-f4 WLAN 6(2437 MHz) 16 ESS 0 0
Aruba Networks AP-80MB#
```

Link Integrity Commands

The access point provides a link integrity feature that can be used to ensure that wireless clients are connected to resources on the wired network. The access point does this by periodically sending Ping messages to a host device in the wired Ethernet network. If the access point detects that the connection to the host has failed, it disables the radio interfaces, forcing clients to find and associate with another

access point. When the connection to the host is restored, the access point re-enables the radio interfaces.

Table 35 *Link Integrity Commands*

Command	Function	Mode
<code>link-integrity ping-detect</code>	Enables link integrity detection	GC
<code>link-integrity ping-host</code>	Specifies the IP address of a host device in the wired network	GC
<code>link-integrity ping-interval</code>	Specifies the time between each Ping sent to the link host	GC
<code>link-integrity ping-fail-retry</code>	Specifies the number of consecutive failed Ping counts before the link is determined as lost	GC
<code>link-integrity ethernet-detect</code>	Enables integrity check for Ethernet link	GC
<code>show link-integrity</code>	Displays the current link integrity configuration	Exec

link-integrity ping-detect

This command enables link integrity detection. Use the no form to disable link integrity detection.

Syntax

```
[no] link-integrity ping-detect
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- When link integrity is enabled, the IP address of a host device in the wired network must be specified.
- The access point periodically sends an ICMP echo request (Ping) packet to the link host IP address. When the number of failed responses (either the host does not respond or is unreachable) exceeds the limit set by the link-integrity ping-fail-retry command, the link is determined as lost.

Example

```
Aruba Networks AP-80MB(config)#link-integrity ping-detect
Aruba Networks AP-80MB(config)#
```

link-integrity ping-host

This command configures the link host name or IP address. Use the no form to remove the host setting.

Syntax

```
link-integrity ping-host <host_name | ip_address>
```

```
no link-integrity ping-host
```

- *host_name* - Alias of the host.
- *ip_address* - IP address of the host.

Default Setting

None

Command Mode

Global Configuration

Example

```
Aruba Networks AP-80MB(config)#link-integrity ping-host 192.168.1.10
Aruba Networks AP-80MB(config)#
```

link-integrity ping-interval

This command configures the time between each Ping sent to the link host.

Syntax

```
link-integrity ping-interval <interval>
```

- *interval* - The time between ping messages. (Range: 5 - 60 seconds)

Default Setting

30 seconds

Command Mode

Global Configuration

Example

```
Aruba Networks AP-80MB(config)#link-integrity ping-interval 50
Aruba Networks AP-80MB(config)#
```

link-integrity ping-fail-retry

This command configures the number of consecutive failed ping counts before the link is determined as lost.

Syntax

```
link-integrity ping-fail-retry <counts>
```

- *counts* - The number of failed ping counts before the link is determined as lost. (Range: 1 - 10)

Default Setting

6

Command Mode

Global Configuration

Example

```
Aruba Networks AP-80MB(config)#link-integrity ping-fail-retry 5
Aruba Networks AP-80MB(config)#
```

link-integrity ethernet-detect

This command enables an integrity check to determine whether or not the access point is connected to the wired Ethernet.

Syntax

```
[no] link-integrity ethernet-detect
```

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Aruba Networks AP-80MB(config)#link-integrity ethernet-detect
Aruba Networks AP-80MB(config)#
```

show link-integrity

This command displays the current link integrity configuration.

Syntax

```
show link-integrity
```

Command Mode

Exec

Example

```
Aruba Networks AP-80MB#show link-integrity

Link Integrity Information
=====
Ethernet Detect : Disabled
Ping Detect     : Disabled
Target IP/Name : 0.0.0.0
Ping Fail Retry : 6
Ping Interval  : 50
=====
Aruba Networks AP-80MB#
```

IAPP Commands

The command described in this section enables the protocol signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points. In other words, the Inter Access-Point Protocol (IAPP), as defined by IEEE standard 802.11f, can ensure successful roaming between access points in a multi-vendor environment.

iapp

This command enables the protocol signaling required to hand over wireless clients roaming between different 802.11f-compliant access points. Use the **no** form to disable 802.11f signaling.

Syntax

```
iapp
no iapp
```

Default

Enabled

Command Mode

Global Configuration

Command Usage

The current 802.11 standard does not specify the signaling required between access points in order to support clients roaming from one access point to another. In particular, this can create a problem for clients roaming between access points from different vendors. This command is used to enable or disable 802.11f handover signaling between different access points, especially in a multi-vendor environment.

Example

This example enables IAPP.

```
AP(config)#iapp
```

VLAN Commands

The wireless bridge can enable the support of VLAN-tagged traffic passing between the wireless interface and the wired network.

The wireless bridge tags traffic passing to the wired network with the assigned VLAN ID. Traffic received from the wired network must also be tagged with the same VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.

The VLAN commands supported by the wireless bridge are listed below.

Table 36 *VLAN Commands*

Command	Function	Mode
<code>management-vlanid</code>	Sets the ID for the management VLAN	GC
<code>untagged-vlanid</code>	Sets the default VLAN ID for incoming packets	GC

Table 36 VLAN Commands (Continued)

Command	Function	Mode
vlan-id	Configures the default VLAN ID for the VAP interface	GC

management-vlanid

This command sets the ID for the management VLAN.

Syntax

```
management-vlanid <id>
```

- *id* - VLAN ID (1-4096)

Default

1

Command Mode

Global Configuration

Example

This example assigns VLAN ID **2** for the management VLAN.

```
AP(config)#management-vlanid 2
AP(config)#
```

untagged-vlanid

This command sets the default VLAN ID for incoming packets.

Syntax

```
untagged-vlanid <id>
```

- *id* - VLAN ID (1-4096)

Default Setting

None

Command Mode

Interface Ethernet

Example

This example assigns VLAN ID **10** for untagged packets.

```
Aruba Networks AP-80MB(if-ethernet)#untagged-vlanid 10
```

vlan-id

This command configures the default VLAN ID for the VAP interface.

Syntax

vlan-id <vlan-id>

- **vlan-id** - Native VLAN ID. (Range: 1-4094)

Default Setting

1

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- To implement the default VLAN ID setting for VAP interface, the access point must enable VLAN support using the `vlan` command.
- When VLANs are enabled, the access point tags frames received from wireless clients with the default VLAN ID for the VAP interface. If IEEE 802.1X is being used to authenticate wireless clients, specific VLAN IDs can be configured on the RADIUS server to be assigned to each client. Using IEEE 802.1X and a central RADIUS server, up to 64 VLAN IDs can be mapped to specific wireless clients.
- If the VLAN ID has not been configured for a client on the RADIUS server, then the frames are tagged with the default VLAN ID of the VAP interface.

Example

WMM Commands

The access point implements QoS using the Wi-Fi Multimedia (WMM) standard. Using WMM, the access point is able to prioritize traffic and optimize performance when multiple applications compete for wireless network bandwidth at the same time. WMM employs techniques that are a subset of the developing IEEE 802.11e QoS standard and it enables the access point to inter-operate with both WMM enabled clients and other devices that may lack any WMM functionality.

The WMM commands supported by the access point are listed below.

Table 37 *WMM Commands*

Command	Function	Mode
<code>wmm</code>	Sets the WMM operational mode on the access point	IC-W
<code>wmm-acknowledge-policy</code>	Allows the acknowledgement wait time to be enabled or disabled for each Access Category (AC)	IC-W
<code>wmmparam</code>	Configures detailed WMM parameters that apply to the access point (AP) or the wireless clients (BSS)	IC-W

wmm

This command sets the WMM operational mode on the access point. Use the no form to disable WMM.

Syntax

```
wmm {supported | required}
no wmm {supported | required}
```

- supported - WMM will be used for any associated device that supports this feature. Devices that do not support this feature may still associate with the access point.
- required - WMM must be supported on any device trying to associated with the access point. Devices that do not support this feature will not be allowed to associate with the access point.

Default

supported

Command Mode

Interface Configuration (Wireless)

Example

This example specifies that WMM operational mode is required for the 802.11a interface.

```
Aruba Networks AP-80MB(if-wireless a)#wmm required
Aruba Networks AP-80MB(if-wireless a)#
```

wmm-acknowledge-policy

This command allows the acknowledgement wait time to be enabled or disabled for each Access Category (AC).

Syntax

```
wmm-acknowledge-policy <ac_number> {ack | noack}
```

- *ac_number* - Access categories. (Range: 0-3; 0 = BE, 1 = BK, 2= VI, 3= VO)
- **ack** - Require the sender to wait for an acknowledgement from the receiver.
- **noack** - Does not require the sender to wait for an acknowledgement from the receiver.

Default

ack

Command Mode

Interface Configuration (Wireless)

Command Usage

- WMM defines four access categories (ACs) – voice, video, best effort, and background. These categories correspond to traffic priority levels and are mapped to IEEE 802.1D priority tags (see Table 6-1). The direct mapping interpretability with other wired network QoS policies. While the four ACs are specified for specific types of traffic, WMM allows the priority levels to be configured to match any network-wide QoS policy. WMM also specifies a protocol that access points can use to communicate the configured traffic priority levels to QoS-enabled wireless clients.

- Although turning off the requirement for the sender to wait for an acknowledgement can increase data throughput, it can also result in a high number of errors when traffic levels are heavy.

Example

This example configures the 802.11a interface so that acknowledgement is not required for voice access.

```
Aruba Networks AP-80MB(if-wireless a)#wmm-acknowledge-policy 0 noack
Aruba Networks AP-80MB(if-wireless a)#
```

wmmparam

This command configures detailed WMM parameters that apply to the access point (AP) or the wireless clients (BSS).

Syntax

```
wmmparam {AP | BSS} <ac_number> <LogCwMin> <LogCwMax> <AIFS> <TxOpLimit>
<admission_control>
```

- **AP** - Access Point
- **BSS** - Wireless client
- *ac_number* - Access categories. (Range: 0-3; 0 = BE, 1 = BK, 2= VI, 3= VO). These categories correspond to traffic priority levels and are mapped to IEEE 802.1D priority tags as shown in Table 6-1. (Range: 0-3)
- *LogCwMin* - Minimum log value of the contention window. This is the initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the LogCwMin value. Specify the LogCwMin value. Note that the LogCwMin value must be equal or less than the LogCwMax value. (Range: 1-15 microseconds)
- *LogCwMax* - Maximum log value of the contention window. This is the maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the LogCwMax value. Note that the CWMax value must be greater or equal to the LogCwMin value. (Range: 1-15 microseconds)
- *AIFS* - Arbitrary InterFrame Space specifies the minimum amount of wait time before the next data transmission attempt. (Range: 1-15 microseconds)
- *TXOPLimit* - Transmission Opportunity Limit specifies the maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TxOpLimit. This data bursting greatly improves the efficiency for high data-rate traffic. (Range: 0-65535 microseconds)
- *admission_control* - The admission control mode for the access category. When enabled, clients are blocked from using the access category. (Options: 0 to disable, 1 to enable)

Command Mode

Interface Configuration (Wireless)

Example

This example sets the following WMM AP parameters for the 802.11a interface: AC=0, LogCwMin=4, LogCwMax=6, AIFS=3, TxOpLimit= 1, admission_contro=1.

```
Aruba Networks AP-80MB(if-wireless a)#wmmparams ap 0 4 6 3 1 1
Aruba Networks AP-80MB(if-wireless a)#
```


This chapter includes some basic verifications that you should perform before you contact your local Technical Support.

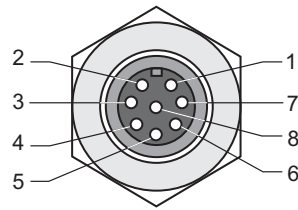
1. If wireless bridge units do not associate with each other, check the following:
 - Check the power injector LED for each bridge unit to be sure that power is being supplied.
 - Be sure that antennas in the link are properly aligned.
 - Be sure that channel settings match on all bridges.
 - If encryption is enabled, ensure that all bridge links are configured with the same encryption keys.
2. If wireless clients cannot access the network, check the following:
 - Be sure the access point and the wireless clients are configured with the same Service Set ID (SSID).
 - If authentication or encryption are enabled, ensure that the wireless clients are properly configured with the appropriate authentication or encryption keys.
 - If authentication is being performed through a RADIUS server, ensure that the clients are properly configured on the RADIUS server.
 - If authentication is being performed through IEEE 802.1X, be sure the wireless users have installed and properly configured 802.1X client software.
 - If MAC address filtering is enabled, be sure the client's address is included in the local filtering database or on the RADIUS server database.
 - If the wireless clients are roaming between access points, make sure that all the access points and wireless devices in the Extended Service Set (ESS) are configured to the same SSID, and authentication method.
3. If you experience poor performance (such as a high rate of packet loss) over the wireless bridge link:
 - Check that the range of the link is within the limits for the antennas used.
 - Be sure that antennas in the link are properly aligned.
 - Check that there is an unobstructed radio line of sight between the antennas.
 - Be sure there is no interference from other radio sources. Try setting the bridge link to another radio channel.
 - Be sure there is no other radio transmitter too close to either antenna. If necessary, move the antennas to another location.
4. If the wireless bridge cannot be configured using Telnet, a web browser, or SNMP software:
 - Be sure you have configured the wireless bridge with a valid IP address, subnet mask and default gateway.
 - Check that you have a valid network connection to the wireless bridge and that the Ethernet port or the wireless interface has not been disabled.
 - If you are connecting to the wireless bridge through the wired Ethernet interface, check the network cabling between the management station and the wireless bridge.
 - If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted (four sessions). Try connecting again at a later time.

5. If all other recovery measures fail, and the wireless bridge is still not functioning properly, take any of these steps:
 - Reset the wireless bridge's hardware using the CLI, web interface, or through a power reset.
 - Reset the wireless bridge to its default configuration.
6. If you forgot or lost the password:
 - Contact Technical Support.

Aruba 80 8-Pin DIN Ethernet Connector Pinout

The Ethernet cable from the power injector connects to an 8-pin DIN connector on the Aruba 80 outdoor wireless Access Point. This IP67 8-pin male (pole) M12 circular DIN connector (with gold-plated (Au) contacts) is described below.

8-Pin DIN Ethernet Port Pinout	
Pin	Signal Name
1	Transmit Data plus (TD+)
2	Transmit Data minus (TD-)
3	Receive Data plus (RD+)
4	+48 VDC power
5	+48 VDC power
6	Receive Data minus (RD-)
7	Return power
8	Return power



Note: The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Aruba 80 8-Pin DIN to RJ-45 Cable Wiring

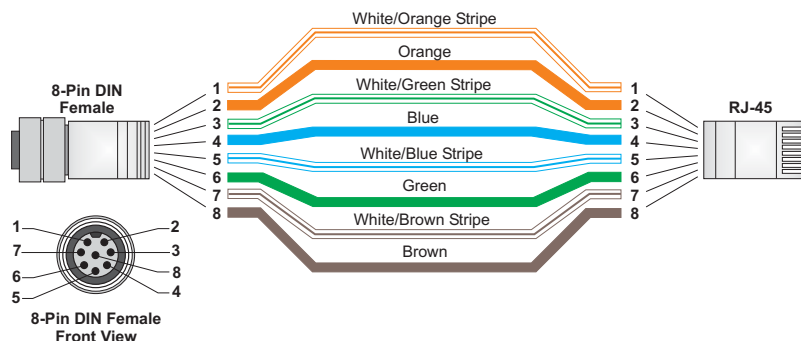
The AP port to the wireless access point's 8-pin DIN connector uses straight-through IEEE standards based Ethernet, illustrated in the diagram below. Use Category 5 or better UTP or STP cable and be sure to connect all four wire pairs.



Make sure that the combined length of any wiring connection between the Mobility Controller and the PoE injector, and the PoE injector to the AP does not exceed 90 meters (295 feet).



To construct a reliable Ethernet cable, always use the proper tools or ask a professional cable supplier to construct the cable.



Aruba 80 Power over Ethernet Injector Module 10/100BASE-TX Pin Assignments

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections, or 100-ohm Category 5 or better cable for 100 Mbps connections.



Make sure that the combined length of any twisted-pair connection between the Mobility Controller and the PoE injector, and the PoE injector to the access point does not exceed 90 meters (295 feet).

The RJ-45 Ethernet port on the power injector is wired with MDI pinouts. This means that you must use crossover cables for connections to PCs or servers, and straight-through cable for connections to switches or hubs. However, when connecting to devices that support automatic MDI/MDI-X pinout configuration, you can use straight-through cabling.

10/100BASE-TX MDI and MDI-X Port Pinouts		
Pin	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)
4,5,7,8	Not used	Not used

Note: The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

Product Features

- Wireless dual-band transceiver
- Various antenna options
- Protocol-independent networking functionality
- Supports IEEE 802.11a or IEEE 802.11b/g operation as an AP
- Supports IEEE 802.11a and IEEE 802.11b/g operation as an AM
- Seamless connectivity to wired LANs augment existing networks quickly and easily

Ethernet Compatibility

The Aruba AP 80 Outdoor Wireless Access Point/Bridge attaches to 10/100 Mbps Ethernet (FE) LAN segments that utilize 10Base-T/100Base-TX (twisted-pair) wiring. The device appears as an Ethernet node and performs a routing function by moving packets between the wired LAN and remote workstations on the wireless infrastructure.

Power Over Ethernet

The Aruba AP 80 Outdoor Wireless Access Point/Bridge supports non-standard Power Over Ethernet (POE) using the Aruba 80 POE Injector Module, due to its 30W power draw requirement.

Radio Characteristics

The Aruba AP 80 Outdoor Wireless Access Point/Bridge can be configured to support IEEE 802.11a or IEEE 802.11b/g operation as an AP, and supports both IEEE 802.11a and IEEE 802.11b/g operation as an AM (where allowed):

- 802.11a provides a high data rate and reliable wireless connectivity
802.11a operation uses a radio modulation technique known as Orthogonal Frequency Division Multiplexing (OFDM), and a shared collision domain (CSMA/CA). It operates in the 5 GHz Unlicensed National Information Infrastructure (UNII) band. Data is transmitted over a half-duplex radio channel operating at up to 54 Megabits per second (Mbps), and with a maximum operating range up to 503 m (1650 ft.).
- 802.11b provides an alternative to wired LANs that can dramatically cut costs
802.11b operation uses the IEEE 802.11 High-Rate Direct Sequence (HRDS) specification, and a shared collision domain (CSMA/CA). It operates in the 2.4 GHz Industrial/Scientific/Medical (ISM) band. The ISM band is available worldwide for unlicensed use. Data is transmitted at speeds of up to 11 Mbps, and with a maximum operating range of up to 396 m (1300 ft.).
- 802.11g provides a high data rate and is backwards compatible with 802.11b.
802.11g operation uses OFDM and a shared collision domain (CSMA/CA). It operates in the 2.4 GHz Industrial/Scientific/Medical (ISM) band. The ISM band is available worldwide for unlicensed use. Data is transmitted at speeds of up to 54 Mbps.

Compliance

United States



FCC - Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for fixed indoor use only. This equipment should be installed and operated with a minimum distance of 38.5 centimeters (15.2 inches) between the radiator and your body for 2.4 GHz and 5 GHz operations. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radio Frequency Interference Requirements

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. The FCC requires this product to be used indoors to reduce the potential for harmful interference to co-channel Mobile Satellite systems. High power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with and/or damage this device.

Canada

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministère des Communications.

The use of this device operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

RSS-210

This device, when operated in the 5150-5250 MHz frequency range, is only for indoor use.



High power radars are allocated as primary users (meaning they have priority) in the 5250-5350 MHz and 5650-5850 MHz frequency ranges, and these radars could cause interference and/or damage to LE-LAN devices.

RSS-Gen

This device has been designed to operate with the antennas listed at [on page 230](#) and [on page 231](#), and having a maximum gain of 15.0dBi for 2.4GHz and 14.0dBi for 5GHz. Antennas not included in this list or having a gain greater than 15.0dBi for 2.4GHz and 14.0dBi for 5GHz are strictly prohibited for use with this device. The required antenna impedance is 50 Ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that permitted for successful communication.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Japan

Indoor Restriction for 5GHz Frequency Range

この製品は法律により、5GHz帯での屋外使用を禁じられています。

VCCI - Class B

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると受信障害を引き起こすことがあります。
取り扱い説明書に従って正しい取り扱いをして下さい。

Korea

Class B Equipment (Household purpose info/telecommunication equipment)

As this equipment has undergone EMC registration for household purpose, this product can be used in any area including residential area.



Turbo mode is disabled in Korea.

B급 기기 (가정용 정보통신기기)

이 기기는 가정용으로 전자파적합등록을 한 기기로서
주거지역에서는 물론 모든지역에서 사용할 수 있습니다.

Europe



This is a Class B product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures

This product complies with Directive 1999/5/EC as well as with EN5022 Class B and EN5024 standards.

Taiwan

Low-power, radio-frequency devices must not be altered by changing the operating frequency, increasing emission power, adding external antennas, and changing other original design features and functions.

The operation of low-power, radio-frequency devices must not cause harmful interference, and that interference caused by the operation of authorized radio stations, by another intentional or unintentional radiator, by industrial, scientific, and medical (ISM) equipment, or by an incidental radiator must be accepted. If interference is caused, the user must immediately stop operating the low-power, radio-frequency device and not resume operation until all harmful interference is cleared.

Maximum Distance

Maximum distances posted below are the actual tested distance thresholds. However, there are many variables such as barrier composition and construction and local environmental interference that may impact your actual distances and cause you to experience distance thresholds far lower than those we post below:

Table 38 IEEE 802.11a Maximum Distances

Condition	Speed (Mbps)							
	54	48	36	24	18	12	9	6
Outdoor Environment	40 m (132 ft.)	221 m (726 ft.)	251 m (825 ft.)	322 m (1056 ft.)	350 m (1155 ft.)	382 m (1254 ft.)	453 m (1485 ft.)	503 m (1650 ft.)
Indoor Environment	18 m (60 ft.)	25 m (82 ft.)	30 m (99 ft.)	35 m (115 ft.)	40 m (132 ft.)	45 m (149 ft.)	48 m (157 ft.)	50 m (165 ft.)

Table 39 IEEE 802.11b Maximum Distances

Condition	Speed (Mbps)			
	11	5.5	2	1
Outdoor Environment	152 m (500 ft.)	233 m (766 ft.)	315 m (1033 ft.)	396 m (1300 ft.)
Indoor Environment	23 m (75 ft.)	30 m (100 ft.)	61 m (200 ft.)	61 m (200 ft.)

An Outdoor Environment is a line-of-sight environment with no interference or obstruction between the access point and clients.

An Indoor Environment is a typical office or home environment with floor to ceiling obstructions between the access point and clients.

Sensitivity and Modulation

Table 40 IEEE 802.11a Sensitivity and Modulation

Modulation/Rates	Sensitivity (dBm)	5.15-5.25GHZ (dBm)	5.25-5.35GHZ (dBm)
BPSK (6 Mbps)	-85	16	20
BPSK (9 Mbps)	-84	16	20
QPSK (12 Mbps)	-83	16	19
QPSK (18 Mbps)	-81	16	19
16 QAM (24 Mbps)	-78	16	18
16 QAM (36 Mbps)	-74	16	18
64 QAM (48 Mbps)	-69	16	16
64 QAM(54 Mbps)	-65	14	14

Table 41 IEEE 802.11b Sensitivity and Modulation

Modulation/Rates	Sensitivity (dBm)	2.412-2.484GHZ (dBm)
DBPSK (1 Mbps)	-86	20
DQPSK (2 Mbps)	-85	17
PBCC (5.5 Mbps)	-85	15
CCK (5.5 Mbps)	-81	13
PBCC (11 Mbps)	-83	7
CCK (11 Mbps)	-81	0

Specifications

Table 42 *Aruba 80 802.11 Specifications^a*

Description	802.11a	802.11b/g
External Antenna	Aruba offer a wide variety of detachable antenna types suitable for use with the Aruba AP-80 MB/SB. Please contact your local sales representative for details	
Frequency Band	<ul style="list-style-type: none"> 5.150 ~ 5.250 GHz, channels country-specific 5.250 ~ 5.350 GHz (ETSI), channels country-specific 5.470 ~ 5.725 GHz, channels country-specific 5.725 ~ 5.825/5.850 GHz, channels country-specific and in Taiwan 5ch (normal mode), 2ch (turbo mode) <p>Note: Radio frequency band 5.150 ~ 5.725 GHz not supported in Taiwan</p> <ul style="list-style-type: none"> For Korea, 5.725-5.850 GHz only 	<ul style="list-style-type: none"> 2.4 ~ 2.4835 GHz <p>Channels country-specific</p>
Operating Channels	<ul style="list-style-type: none"> US, Canada - 13 ETSI - up to 19 Japan - disabled 	<ul style="list-style-type: none"> US, Canada - 11 ETSI - 13 Japan - 13
Radio Technology	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS) Orthogonal Frequency Division Multiplexing (OFDM)
Modulation Type	BPSK, QPSK, 16-QAM, 64-QAM	CCK, BPSK, QPSK, 16-QAM, 64-QAM
Transmit Power	Configurable by system administrator/ professional installer	Configurable by system administrator/ professional installer
Media Access Control	CSMA/CA with ACK	CSMA/CA with ACK
Data Rates	6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel. 108 Mbps in Turbo mode.	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel. 108 Mbps in Turbo mode.

a. Not all frequencies or frequency bands are available to all countries. Frequencies are enabled or disabled on a country-specific basis and are not configurable by the user.

Table 43 *Aruba 80 Characteristics²*

Description	
Maximum Clients	128
Multi-mode Radio Band	Selectable via software

Table 43 Aruba 80 Characteristics² (Continued)

Description	
Manageability:	<ul style="list-style-type: none"> • Management of all 802.11 parameters as AP • Network-wide AP management via: <ul style="list-style-type: none"> • Telnet • WEB GUI • SNMP • Access point profiles • Management by: <ul style="list-style-type: none"> • Geographical location • BSSID • Radio type • Encryption support (AP and Switch) <ul style="list-style-type: none"> • 40-bit / 64-bit / 128-bit / 152-bit WEP, • TKIP, AES, WPA, WPA2
Encryption Support (AP and Mobility Controller)	40bit / 64bit / 128bit / 152bit WEP, TKIP, AES, WPA, WPA2.0
Physical (HxWxD):	<ul style="list-style-type: none"> • 198 x 198 x 70mm (7.80 x 7.80 x 2.76 in.) Weight 1.6 kilograms (3.53 pounds)
Part Numbers	<ul style="list-style-type: none"> • AP-80SB—Aruba 80 Slave Outdoor Wireless Access Point/Bridge • AP-80MB—Aruba 80 Master Outdoor Wireless Access Point/Bridge • AP-AC-80-1—Indoor-rated Power Injector Kit
Interfaces (Electrical):	<p>AP-80 MB/SB Common Interfaces</p> <ul style="list-style-type: none"> • 1 x 10/100 Base-TX auto-sensing Ethernet interface (IP67 8-pin male (pole) M12 circular DIN connector Au contacts): <ul style="list-style-type: none"> • Auto-sensing MDI/MDX • PoE 48V DC / 1.2A (30W) power over Ethernet (non-standard 802.3af) • Integral lightning arrester • 1 x 2.4GHz N-type female antenna interface • 1 x 5GHz N-type female antenna interface • 1 x Electrical ground / Safety terminal • 1 x Integral ENET lightning arrester <p>Power Adapter Interfaces</p> <p>AP (Access Point) Port</p> <ul style="list-style-type: none"> • 1 x 10/100 Base-TX auto-sensing Ethernet (RJ-45) network (AP) interface: <ul style="list-style-type: none"> • Auto-sensing MDI/MDX • PoE 48V DC / 1.2A power over Ethernet (non-standard 802.3af) <p>ENET (Network) Port</p> <ul style="list-style-type: none"> • 1 x 10/100 Base-TX auto-sensing Ethernet (RJ-45) network (ENET), auto-sensing MDI/MDX Ethernet interface supplied with 8-pin DIN to RJ-45 CAT-5 Shielded Ethernet cable (50m / 164 ft)
Interfaces (Mechanical):	<ul style="list-style-type: none"> • 4 x Mounting Bracket Hex Screw Mounting Points • Ruggedized wall, pole or mast mount hardware provided (articulating in horizontal and vertical planes)
Visual Indicators (LEDs)	<ul style="list-style-type: none"> • Ready -- Power on/off (provided on Power Injector)

Table 43 Aruba 80 Characteristics² (Continued)

Description	
Power Requirements	AP-80 MB/SB <ul style="list-style-type: none"> DC Input Voltage: 48 VDC DC Input Current: 1.2 A30W (non-standard 802.3af Power over Ethernet) Power Consumption: 30W, maximum External Power Adapter <ul style="list-style-type: none"> AC Input Voltage: 90VAC to 240VAC, auto-sensing AC Input Current: 1.5A @ 110 VAC AC Input Frequency: 47-63 Hz DC Output Voltage: 48VDC DC Output Current: 1.2A POE information: <ul style="list-style-type: none"> Brand: Microelectronics Tech. Inc. Model: TR60A-POE-L (0640-0086) Input: 100-240 V - 1.5 A 47-63 Hz Output: 48V, 1.2A
Environmental:	AP-80 MB/SB <ul style="list-style-type: none"> Temperature: <ul style="list-style-type: none"> Operating: -30 to 55 °C (-22 to 131 °F) Storage: -40 to 80°C (-40 to 176 °F) Humidity 0% to 95% (non-condensing) Altitude: Up to 15,000 feet (4572 m) Survival Wind Speed: 201Km/hr (125 MPH) External Power Adapter <ul style="list-style-type: none"> Temperature: <ul style="list-style-type: none"> Operating: -0 to 40 °C (32 to 104 °F) Storage: -20 to 70°C (-4 to 158 °F) Relative Humidity 15% to 85%
Standards Compliance	<ul style="list-style-type: none"> Ethernet IEEE 802.3 / IEEE 802.3u Wireless IEEE 802.11a/b/g RFC 2516 PPP over Ethernet UL 50 outdoor rating

2. The maximum output power at permitted operating frequencies is preset by country and cannot be increased by the user.

Aruba 80 Detachable Antennas

The following detachable antennas are supported by the Aruba 80.

Table 44 Detachable Antennas

Part Number	Description	Vendor
AP-ANT-80	2.4Ghz / 8.0dBi High-Gain, Omni-Directional Cylindrical Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # S2406BP36NM
AP-ANT-81	2.4Ghz / 8.0dBi High-Gain, 60° Sector Directional Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # S2408PA36NM
AP-ANT-82	2.4Ghz / 12.0dBi High-Gain, Wide-Angle 90° Directional Sector Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # S2401290PA36NM
AP-ANT-83	2.4Ghz / 7.0dBi Wide-Angle 90° Directional Sector Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # S240790PA36NM

Table 44 Detachable Antennas (Continued)

Part Number	Description	Vendor
Not certified for use in Japan.		
AP-ANT-84	2.4Ghz / 5.0dBi Wide-Angle 135° Directional Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # SR24135DA36NM
Not certified for use in Japan.		
AP-ANT-85	2.4Ghz / 15.0dBi High-Gain, Directional Panel Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # S24015P36NM
Not certified for use in Japan.		
AP-ANT-86	5.10Ghz-5.90Ghz / 10.0dBi High-Gain, Omni-Directional Cylindrical Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # S5158WBP36NM
Not certified for use in Japan.		
AP-ANT-87	2.4Ghz-2.5Ghz / 4.90Ghz-5.99Ghz / 7.0dBi Dual-Band, High-Gain, 60° Sector Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # S24497P36NM
Not certified for use in Japan.		
AP-ANT-88	4.90Ghz-5.90Ghz / 10.5dBi Wide-Angle 120° Directional Sector Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # SR49120DA36NM
Not certified for use in Japan.		
AP-ANT-89	5Ghz / 14.0dBi High-Gain, Directional Panel Antenna. N-Type Connector	Indoor / Outdoor Use. Cushcraft Part # S51514WP36NM
Not certified for use in Japan.		

AP-80SB Integrated Antenna

The Aruba AP-80SB includes a 17 dBi integrated flat-panel directional antenna.

Table 45 AP-80SB Integrated Antenna Specifications

Description	
Frequency Range	5.150 - 5.850 GHz For Korea, 5.725-5.850 GHz only
Gain	17 dBi
VSWR	1.8 : 1 max
Polarization	Linear, vertical/horizontal
HPBW	<ul style="list-style-type: none"> ● Horizontal: 20° ● Vertical: 22°
Front-to-Back Ratio	> 25 dB
Power Handling	10 W (cw)
Impedance	50 Ohms
Connector	N-type Female

Proper Disposal of Aruba Equipment

For the most current information on Global Environmental Compliance and Aruba products please see our website at www.arubanetworks.com.

Waste of Electrical and Electronic Equipment



Aruba products at end of life are subject to separate collection and treatment in the EU Member States, Norway, and Switzerland and therefore are marked with the symbol shown at the left (crossed-out wheelie bin). The treatment applied at end of life of these products in these countries shall comply with the applicable national laws of countries implementing Directive 2002/96EC on Waste of Electrical and Electronic Equipment (WEEE).

European Union RoHS



Aruba products also comply with the EU Restriction of Hazardous Substances Directive 2002/95/EC (RoHS). EU RoHS restricts the use of specific hazardous materials in the manufacture of electrical and electronic equipment. Specifically, restricted materials under the RoHS Directive are Lead (including Solder used in printed circuit assemblies), Cadmium, Mercury, Hexavalent Chromium, and Bromine. Some Aruba products are subject to the exemptions listed in RoHS Directive Annex 7 (Lead in solder used in printed circuit assemblies). Products and packaging will be marked with the “RoHS” label shown at the left indicating conformance to this Directive.

China RoHS



Aruba products also comply with China environmental declaration requirements and are labeled with the “EFUP 50” label shown at the left.

有毒有害物质声明 Hazardous Materials Declaration

部件名称 (Parts)	有毒有害物质或元素 (Hazardous Substances)					
	铅 Lead (Pb)	汞 Mercury (Hg)	镉 Cadmium (Cd)	六价铬 Chromium VI Compounds (Cr ⁶⁺)	多溴联苯 Polybrominated Biphenyls (PBB)	多溴二苯醚 Polybrominated Diphenyl Ether (PBDE)
电路板 PCA Board	X	O	O	O	O	O
机械组件 Mechanical Subassembly	X	O	O	O	O	O
<p>O: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T11363-2006标准规定的限量要求以下。 This component does not contain this hazardous substance above the maximum concentration values in homogeneous materials specified in the SJ/T11363-2006 Industry Standard.</p>						
<p>X: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T11363-2006标准规定的限量要求。 This component does contain this hazardous substance above the maximum concentration values in homogeneous materials specified in the SJ/T11363-2006 Industry Standard.</p>						
<p>对销售之日的所售产品, 本表显示, 供应链的电子产品信息产品可能包含这些物质。 This table shows where these substances may be found in the supply chain of electronic information products, as of the date of sale of the enclosed product.</p>						
<p>此标志为针对所涉及产品的环保使用期标志。 某些零部件会有一个不同的环保使用期(例如, 电池单元模块)贴在其产品上。 此环保使用期限只适用于产品是在产品手册中所规定的条件下工作。 The Environment- Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here. The Environment- Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.</p>						



10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

Access Point

An internetworking device that seamlessly connects wired and wireless networks. Access points attached to a wired network support the creation of multiple radio cells that enable roaming throughout a facility.

Advanced Encryption Standard (AES)

An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm than TKIP and WEP.

Authentication

The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

Backbone

The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Basic Service Set (BSS)

A set of 802.11-compliant stations and an access point that operate as a fully-connected wireless network.

Beacon

A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

Broadcast Key

Broadcast keys are sent to stations using 802.1X dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance.

dBm

The unit dBm refers to a precise measure of power based upon the decibel scale, but referenced to the milliwatt: i.e. 1 dBm = .001 Watt. The dBm is often used to describe absolute power level where the point of reference is 1 milliwatt.

Data Encryption Standard (DES)

A widely used method of private key data encryption.

Dynamic Host Configuration Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Encryption

Data passing between the access point and clients can use encryption to protect from interception and eavesdropping.

Ethernet

A popular local area data communications network which accepts transmission from computers and terminals.

Extended Service Set (ESS)

More than one wireless cell can be configured with the same Service Set Identifier to allow mobile users can roam between different cells with the Extended Service Set.

Extensible Authentication Protocol (EAP)

An authentication protocol used to authenticate network clients. EAP is combined with IEEE 802.1X port authentication and a RADIUS authentication server to provide

File Transfer Protocol (FTP)

A TCP/IP protocol used for file transfer.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard used to transmit and receive data over the World Wide Web.

Internet Control Message Protocol (ICMP)

A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

IEEE 802.11a

A wireless standard that supports high-speed communications in the 5 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard supports data rates of 6, 12, 24, and 54 Mbps.

IEEE 802.11g

A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

IEEE 802.1X

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

Inter Access Point Protocol (IAPP)

A protocol that specifies the wireless signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points.

Local Area Network (LAN)

A group of interconnected computer and support devices.

MAC Address

The physical layer address used to uniquely identify network nodes.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical master-slave configuration in order to synchronize local clocks within the subnet with global time standards via wire or radio.

Open System

A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

Orthogonal Frequency Division Multiplexing (OFDM)

OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

Power over Ethernet (PoE)

A specification for providing both power and data to low-power network devices using a single Category 5 Ethernet cable. PoE provides greater flexibility in the locating of access point's and network devices, and significantly decreased installation costs.

RADIUS

A logon authentication protocol that uses software running on a central server to control access to the network.

Roaming

A wireless LAN mobile user moves around an ESS and maintains a continuous connection to the infrastructure network.

Rogue AP

An access point that is not authorized to participate in the wireless network or does not have the correct security configuration.

Receive Signal Strength Indication (RSSI)

A measure of the signal strength of a received wireless signal (dBm).

RTS Threshold

The Request to Send/Clear to Send (RTS/CTS) mechanism can solve the problem where transmitters contending for the medium may not be aware of each other. If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

Service Set Identifier (SSID)

An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

Session Key

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Shared Key

A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy (WEP) algorithm.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Temporal Key Integrity Protocol (TKIP)

A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Turbo mode

Mode for enhanced wireless data rates of up to 108 Mbps. This mode is not regulated in IEEE 802.11a.

Virtual Access Point (VAP)

A logical access point that is implemented within a physical device. VAP technology allows one physical access point to operate as multiple access points.

Virtual LAN (VLAN)

Logical structure that allows multiple devices to function as if they are on one LAN even though they may be physically located on different LANs. VLAN tagging is the method by which packets are directed to specific VLANs.

Wi-Fi Protected Access

WPA employs 802.1X as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.

Wired Equivalent Privacy (WEP)

WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key are excluded from network traffic.

WPA Pre-shared Key (PSK)

PSK can be used for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access.

Symbols

Numerics

802.1x	
overview	74
802.1x authentication	94
802.1x supplicant	55
description	55

A

access point	
mode	70
rogue	80
topology example	33
administration parameters	64
Advanced Encryption Standard <i>See</i> AES.	
AES	92
AES, configuring	192
antenna	
extension	12
antennas	
aligning	23
connecting external	21
data rates and distance	27, 28
diversity	82
external connector	14
external options	15
height and clearance	30
integrated	14
location	81
point-to-multipoint	23
point-to-point	23
polarization	31
position and orientation	31
AP management	63
AP-80 MB/SB	
about	11
antenna requirements	11
compliance	224
connecting Ethernet cables	21
connecting external antennas	21
connecting power injector	22
external antenna options	15

initial setup	38
logging in	45
management interfaces	35
optional items	12
package contents	12
pole mounting	18
pole mounting, large diameter	19
ports and connectors	14
specifications	223
wall mounting	20
AP-80MB	
features	11
hardware overview	14
AP-80SB	
features	11
hardware overview	13
ASCII WEP key	88
Atheros enhancements	
super a, super g enhancements	81
Atheros super-g or super a	203
authentication	187
802.1x	55
configuring	54, 187
MAC address	55, 160, 161
MAC, timing	55
open	84
type	42
types	84
auto sync channel	71
B	
backing up configuration	66
beacon	
interval	81, 188
rate	81, 191
BPDU	72
bridge	71
child	72
mode	71
priority	73
C	
cable wiring	221
channel	80, 189

auto sync	71	fragmentation length	193
cipher suite	93	hide-ssid	193
Clear To Send <i>See</i> CTS		iapp	213, 214
CLI	55	interface ethernet	180
CLI command modes	105	interface wireless	194
command line interface <i>See</i> CLI		ip address	180
commands		ip dhcp	181
802.1x broadcast-key-refresh-rate	156	ip http port	121
802.1x session-key-refresh-rate	156	ip http server	122
802.1x session-timeout	157	ip http session-timeout	122
802.1x supplicant	158	ip https port	123
802.1x supported	157	ip https server	123
address filter default	160	ip ssh-server enable	118
address filter delete	161	ip ssh-server port	119
address filter entry	161	ip telnet-server enable	119
antenna	185	key	194
ant-gain-reduction	185	link-integrity ethernet-detect	212
APmgmtIP	117	link-integrity ping-detect	210
APmgmtUI	118	link-integrity ping-fail-retry	211
assoc-timeout-interval	186	link-integrity ping-host	210
auth	187	link-integrity ping-interval	211
auth-timeout-value	186	logging clear	126
beacon interval	188	logging console	126
bootfile	146	logging facility-type	126
bridge	189	logging host	127
bridge channel-auto-sync	168	logging level	127
bridge dynamic-entry	173	logging on	128
bridge dynamic-entry age-time	170	mac-authentication server	162
bridge mode	167	mac-authentication session-timeout	162
bridge role	168	max-association	195
bridge stp forwarding-delay	174	MIC_mode	195
bridge stp hello-time	174	multicast-data-rate	196
bridge stp max-age	175	password	120
bridge stp priority	176	ping	110
bridge stp-enable	173	pmksa-lifetime	197
bridge-link child	169	preamble	196
bridge-link parent	169	pre-authentication	198
channel	189	prompt	115
cipher-suite	190	protection method	198
copy	147	radio-mode	199
country	113	radius-server address	150
delete	148	radius-server enable	150
description	191	radius-server key	151
dhcp-relay	134	radius-server port	151
dhcp-relay enable	134	radius-server port-accounting	152
dir	148	radius-server radius-mac-format	152
dns	179	radius-server retransmit	153
dtim period	191	radius-server timeout	153
encryption	192	radius-server timeout-interim	154
end	109	radius-server vlan-format	154
exit	109	rogue-ap authenticate	206
filter ap-manage	164	rogue-ap duration	207
filter bridge	163	rogue-ap enable	207
filter ethernet-type protocol	165	rogue-ap interval	208
filter uplink	164	rogue-ap scan	208
filter uplink enable	164	rssi	199
		rts threshold	200
		show apmanagement	120

show authentication	159	wmmparam	217
show bootfile	149	community name, configuring	58, 136
show bridge aging-time	170, 176	compliance	224
show bridge filter-entry	171, 177	configuration	
show bridge link	171, 177	advanced options	46
show bridge stp	178	backup and restore	66
show dhcp-relay	135	default	35
show event log	128	configuration settings, saving or restoring	66, 147
show filters	166	connector pinouts	221
show hardware	124	connectors	
show history	111	AP-80 MB/SB	14
show interface ethernet	183	MDI	16
show interface wireless	201	RSSI	15
show line	112	country code	
show link-integrity	212	configuring	113
show logging	129	setting	38
show radius	155	country command codes	113
show rogue-ap	209	CTS	82, 200
show snmp	143	D	
show snmp filter	143	data rate	
show snmp filter-assignments	144	configuring maximum	81
show snmp group-assignments	145	data rates	
show snmp groups	144	and distance covered	27, 28
show snmp target	145	overview	27
show snmp users	145	default	
show snmp	133	gateway	50
show station	202	password	38
shutdown	182, 201	resetting to factory	67
snmp-server community	136	user name	38
snmp-server contact	115	default configuration	
snmp-server enable server	136	parameters	35
snmp-server engine-id	137	default settings	35
snmp-server filter	137	description	84
snmp-server filter-assignments	138	device status, displaying	95, 124
snmp-server host	139	DHCP	41, 49, 181
snmp-server location	116	distance covered	27, 28
snmp-server targets	140	diversity, antenna	82
snmp-server trap	140	DNS	179
snmp-server user	142	DNS, primary and secondary servers	50
sntp-server date-time	130	Domain Name Server <i>See</i> DNS	
sntp-server daylight-saving	130	downloading software	65, 147
sntp-server enable	131	DTIM	81, 191
sntp-server ip	132	duplex settings	50
sntp-server timezone	132		
speed	200		
speed-duplex	182		
ssid	202		
super-g or super-a	203		
system management	112		
system name	115		
transmit-key	203		
transmit-power	204		
turbo	204		
untagged-vlanid	214		
username	121		
vap	205		
wmm	216		
wmm-acknowledge-policy	216		

E

EAP	91, 94, 188
EAP-TLS	91
EAP-TTLS	91
encryption	84, 87, 91, 192
engine ID	60
Ethernet	221
cable requirements	18
cabling and grounding	32
connecting cables	21
pin assignments	222
Ethernet port	14
ethernet-type enable	165
event logs	100, 129
Extensible Authentication Protocol	<i>See</i> EAP. EAP
description	

F

factory defaults, restoring	66, 111
FAT access point	33, 34
features	
AP-80MB	11
AP-80SB	11
filter	57, 160
address	160
CLI	58
management access	164
parameters	57
VLANs	213
firmware	
displaying version	66, 125
upgrading	65, 66, 147
fragment length	82
fragmentation	193

G

gateway address	103, 180
gateway, default	50
GMT	68
grounding screw	15

H

hardware version, displaying	125
height and clearance	30
hexadecimal WEP key	88

I

IAPP	213
IEEE 802.11a	76, 194
configuring interface	77, 194
maximum data rate	81, 200
radio channel	80, 189
IEEE 802.11b	76
IEEE 802.11f	213
IEEE 802.11g	76
configuring interface	77
maximum data rate	200
radio channel	189
IEEE 802.1x	155, 160
and EAP	91
configuring	54, 155
installation	
overview	17
personnel requirement	27
preparing for	18
requirements	18
tasks	17
interface	
management	35
interference	31
IP address	
configuring	41, 48, 180
static	35

L

lightning arrester hardware	12
line of sight	28
link	
cost	74
distances	76
port priority	74
local CLI	55
log	
CLI	69
CLI, event	101
event	100
messages	127
server	67, 127
system	67
logging in	45
RADIUS client authentication	149
web	39

M

MAC address	
authentication commands	160

authentication, timing	55	pinouts	221
security	84	planning	
MAC address, authentication	160, 161	Ethernet cabling and grounding	32
MAC authentication	55	radio path	28
CLI	56	weather factors	32
description	55	PoE	22
local	55	injector/adaptor	15
master mode	71	point-to-multipoint bridge	33
maximum data rate	81, 200	point-to-multipoint configuration	23
802.11a interface	81, 200	point-to-point bridge	32
802.11g interface	200	point-to-point configuration	23
MD5	55	polarization of antennas	31
MDI connector	16	ports	
MDI, RJ-45 pin configuration	16	AP-80 MB/SB	14
Message Integrity Check (MIC)	81	Ethernet	14
mode		power injector, connecting	22
access point	70	Power over Ethernet <i>See</i> PoE	
bridge	71	powering on	16
master/slave	71	preauthentication	92
radio	76	preparing for installation	18
root bridge	71	PSK	91
turbo	80		
mounting		Q	
outdoor kit	12	Quality of Service (QoS)	82
pole	18, 19		
wall	20	R	
multicast cipher	190	radio	
N		802.11a	76
network topologies	32	802.11g	76
O		beacon interval	81
open system	42, 84	interference planning	31
outdoor mounting kit	12	modes	76
overview		radio channel	
AP-80MB hardware	14	802.11a interface	80, 189
AP-80SB hardware	13	802.11g interface	189
installation	17	configuring	40
P		radio path planning	
package checklist	13	guidelines	29
parent	71	line of sight	28
password		RADIUS	149
CLI	65	and EAP	91
configuring	65, 120	attributes	62
default	38	CLI	53
management	65, 120	overview	
PEAP	91	primary server	52
		secondary server	53
		VLAN IDs	62
		RADIUS, login authentication	149

Remote Authentication Dial-in User Service <i>See RADIUS</i>		trap manager	60, 139
Request to Send <i>See RTS</i>		trap recipients	60
reset	66, 111	user parameters	60
reset button	66	using	
resetting		v3 parameters	60
access point	66	SNTP	68, 132
hard reset	67	CLI	69
without CLI, WebUI access	67	enabling client	68, 131
resetting the access point	111	server	68, 132
restarting the system	66, 111	software	
restoring configuration	66	displaying version	65, 95, 125
rogue AP		downloading	66, 147
identifying	80	software, CLI for download	67
settings	80	Spanning Tree Protocol. <i>See</i> STP.	
root bridge mode	71	specifications	223
RSSI		speed settings	50
CLI	76	SSH	50
connector	15	SSID	39, 202
RTS		security	84
threshold	82	staging	17, 18
RTS threshold	82, 200	startup files, setting	146
S		static IP address	48
security	84	station information, CLI	99
combinations	85	station status	202
MAC address	84	CLI	98
options	84	displaying	98
SSID	84	status	
WEP settings	89	displaying device status	95, 124
WPA over 802.1x	84	displaying station	98
WPA PSK	85	displaying station status	202
session key	156	WPS-STP	99
session timeout	65	STP	
setup		bridge priority	73
initial	38	CLI	74
wizard	38	description	
shared key	42, 194	status	99
Simple Network Management Protocol <i>See</i> SNMP.		stp	
Simple Network Time Protocol <i>See</i> SNTP		commands	172
slave mode	71	super a	81
SNMP	58, 135	super g	81
CLI	61	super-a	203
community name	58, 136	super-g	203
community string	136	system clock CLI	70
enabling traps	60, 136	system clock, setting	68, 130
filters	60	system identification parameters	47
parameters	60	system log	67
trap destination	60, 139	enabling	67, 128
		server	67, 127

