User Guide

3Com Outdoor 11a Building to Building Bridge and 11bg Access Point

3CRWEASYA73 / WL-546

http://www.3com.com/
http://www.3com.com/support/en_US/productreg/frontpg

Published June, 2006
Version 2.0.2

3Com Corporation
350 Campus Drive
Marlborough, MA
01752-3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (November 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, and SuperStack are registered trademarks of 3Com Corporation.

Wi-Fi is a trademark of the Wireless Ethernet Compatibility Alliance.

All other company and product names may be trademarks of the respective companies with which they are associated.

EXPORT RESTRICTIONS: This product contains Encryption and may require US and/or Local Government authorization prior to export or import to another country.

Contents

1 INTRODUCTION

The 3Com Outdoor 11a Building to Building Bridge and 11bg Access Point system provides point-to-point or point-to-multipoint bridge links between remote Ethernet LANs, and wireless access point services for clients in the local LAN area.

It includes an integrated high-gain antenna for the 802.11a radio and can operate as a “Slave” or “Master” bridge in point-to-multipoint configurations, or provide a high-speed point-to-point wireless link between two sites that can be up to 15.4 km (9.6 miles) apart. As a “Master” bridge in point-to-multipoint configurations it can support connections to as many as 16 “Slave” units. The 802.11b/g radio requires an external antenna option.

Each model is housed in a weatherproof enclosure for mounting outdoors and includes its own brackets for attaching to a wall, pole, radio mast, or tower structure. The unit is powered through its Ethernet cable connection from a power injector module that is installed indoors.

The wireless bridge system offers a fast, reliable, and cost-effective solution for connectivity between remote Ethernet wired LANs or to provide Internet access to an isolated site. The system is also easy to install and operate, ideal for situations where a wired link may be difficult or expensive to deploy. The wireless bridge connection provides data rates of up to 108 Mbps.

In addition, both wireless bridge models offer full network management capabilities through an easy-to-use web interface, a command-line interface, and support for Simple Network Management Protocol (SNMP) tools.

RADIO CHARACTERISTICS

The IEEE 802.11a and 802.11g standards use a radio modulation technique known as Orthogonal Frequency Division Multiplexing (OFDM), and a shared collision domain (CSMA/CA). The 802.11a standard operates in the 5 GHz Unlicensed National Information Infrastructure (UNII) band, and the 802.11g standard in the 2.4 GHz band.

IEEE 802.11g includes backward compatibility with the IEEE 802.11b standard. IEEE 802.11b also operates at 2.4 GHz, but uses Direct Sequence Spread Spectrum (DSSS) and Complementary Code Keying (CCK) modulation technology to achieve a communication rate of up to 11 Mbps.

The wireless bridge provides a 54 Mbps half-duplex connection for each active channel (up to 108 Mbps in turbo mode on the 802.11a interface).

APPROVED CHANNELS

Use of this product is only authorized for the channels approved by each country. For proper installation, select your country from the country selection list.

To conform to FCC and other country restrictions your product may be limited in the channels that are available. If other channels are permitted in your country please visit the 3Comwebsite for the latest software version.

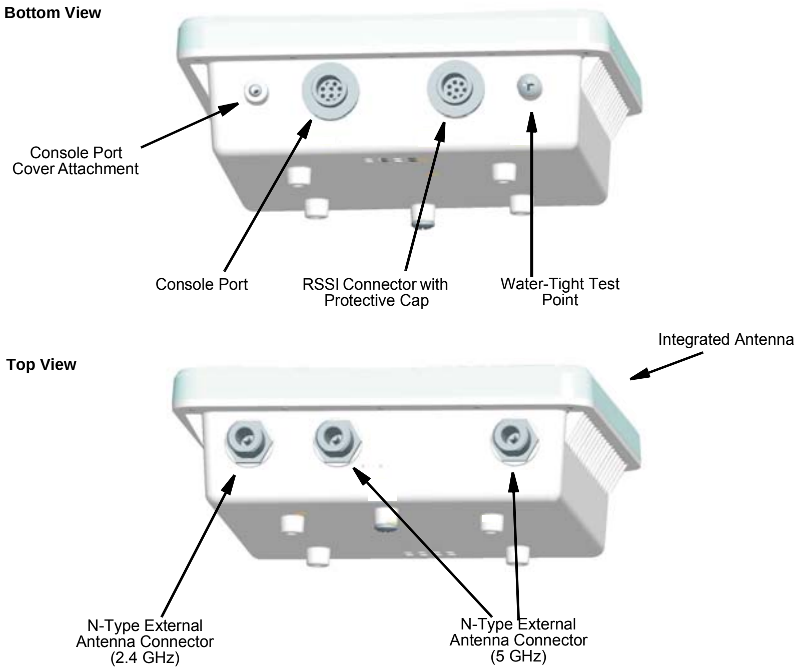
PACKAGE CHECKLIST

The 3Com Outdoor 11a Building to Building Bridge and 11bg Access Point package includes:

- One Dual-band Outdoor Access Point / Bridge
- One Category 5 network cable, length 164 ft (50 m)
- One power injector module and power cord
- Outdoor pole-mounting bracket kit
- This User Guide
- Optional: One N-type RF coaxial cable
- Optional: Outdoor wall-mounting bracket kit

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

HARDWARE DESCRIPTION


Bottom View
Console Port Cover Attachment
Console Port
RSSI Connector with Protective Cap
Water-Tight Test Point
Integrated Antenna
Top View
N-Type External Antenna Connector (2.4 GHz)
N-Type External Antenna Connector (5 GHz)

INTEGRATED HIGH-GAIN ANTENNA

The OAP6626A wireless bridge includes an integrated high-gain (17 dBi) flat-panel antenna for 5 GHz operation. The antenna can provide a direct line-of-sight link up to 15.4 km (9.6 miles) with a 6 Mbps data rate.

EXTERNAL ANTENNA OPTIONS

The OAP6626A Master bridge unit does not include an integrated antenna, but provides various external antenna options for both 5 GHz and 2.4 GHz operation. In a point-to-multipoint configuration, an external high-gain omnidirectional, sector, or high-gain panel antenna can be attached to communicate with bridges spread over a wide area. The OAP6626A and OAP6626A units both require the 2.4 GHz 8 dBi omnidirectional external antenna for 2.4 GHz operation. The following table summarizes the external antenna options:

Antenna Type	Gain (dBi)	HPBW* Horizontal	HPBW* Vertical	Polarization	Max Range/Speed
5 GHz Omnidirectional	8	360	12	Linear, vertical	3.3 km at 6 Mbps
5 GHz 120-Degree Sector	14	120	6	Linear, vertical	10.3 km at 6 Mbps
5 GHz 60-Degree Sector	17	60	6	Linear, vertical	14 km at 6 Mbps
5 GHz High-Gain Panel	23	9	9	Linear	24.4 km at 6 Mbps
2.4 GHz Omnidirectional	8	360	15	Linear, vertical	7.6 km at 6 Mbps

* Half-power beam width in degrees

External antennas connect to the N-type RF connectors on the wireless bridge using the provided coaxial cables.

ETHERNET PORT

The wireless bridge has one 10BASE-T/100BASE-TX 8-pin DIN port that connects to the power injector module using the included Ethernet cable. The Ethernet port connection provides power to the wireless bridge as well as a data link to the local network.

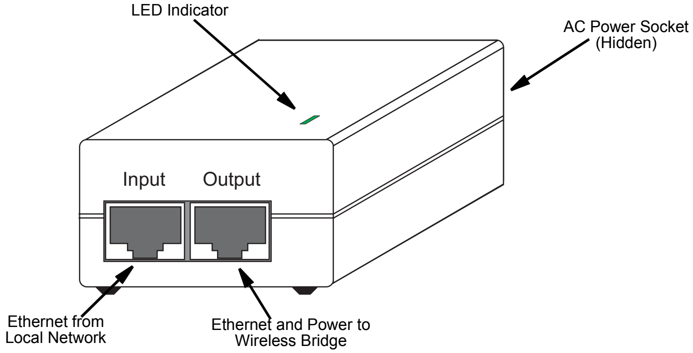
The wireless bridge appears as an Ethernet node and performs a bridging function by moving packets from the wired LAN to the remote end of the wireless bridge link.

NOTE*: The power injector module does not support Power over Ethernet (PoE) based on the IEEE 802.3af standard. The wireless bridge unit must always be powered on by being connected to the power injector module.*

POWER INJECTOR MODULE

The wireless bridge receives power through its network cable connection using power-over-Ethernet technology. A power injector module is included in the wireless bridge package and provides two RJ-45 Ethernet ports, one for connecting to the wireless bridge (Output), and the other for connecting to a local LAN switch (Input).

The Input port uses an MDI (i.e., internal straight-through) pin configuration. You can therefore use straight-through twisted-pair cable to connect this port to most network interconnection devices such as a switch or router that provide MDI-X ports. However, when connecting the access point to a workstation or other device that does not have MDI-X ports, you must use crossover twisted-pair cable.


LED Indicator
AC Power Socket (Hidden)
Input
Output
Ethernet from Local Network
Ethernet and Power to Wireless Bridge

The wireless bridge does not have a power switch. It is powered on when its Ethernet port is connected to the power injector module, 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.

⚠ ***WARNING**: The power injector module is designed for indoor use only. Never mount the power injector outside with the wireless bridge unit.*

Receive Signal Strength Indicator (RSSI) BNC Connector

The RSSI connector provides an output voltage that is proportional to the received radio signal strength. A DC voltmeter can be connected the this port to assist in aligning the antennas at both ends of a wireless bridge link.

Grounding Point

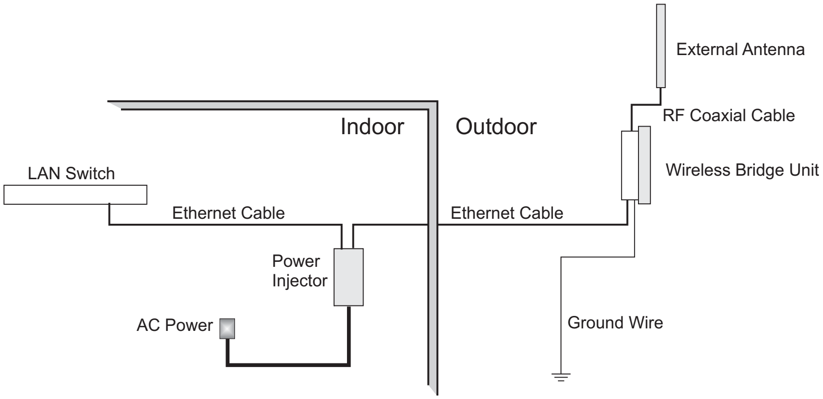
Even though the wireless bridge includes its own built-in lightning protection, it is important that the unit is properly connected to ground. A grounding screw is provided for attaching a ground wire to the unit.

Wall- and Pole-Mounting Bracket Kits

The wireless bridge includes bracket kits that can be used to mount the bridge to a wall, pole, radio mast, or part of a tower structure.

SYSTEM CONFIGURATION

At each location where a unit is installed, it must be connected to the local network using the power injector module. The following figure illustrates the system component connections.



FEATURES AND BENEFITS

- OAP6626A Slave units support a 5 GHz point-to-point wireless link up 15.4 km (at 6 Mbps data rate) using integrated high-gain 17 dBi antennas
- OAP6626A Master units support 5 GHz point-to-multipoint links using various external antenna options
- Both OAP6626A and OAP6626A units also support access point services for the 5 GHz and 2.4 GHz radios using various external antenna options
- Maximum data rate up to 108 Mbps on the 802.11a (5 GHz) radio
- Outdoor weatherproof design
- IEEE 802.11a and 802.11b/g compliant
- Local network connection via 10/100 Mbps Ethernet port
- Powered through its Ethernet cable connection to the power injector module
- Includes wall- and pole-mount brackets
- Security through 64/128/152-bit Wired Equivalent Protection (WEP) or 128-bit Advanced Encryption Standard (AES) encryption
- Scans all available channels and selects the best channel and data rate based on the signal-to-noise ratio
- Manageable through an easy-to-use web-browser interface, command line (via Telnet), or SNMP network management tools

SYSTEM DEFAULTS

The following table lists some of the wireless bridge’s basic system defaults. To reset the bridge defaults, use the CLI command “reset configuration” from the Exec level prompt.

Feature	Parameter	Default
Identification	System Name	Dual Band Outdoor AP
Administration	User Name	admin
	Password	null
General	HTTP Server	Enabled
	HTTP Server Port	80
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

Feature	Parameter	Default
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	A (802.11a)
Wireless Interface 802.11a	Status	Enabled
	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

Feature	Parameter	Default
Wireless Interface 802.11b/g	Status	Enabled
	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

2 INSTALLING THE BRIDGE

The 3Com Outdoor 11a Building to Building Bridge and 11bg Access Point system provides access point or bridging services through either the 5 GHz or 2.4 GHz radio interfaces.

The wireless bridge units can be used just 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 connecting remote LANs. Alternatively, you can employ both access point and bridging functions together, offering a flexible and convenient wireless solution for many applications.

This chapter describes the role of wireless bridge in various wireless network configurations.

ACCESS POINT TOPOLOGIES

Wireless networks support a stand-alone wireless configuration as well as an integrated configuration with 10/100 Mbps Ethernet LANs.

Wireless network cards, adapters, and access points can be configured as:

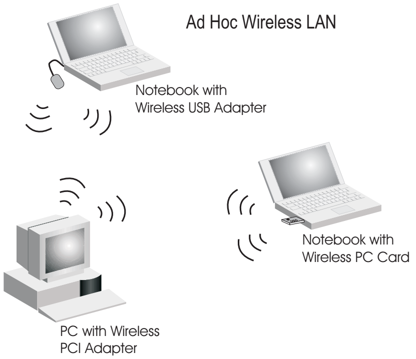
- Ad hoc for departmental, SOHO, or enterprise LANs
- Infrastructure for wireless LANs
- Infrastructure wireless LAN for roaming wireless PCs

The 802.11b and 802.11g frequency band, which operates at 2.4 GHz, can easily encounter interference from other 2.4 GHz devices, such as other 802.11b or g wireless devices, cordless phones and microwave ovens. If you experience poor wireless LAN performance, try the following measures:

- Limit any possible sources of radio interference within the service area
- Increase the distance between neighboring access points
- Increase the channel separation of neighboring access points (e.g., up to 3 channels of separation for 802.11b or up to 5 channels for 802.11g)

AD HOC WIRELESS LAN (NO ACCESS POINT OR BRIDGE)

An ad hoc wireless LAN consists of a group of computers, each equipped with a wireless adapter, connected through radio signals as an independent wireless LAN. Computers in a specific ad hoc wireless LAN must therefore be configured to the same radio channel.

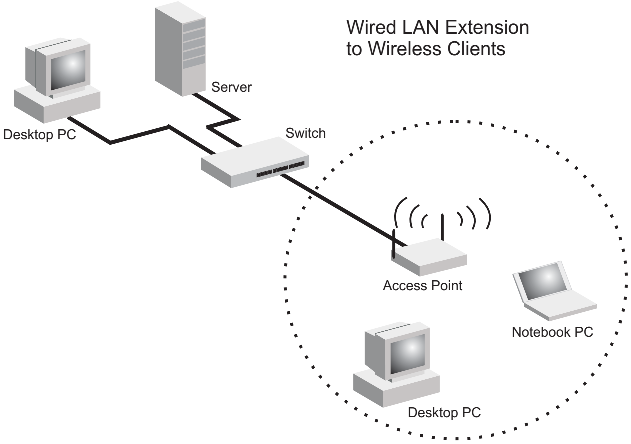


INFRASTRUCTURE WIRELESS LAN

The access point function of the wireless bridge provides access to a wired LAN for 802.11a/b/g wireless workstations. An integrated wired/wireless LAN is called an Infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users and an access point that is directly connected to the wired LAN. Each wireless PC in a BSS can connect to any computer in its wireless group or access other computers or network resources in the wired LAN infrastructure through the access point.

The infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also increases the effective wireless transmission range for wireless PCs by passing their signals through one or more access points.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure.

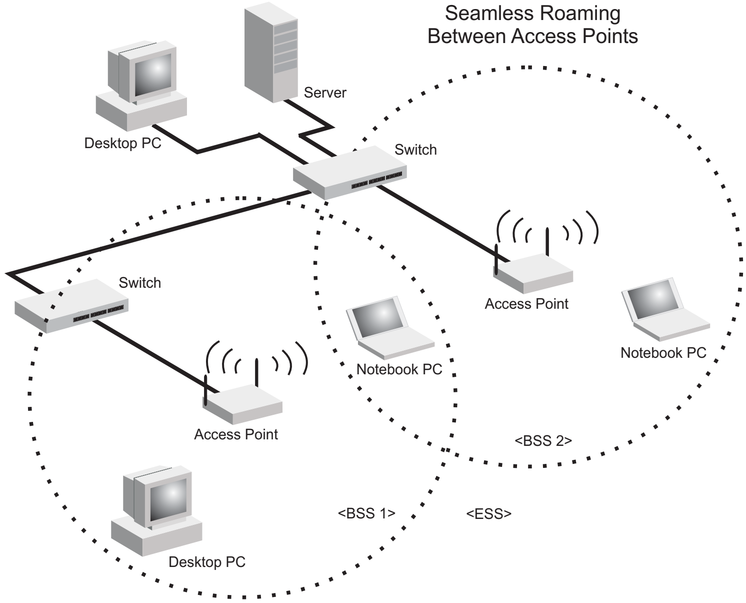


INFRASTRUCTURE WIRELESS LAN FOR ROAMING WIRELESS PCS

The Basic Service Set (BSS) defines the communications domain for each access point and its associated wireless clients. The BSS ID is a 48-bit binary number based on the access point's wireless MAC address, and is set automatically and transparently as clients associate with the access point. The BSS ID is used in frames sent between the access point and its clients to identify traffic in the service area.

The BSS ID is only set by the access point, never by its clients. The clients only need to set the Service Set Identifier (SSID) that identifies the service set provided by one or more access points. The SSID can be manually configured by the clients, can be detected in an access point's beacon, or can be obtained by querying for the identity of the nearest access point. For clients that do not need to roam, set the SSID for the wireless card to that used by the access point to which you want to connect.

A wireless infrastructure can also support roaming for mobile workers. More than one access point can be configured to create an Extended Service Set (ESS). By placing the access points so that a continuous coverage area is created, wireless users within this ESS can roam freely. All wireless network card adapters and wireless access points within a specific ESS must be configured with the same SSID.



BRIDGE LINK TOPOLOGIES

The IEEE 802.11 standard defines a WIreless Distribution System (WDS) for bridge connections between BSS areas (access points). The outdoor wireless bridge uses WDS to forward traffic on links between units. Up to 16 WDS links can be specified for a OAP6626A unit, which acts as the "Master" in the wireless bridge network. OAP6626A units support only one WDS link, which must be to the network's master unit.

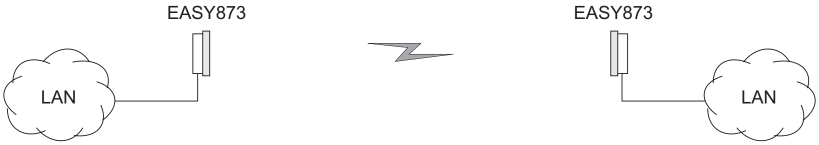
The unit supports WDS bridge links on either the 5 GHz (802.11a) or 2.4 GHz (802.11b/g) bands and can be used with various external antennas to offer flexible deployment options.

***NOTE**: The external antennas offer longer range options using the 5 GHz radio, which makes this interface more suitable for bridge links. The 2.4 GHz radio has only the 8 dBi omnidirectional antenna option, which is better suited for local access point services.*

When using WDS on a radio band, only wireless bridge units can associate to each other. Wireless clients can only associate with the wireless bridge using a radio band set to access point mode.

POINT-TO-POINT CONFIGURATION

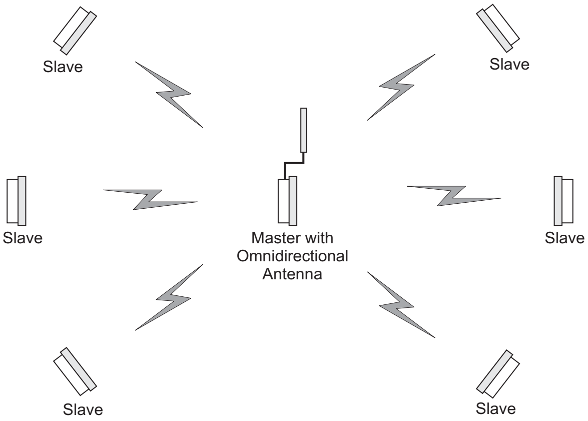
Two OAP6626A bridges can form a wireless point-to-point link using their 5 GHz (802.11a) integrated antennas. A point-to-point configuration can provide a limited data rate (6 Mbps) link over a long range (up to 15.4 km), or a high data rate (108 Mbps) over a short range (1.3 km).

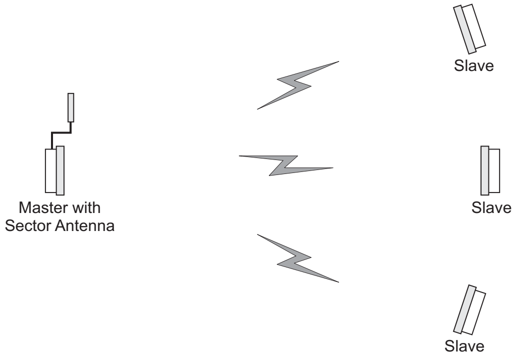


POINT-TO-MULTIPOINT CONFIGURATION

A OAP6626A wireless bridge set to “Master” mode can use an omnidirectional or sector antenna to connect to as many as 16 bridges in a point-to-multipoint configuration. There can only be one “Master” unit in the wireless bridge network, all other bridges must be “Slave” units.

Using the 5 GHz 8 dBi omnidirectional external antenna, the Master unit can connect to Slave units up to 3.3 km (2 miles) away. Using the 13.5 dBi 120-degree sector antenna, the Master can connect to Slave units up to 10.3 km (6.4 miles) away.


Slave
Slave
Slave
Master with
Omnidirectional
Antenna
Slave
Slave
Slave


Slave
Master with
Sector Antenna
Slave
Slave

3 BRIDGE LINK PLANNING

The 3Com Outdoor 11a Building to Building Bridge and 11bg Access Point 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 larger core network. Multiple bridge links can provide a way to connect widespread Ethernet LANs.

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.

***NOTE**: The planning and installation of the wireless bridge requires professional personnel that 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

Using its 5 GHz integrated antenna, the OAP6626A bridge set to “Slave” mode can operate 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). However, 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 you are planning each wireless bridge link, take into account the maximum distance and data rates for the various antenna options. A summary for 5 GHz (802.11a) antennas is provided in the following table. For full specifications for each antenna, see “Antenna Specifications” on page B-3.

Distances Achieved Using 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
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.

Distances Achieved Using Turbo Mode

Data Rate	17 dBi Integrated	8 dBi Omni	13.5 dBi 120-Degre e 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

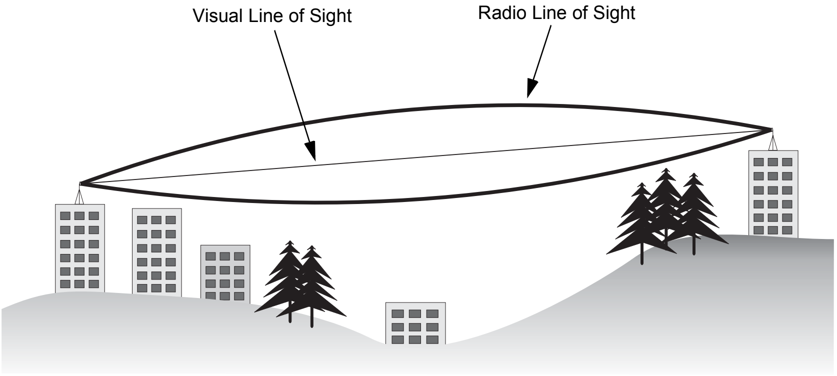
Distances provided in this table are an estimate for a typical deployment and may be reduced by local regulatory limits. For accurate distances, you need to calculate the power link budget for your specific environment.

Radio Path Planning

Although the wireless bridge uses IEEE 802.11a radio technology, which is capable of reducing the effect of multipath signals due to obstructions, 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 radio link path 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 not to be affected by obstacles along its path, no object, including the ground, must intrude within 60% of the first Fresnel Zone.

The following figure illustrates the concept of a good 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.

NOTE*: 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

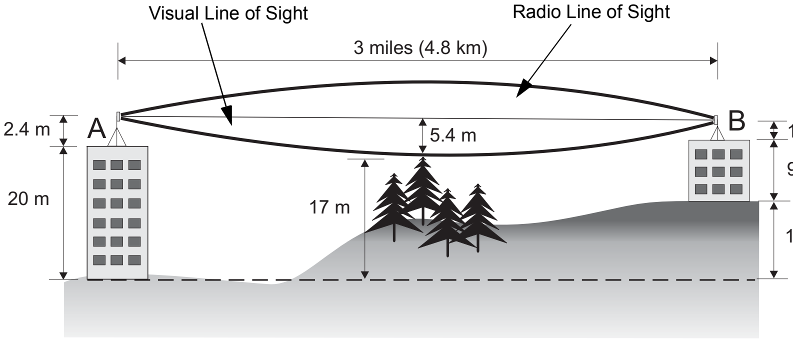
A reliable wireless link is usually best achieved by mounting the antennas at each end high enough for a clear radio line of sight between them. The minimum height required depends on the distance of the link, obstacles that may be in the path, topology of the terrain, and the curvature of the earth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

For long-distance links, a mast or pole may need to be contsructed to attain the minimum required height. Use the following table to estimate the required minimum clearance above the ground or path obstruction (for 5 GHz bridge links).

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)

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
15 miles (24.1 km)	35 ft (10.7 m)	45 ft (13.7 m)	80 ft (24.4 m)
17 miles (27.4 km)	37 ft (11.3 m)	58 ft (17.7 m)	95 ft (29 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 the figure below.



A wireless bridge link is deployed to connect building A to a building B, which is located three miles (4.8 km) away. Mid-way between the two buidings 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 contructed 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 bulding A. To mount an anntena at the required height on building B, a mast or pole of only 1.3 m (4.3 ft) is needed.

⚠ ***WARNING**: Never construct a radio mast, pole, or tower near overhead power lines.*

***NOTE**: 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
- 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
- The wireless bridge antennas at both ends of the link must be positioned with the same polarization direction, either horizontal or vertical

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. Ideally the antennas should be pointing upwards mounted on the top part of a pole.

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 MPH and survive higher wind speeds up to 125 MPH. 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 build up 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

When a suitable antenna location has been determined, you must plan a cable route form the wireless bridge outdoors to the power injector module indoors. Consider these points:

- The Ethernet cable length should never be longer than 100 m (328 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.

4 Hardware Installation

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 2, "Wireless Link Planning."

Also, before mounting units in their intended locations, you should first perform initial configuration and test the basic operation of the wireless bridge links in a controlled environment over a very short range. (See the section "Testing Basic Link Operation" in this chapter.)

The wireless bridge includes its own bracket kit for mounting the unit to a 1.5 to 2 inch diameter steel pole or tube. The pole-mounting bracket allows the unit to be mounted to part of a radio mast or tower structure. The unit also has a wall-mounting bracket kit that enables it to be fixed to a building wall or roof when using external antennas.

Hardware installation of the wireless bridge involves these steps:

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.

TESTING BASIC LINK OPERATION

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, "Initial Configuration." When you are satisfied that the links are operating correctly, proceed to mount the units in their intended locations.

MOUNT THE UNIT

The bridge can be mounted on the following types of surfaces:

- Pole
- Wall, or electrical box (NEMA enclosure)

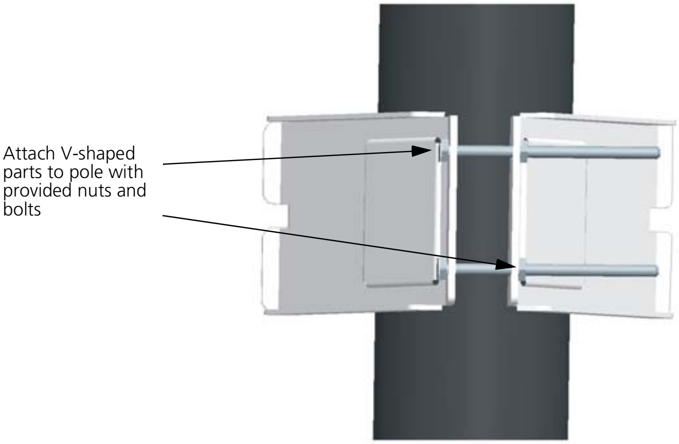
⚠ ***CAUTION**: The bridge is intended for outdoor use only. Do not install the bridge indoors.*

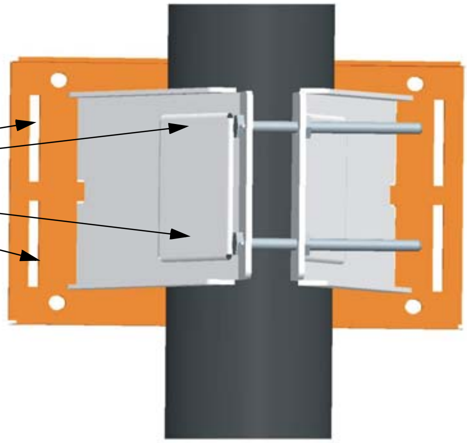
Using the Pole-Mounting Bracket

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

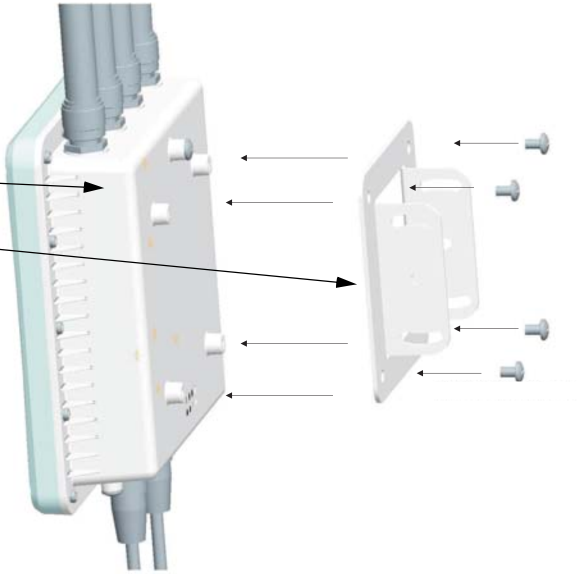
1 Always attach the bracket to a pole with the open end of the mounting grooves facing up.

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

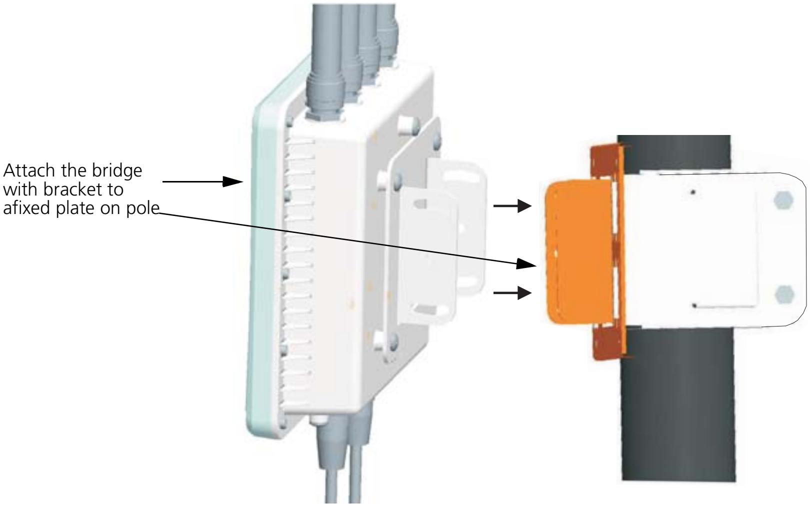




Slot the edges of the V-shaped part into the slats in the rectangular plate, and tighten the nuts



Attach the adjustable rectangular plate to the bridge with supplied screws



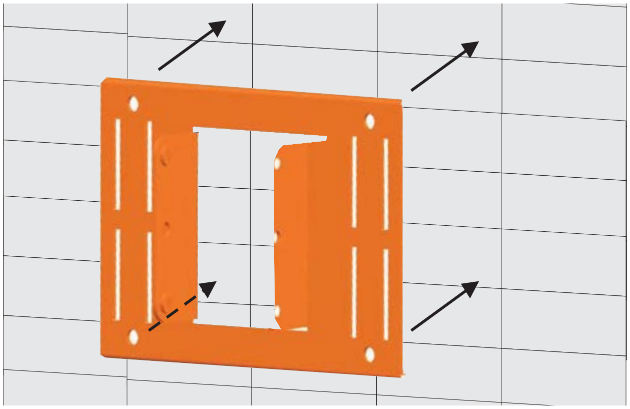
Use the included nuts to tightly secure the wireless bridge to the bracket. Be sure to take account of the antenna polarization direction; all antennas in a link must be mounted with the same polarization.

USING THE WALL-MOUNTING BRACKET

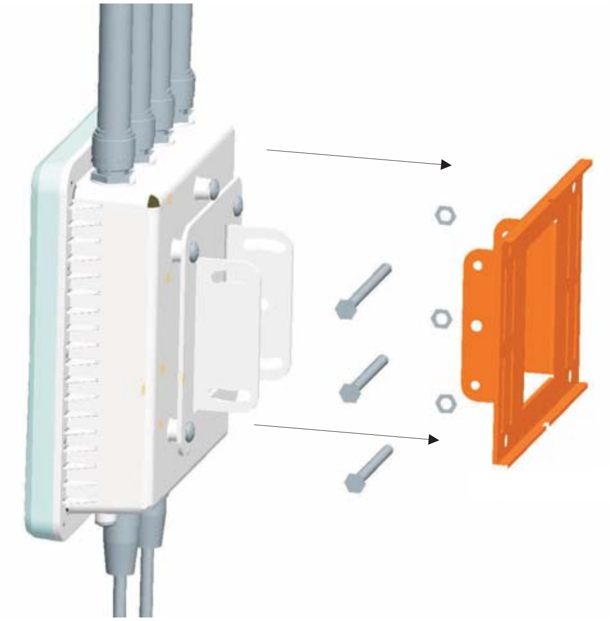
Perform the following steps to mount the unit to a wall using the wall-mounting bracket:

⚠ ***CAUTION**: The wall-mounting bracket does not allow the wireless bridge's intrgrated antenna to be aligned. It is intended for use with the unit using an external antenna.*

1. Always attach the bracket to a wall with flat side flush against the wall (see following figure).



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.



5 Connect the Ethernet cable (and power cable, if applicable) to the port(s) on the front of the *FEM656B - 3Com 10-100 LAN + 56K Modem CardBus PC Card-(Fast Ethernet)*.

Connecting the Bridge to a Switch

It is recommended that you install and configure the 3Com Wireless LAN switch before installing the *FEM656B - 3Com 10-100 LAN + 56K Modem CardBus PC Card-(Fast Ethernet)*. If the switch is already installed and configured for the *FEM656B - 3Com 10-100 LAN + 56K Modem CardBus PC Card-(Fast Ethernet)*, you can immediately verify the cable connection when you plug the cable into the *FEM656B - 3Com 10-100 LAN + 56K Modem CardBus PC Card-(Fast Ethernet)*.

***WARNING**: Do not connect or disconnect cables or otherwise work with the bridge during periods of lightning activity.*

You can connect the bridge directly to a Wireless LAN Switch port or indirectly to Wireless LAN switches through an intermediate Layer 2 or Layer 3 network. In either case, use Category 5 cable with straight-through signaling for each *FEM656B - 3Com 10-100 LAN + 56K Modem CardBus PC Card-(Fast Ethernet)* connection.

Connect External Antennas

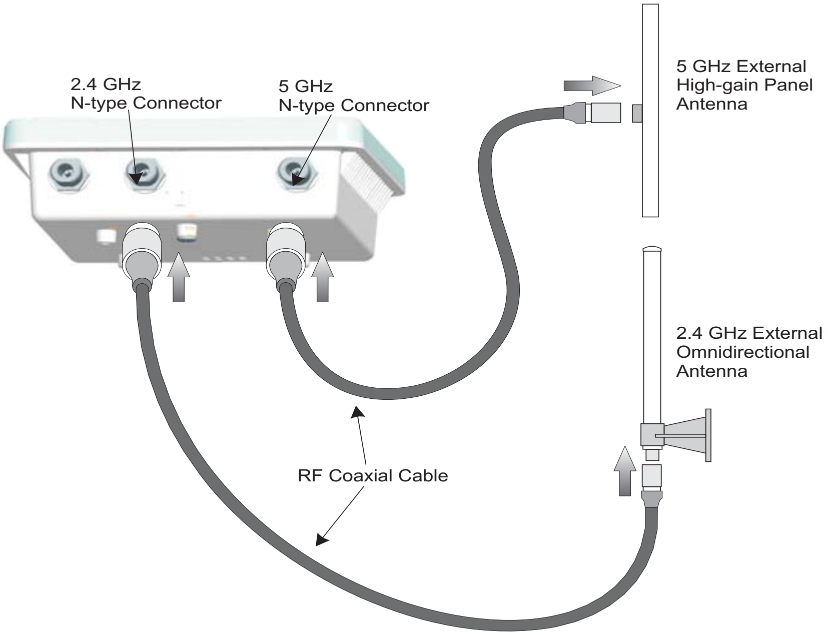
When deploying a OAP6626A Master bridge unit for a bridge link or access point operation, you need to mount external antennas and connect them to the bridge. Typically, a bridge link requires a 5 GHz antenna, and access point operation a 2.4 GHz antenna. OAP6626A Slave units also require an external antenna for 2.4 GHz operation.

Perform these steps:

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.



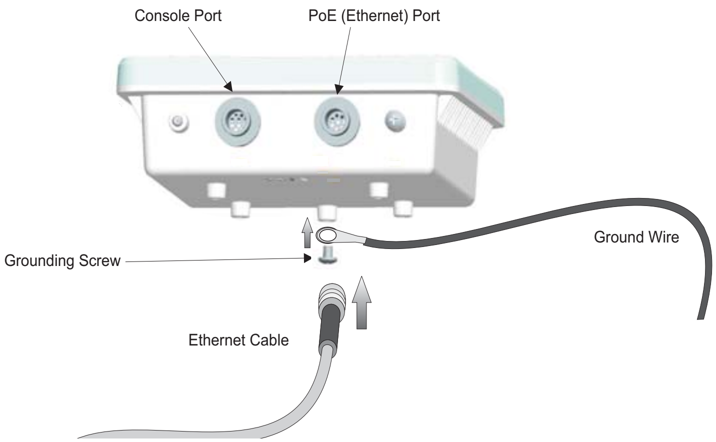
CONNECT CABLES TO THE UNIT

1 Attach the Ethernet cable to the Ethernet port on the wireless bridge.

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.

⚠ ***CAUTION****: 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.*



CONNECT THE POWER INJECTOR

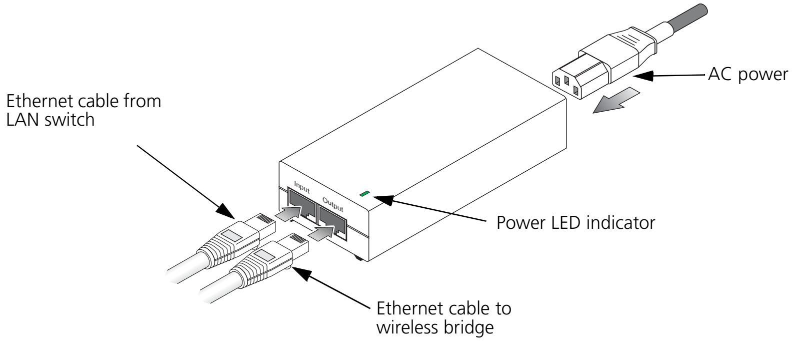
To connect the wireless bridge to a power source:

⚠ ***CAUTION**: Do not install the power injector outdoors. The unit is for indoor installation only.*

***NOTE**: 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 PoE. 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 "Output" 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 "Input" on the power injector. Use Category 5e or better UTP cable for 10/100BASE-TX connections.

***NOTE**: 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.*


Ethernet cable from LAN switch
AC power
Input
Output
Power LED indicator
Ethernet cable to wireless bridge

1 Insert the power cable plug directly into the standard AC receptacle on the power injector.

2 Plug the other end of the power cable into a grounded, 3-pin socket, AC power source.

***NOTE**: 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.*

3 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.

Connect External Antennas

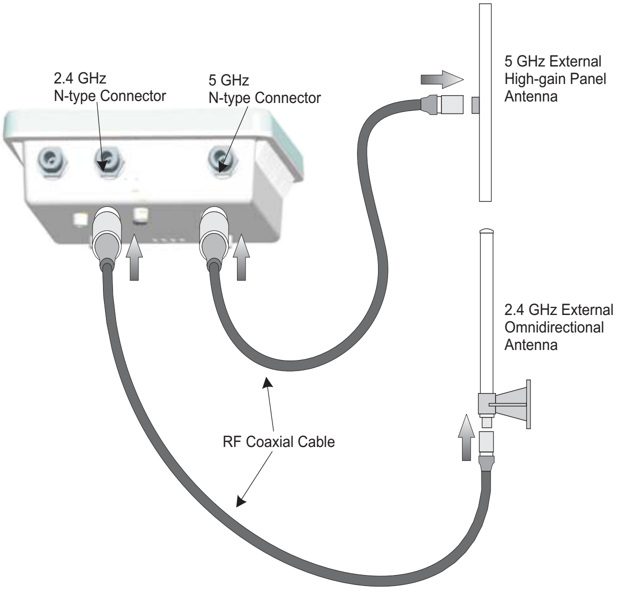
When deploying a OAP6626A set to “Master” mode for a bridge link or access point operation, you need to mount external antennas and connect them to the bridge. Typically, a bridge link requires a 5 GHz antenna, and access point operation a 2.4 GHz antenna. Units set to “Slave” mode also require an external antenna for 2.4 GHz operation.

Perform these steps:

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.



CONNECT CABLES TO THE UNIT

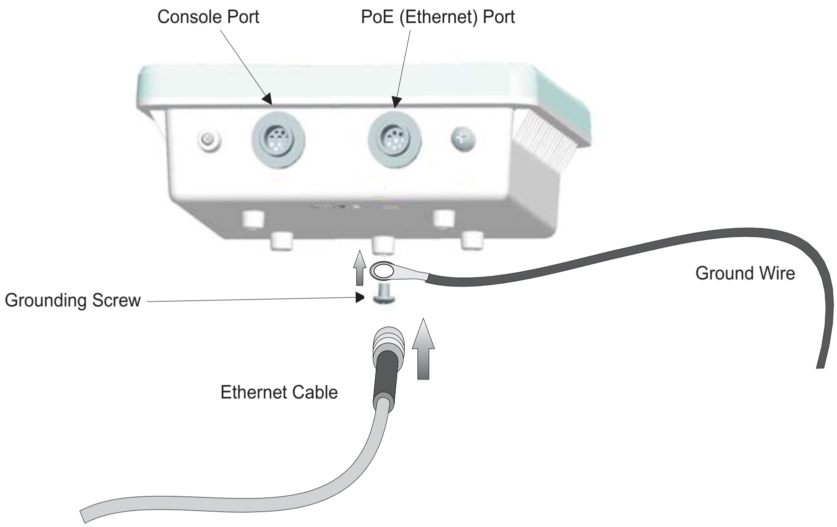
1 Attach the Ethernet cable to the Ethernet port on the wireless bridge.

NOTE: The Ethernet cable included with the package is 30 m (100 ft) long. To wire a longer cable (maximum 100 m, 325 ft), use the connector pinout information in Appendix B.

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.

CAUTION*: 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.*



CONNECT THE POWER INJECTOR

To connect the wireless bridge to a power source:

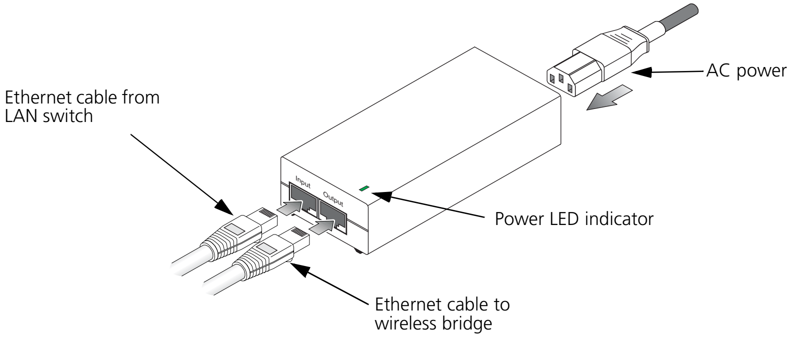
⚠ ***CAUTION**: Do not install the power injector outdoors. The unit is for indoor installation only.*

***NOTE**: 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 PoE. 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 "Output" 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 "Input" on the power injector. Use Category 5 or better UTP cable for 10/100BASE-TX connections.

***NOTE**: 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.*


Ethernet cable from LAN switch
AC power
Input
Output
Power LED indicator
Ethernet cable to wireless bridge

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.

***NOTE**: 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.

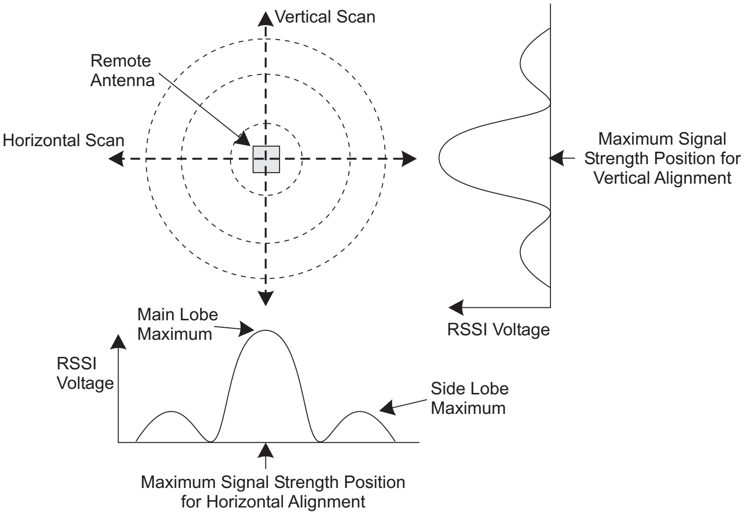
Align Antennas

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 antennna.

- **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.

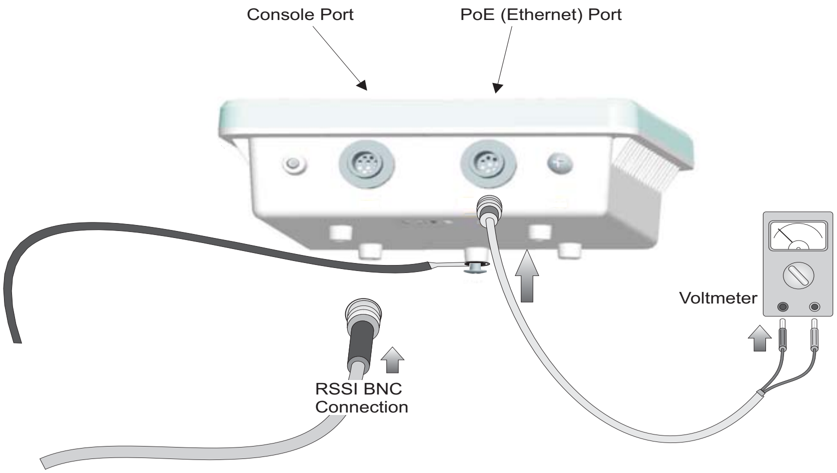

Vertical Scan
Remote Antenna
Horizontal Scan
Maximum Signal Strength Position for Vertical Alignment
RSSI Voltage
Main Lobe Maximum
RSSI Voltage
Side Lobe Maximum
Maximum Signal Strength Position for Horizontal Alignment

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:

Note:

NOTE*: The RSSI output can be configured through management interfaces to output a value for specific WDS ports. See page 6-40 for more information.*

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



2 Pan the antenna horizontally back and forth while checking the RSSI voltage. If 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.

NOTE*: 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.

Chapter 5: Initial Configuration

The 2.4 GHz/5 GHz Wireless Bridge offers a variety of management options, including a web-based interface, a direct connection to the console port, Telnet, Secure Shell (SSH), or using SNMP software.

The initial configuration steps can be made through the web browser interface or CLI. The bridge requests an IP address via DHCP by default. If no response is received from the DHCP server, then the bridge uses the default address 192.168.2.2. If this address is not compatible with your network, you can first use the command line interface (CLI) as described below to configure a valid address.

Note: Units sold in countries outside the United States are not configured with a specific country code. You must use the CLI to set the country code and enable wireless operation (page 5-3).

Initial Setup through the CLI

Required Connections

The bridge provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuration. Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the bridge. You can use the console cable provided with this package, or use a cable that complies with the wiring assignments shown on page B-3.

To connect to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the bridge.
3. Make sure the terminal emulation software is set as follows:
    - Select the appropriate serial port (COM port 1 or 2).
    - Set the data rate to 9600 baud.
    - Set the data format to 8 data bits, 1 stop bit, and no parity.
    - Set flow control to none.
    - Set the emulation mode to VT100.
    - When using HyperTerminal, select Terminal keys, not Windows keys.

Note: When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

4. Once you have set up the terminal correctly, press the [Enter] key to initiate the console connection. The console login screen will be displayed.

For a description of how to use the CLI, see "Using the Command Line Interface" on page 7-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 7-6.

Initial Configuration Steps

Logging In – Enter "admin" for the user name and leave the password blank. The CLI prompt appears displaying the bridge's name.

```
Username: admin
Password:
Enterprise AP#
```

Setting the IP Address – By default, the bridge is configured to obtain IP address settings from a DHCP server. If a DHCP server is not available, the IP address defaults to 192.168.2.2, which may not be compatible with your network. You will therefore have to use the command line interface (CLI) to assign an IP address that is compatible with your network.

Type "configure" to enter configuration mode, then type "interface ethernet" to access the Ethernet interface-configuration mode.

```
Enterprise AP#configure
Enterprise AP(config)#interface ethernet
Enterprise AP(config-if)#
```

First type "no ip dhcp" to disable DHCP client mode. Then type "ip address *ip-address netmask gateway*," where "ip-address" is the bridge's IP address, "netmask" is the network mask for the network, and "gateway" is the default gateway router. Check with your system administrator to obtain an IP address that is compatible with your network.

```
Enterprise AP(if-ethernet)#no ip dhcp
Enterprise AP(if-ethernet)#ip address 192.168.2.2
   255.255.255.0 192.168.2.254
Enterprise AP(if-ethernet)#
```

After configuring the bridge’s IP parameters, you can access the management interface from anywhere within the attached network. The command line interface can also be accessed using Telnet from any computer attached to the network.

Setting the Country Code – Units sold in the United States are configured by default to use only radio channels 1-11 in 802.11b or 802.11g mode as defined by FCC regulations. Units sold in other countries are configured by default without a country code (i.e., 99). You must use the CLI to set the country code. Setting the country code restricts operation of the bridge to the radio channels and transmit power levels permitted for wireless networks in the specified country.

Type “exit” to leave configuration mode. Then type “country ?” to display the list of countries. Select the code for your country, and enter the country command again, following by your country code (e.g., tw for Taiwan).

```
Enterprise AP#country tw
Enterprise AP#
```

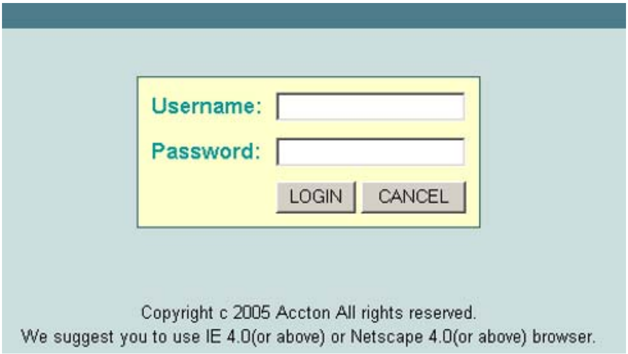
Note: Command examples shown later in this manual abbreviate the console prompt to “AP” for simplicity.

Logging In

There are only a few basic steps you need to complete to connect the bridge to your corporate network, and provide network access to wireless clients.

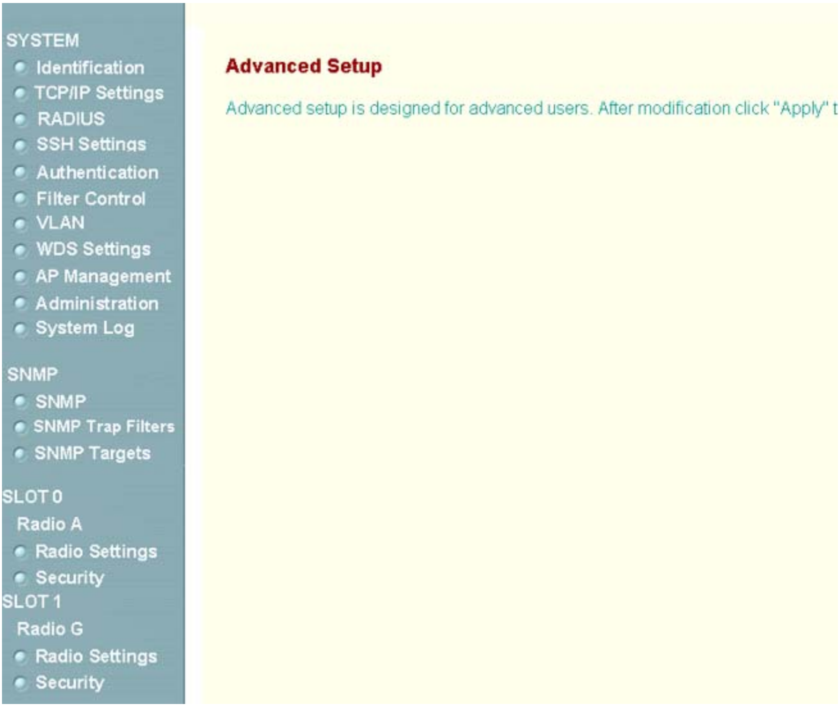
The bridge can be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above). Enter the default IP address: http://192.168.2.2

Logging In – Enter the username “admin,” and password “smcadmin” then click LOGIN. For information on configuring a user name and password, see page 6-23.



Copyright c 2005 Accton All rights reserved.
We suggest you to use IE 4.0(or above) or Netscape 4.0(or above) browser.

The home page displays the Main Menu.



Advanced Setup

Advanced setup is designed for advanced users. After modification click "Apply" t

Chapter 6: System Configuration

Before continuing with advanced configuration, first complete the initial configuration steps described in Chapter 4 to set up an IP address for the wireless bridge.

The wireless bridge 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 default IP address: http://192.168.1.1

To log into the wireless bridge, enter the default user name “admin” and click LOGIN (there is no default password). When the home page displays, click on Advanced Setup. The following page will display.

The information in this chapter is organized to reflect the structure of the web screens for easy reference. However, it is recommended that you configure a user name and password as the first step under advanced configuration to control management access to the wireless bridge (page 6-23).

Advanced Configuration

The Advanced Configuration pages include the following options.

Menu	Description	Page
System	Configures basic administrative and client access	6-3
Identification	Specifies the system name, location and contact information	6-3
TCP / IP Settings	Configures the IP address, subnet mask, gateway, and domain name servers	6-5
RADIUS	Configures the RADIUS server for wireless client authentication	6-7
PPPoE Settings	Configures PPPoE on the Ethernet interface for a connection to an ISP	6-9
Authentication	Configures 802.1X client authentication and MAC address authentication	6-11
Filter Control	Enables VLAN support and filters traffic matching specific Ethernet protocol types	6-18
SNMP	Controls access to this wireless bridge from management stations using SNMP, as well as the hosts that will receive trap messages	6-20
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 wireless bridge	6-23
System Log	Controls logging of error messages; sets the system clock via SNTP server or manual configuration	6-27
WDS	Sets the MAC addresses of other units in the wireless bridge network	6-31
Bridge	Sets the time for aging out entries in the bridge MAC address table	6-33
STP	Configures Spanning Tree Protocol parameters	6-36
RSSI	Controls the maximum RSSI voltage output for specific WDS ports	6-40
Radio Interface A	Configures the IEEE 802.11a interface	6-41
Radio Settings	Configures radio signal parameters, such as radio channel, transmission rate, and beacon settings	6-42
Security	Configures data encryption using Wired Equivalent Protection (WEP) or Wi-Fi Protected Access (WPA)	6-48
Radio Interface G	Configures the IEEE 802.11b/g interface	6-46
Radio Settings	Configures radio signal parameters, such as radio channel, transmission rate, and beacon settings	6-46
Security	Configures data encryption using Wired Equivalent Protection (WEP) or Wi-Fi Protected Access (WPA)	6-48

System Identification

The system information parameters for the wireless bridge can be left at their default settings. However, modifying these parameters can help you to more easily distinguish different devices in your network.

The wireless bridge allows the selection of the band to be used for bridge links. The bridge band can support no wireless clients. Alternatively, bridging can be disabled and both bands can support access point functions.

System Name – An alias for the wireless bridge, enabling the device to be uniquely identified on the network. (Default: Dual Band Outdoor AP; Range: 1-22 characters)

Outdoor Bridge Band – Selects the radio band used for bridge links.

- A – Bridging is supported on the 802.11a 5 GHz band.
- G – Bridging is supported on the 802.11b/g 2.4 GHz band.
- None – Bridging is not supported on either radio band. Allows both bands to support access point operations for wireless clients.

Location – A text string that describes the system location. (Maximum length: 20 characters)

Contact – A 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 wireless bridge 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.

```
DUAL OUTDOOR#configure                                                      6-8
DUAL OUTDOOR(config)#system name R&D                                        6-14
DUAL OUTDOOR(config)#snmp-server location building-1                        6-42
DUAL OUTDOOR(config)#snmp-server contact Paul                               6-41
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show system                                                    6-23

System Information
===================================================
Serial Number       : 0000000005
System Up time      : 0 days, 0 hours, 35 minutes, 56 seconds
System Name         : R&D
System Location     : building-1
System Contact      : Paul
System Country Code : US - UNITED STATES
MAC Address         : 00-30-F1-BE-F4-96
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    : v1.1.0.3
===================================================

DUAL OUTDOOR#
```

CLI Commands for Bridge Band Selection – Enter the global configuration mode and use the **wds channel** command to specify the bridge band.

```
DUAL OUTDOOR#configure                                                      6-8
DUAL OUTDOOR(config)#wds channel a                                          7-43
DUAL OUTDOOR(config)#
```

TCP / IP Settings

Configuring the wireless bridge with an IP address expands your ability to manage the wireless bridge. A number of wireless bridge features depend on IP addressing to operate.

Note: You can use the web browser interface to access IP addressing only if the wireless bridge already has an IP address that is reachable through your network.

By default, the wireless bridge will be automatically configured with IP settings from a Dynamic Host Configuration Protocol (DHCP) server. However, if you are not using a DHCP server to configure IP addressing, use the CLI to manually configure the initial IP values (page 4-2). After you have network access to the wireless bridge, you can use the web browser interface to modify the initial IP configuration, if needed.

Note: If there is no DHCP server on your network, or DHCP fails, the wireless bridge will automatically start up with a default IP address of 192.168.1.1.

DHCP Client (Enable) – Select this option to obtain the IP settings for the wireless bridge 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 wireless bridge by the network DHCP server. (Default: Enabled)

DHCP Client (Disable) – Select this option to manually configure a static address for the wireless bridge.

- IP Address: The IP address of the wireless bridge. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- Subnet Mask: The mask that identifies the host address bits used for routing to specific subnets.
- Default Gateway: The default gateway is the IP address of the router for the wireless bridge, which is used if the requested destination address is not on the local subnet.

  If you have management stations, DNS, 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: The 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 the 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).

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.

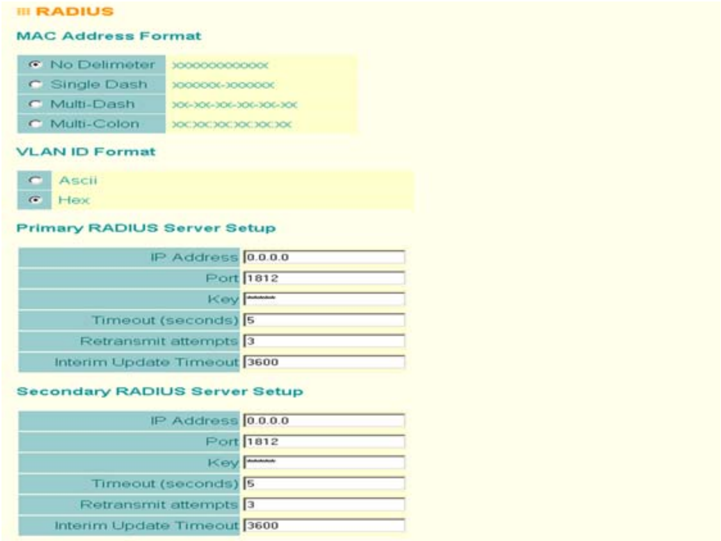
```
DUAL OUTDOOR(config)#interface ethernet                             6-87
Enter Ethernet configuration commands, one per line.
DUAL OUTDOOR(if-ethernet)#no ip dhcp                                6-89
DUAL OUTDOOR(if-ethernet)#ip address 192.168.1.2
255.255.255.0 192.168.1.253                                         6-88
DUAL OUTDOOR(if-ethernet)#dns primary-server 192.168.1.55           6-88
DUAL OUTDOOR(if-ethernet)#dns secondary-server 10.1.0.55            6-88
DUAL OUTDOOR(config)#end                                            6-8
DUAL OUTDOOR#show interface ethernet                                6-91
Ethernet Interface Information
========================================
IP Address          : 192.168.1.2
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
========================================
DUAL OUTDOOR#
```

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 that requires access to the network.

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.

Note: This guide assumes that you have already configured RADIUS server(s) 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.



RADIUS

MAC Address Format

● No Delimeter	XXXXXXXXXXXX
○ Single Dash	XXXXXX-XXXXXX
○ Multi-Dash	XX-XX-XX-XX-XX-XX
○ Multi-Colon	XX:XX:XX:XX:XX:XX

VLAN ID Format

○ Ascii
● Hex

Primary RADIUS Server Setup

IP Address	0.0.0.0
Port	1812
Key	*****
Timeout (seconds)	5
Retransmit attempts	3
Interim Update Timeout	3600

Secondary RADIUS Server Setup

IP Address	0.0.0.0
Port	1812
Key	*****
Timeout (seconds)	5
Retransmit attempts	3
Interim Update Timeout	3600

Primary Radius Server Setup – Configure the following settings to use RADIUS authentication on the access point.

- IP Address: Specifies the IP address or host name of the RADIUS server.
- Port: The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- Key: A 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)

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

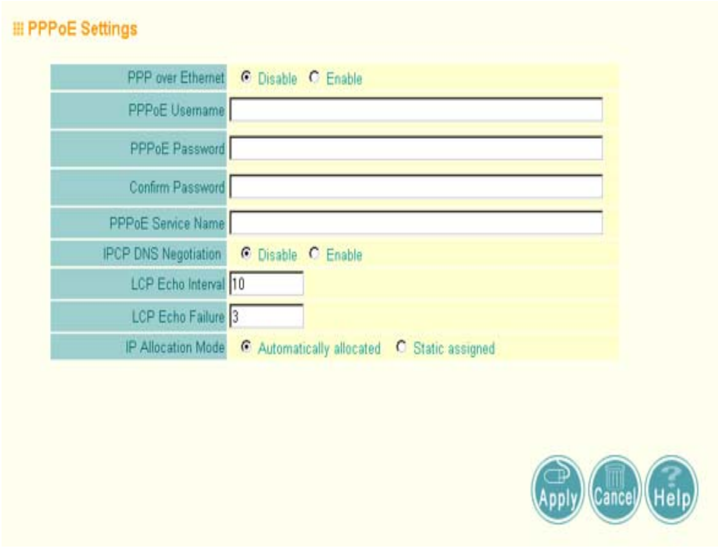
Secondary Radius Server Setup – Configure a secondary RADIUS server to provide a backup in case the primary server fails. The access point uses the secondary server if the primary server fails or becomes inaccessible. Once the access point switches over to the secondary server, it periodically attempts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

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 show radius** command from the Exec mode to display the current settings for the primary and secondary RADIUS servers.

```
DUAL OUTDOOR(config)#radius-server address 192.168.1.25           6-59
DUAL OUTDOOR(config)#radius-server port 181                       6-60
DUAL OUTDOOR(config)#radius-server key green                      6-60
DUAL OUTDOOR(config)#radius-server timeout 10                     6-61
DUAL OUTDOOR(config)#radius-server retransmit 5                   6-61
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show radius                                          6-64

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
========================================
DUAL OUTDOOR#
```

PPPoE Settings

The wireless bridge uses a Point-to-Point Protocol over Ethernet (PPPoE) connection, or tunnel, only for management traffic between the wireless bridge and a remote PPPoE server (typically at an ISP). Examples of management traffic that may initiated by the wireless bridge and carried over a PPPoE tunnel are RADIUS, Syslog, or DHCP traffic.



PPPoE Settings

PPP over Ethernet	● Disable ○ Enable
PPPoE Username	
PPPoE Password	
Confirm Password	
PPPoE Service Name	
IPCP DNS Negotiation	● Disable ○ Enable
LCP Echo Interval	10
LCP Echo Failure	3
IP Allocation Mode	● Automatically allocated ○ Static assigned

PPP over Ethernet – Enable PPPoE on the RJ-45 Ethernet interface to pass management traffic between the unit and a remote PPPoE server. (Default: Disable)

PPPoE Username – The user name assigned for the PPPoE tunnel. (Range: 1-63 alphanumeric characters)

PPPoE Password – The password assigned for the PPPoE tunnel. (Range: 1-63 alphanumeric characters)

Confirm Password – Use this field to confirm the PPPoE password.

PPPoE Service Name – The service name assigned for the PPPoE tunnel. The service name is normally optional, but may be required by some service providers. (Range: 1-63 alphanumeric characters)

IP Allocation Mode – This field specifies how IP adresses for the PPPoE tunnel are configured on the RJ-45 interface. The allocation mode depends on the type of service provided by the PPPoE server. If automatic mode is selected, DHCP is used to allocate the IP addresses for the PPPoE connection. If static addresses have been assigned to you by the service provider, you must manually enter the assigned addresses. (Default: Automatic)

- Automatically allocated: IP addresses are dynamically assigned by the service provider during PPPoE session initialization.
- Static assigned: Fixed addresses are assigned by the service provider for both the local and remote IP addresses.

Local IP Address – IP address of the local end of the PPPoE tunnel. (Must be entered for static IP allocation mode.)

Remote IP Address – IP address of the remote end of the PPPoE tunnel. (Must be entered for static IP allocation mode.)

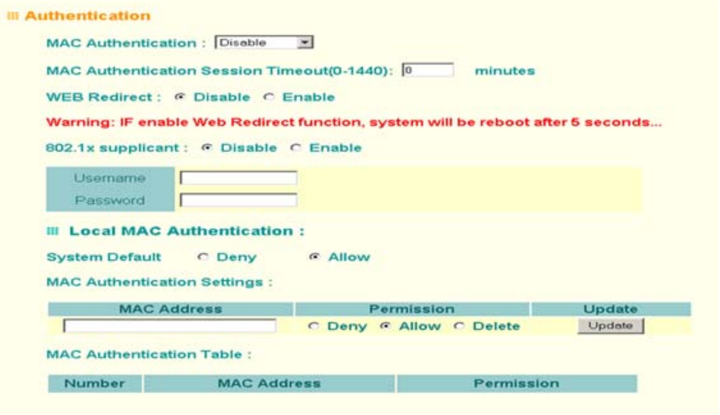
CLI Commands for PPPoE – From the CLI configuration mode, use the **interface ethernet** command to access interface configuration mode. Use the **ip pppoe** command to enable PPPoE on the Ethernet interface. Use the other PPPoE commands shown in the example below to set a user name and password, IP settings, and other PPPoE parameters as required by the service provider. The **pppoe restart** command can then be used to start a new connection using the modified settings. To display the current PPPoE settings, use the **show pppoe** command from the Exec mode.

```
DUAL OUTDOOR(config)#interface ethernet                              6-87
Enter Ethernet configuration commands, one per line.
DUAL OUTDOOR(if-ethernet)#ip pppoe                                   7-57
DUAL OUTDOOR(if-ethernet)#pppoe username mike                        7-61
DUAL OUTDOOR(if-ethernet)#pppoe password 12345                       7-61
DUAL OUTDOOR(if-ethernet)#pppoe service-name classA                  7-62
DUAL OUTDOOR(if-ethernet)#pppoe ip allocation mode static            7-57
DUAL OUTDOOR(if-ethernet)#pppoe local ip 10.7.1.200                  7-60
DUAL OUTDOOR(if-ethernet)#pppoe remote ip 192.168.1.20               7-60
DUAL OUTDOOR(if-ethernet)#pppoe ipcp dns                             7-58
DUAL OUTDOOR(if-ethernet)#pppoe lcp echo-interval 30                 7-58
DUAL OUTDOOR(if-ethernet)#pppoe lcp echo-failure 5                   7-59
DUAL OUTDOOR(if-ethernet)#pppoe restart                              6-87
DUAL OUTDOOR(if-ethernet)#end
DUAL OUTDOOR#show pppoe                                              7-63

PPPoE Information
======================================================
State                  : Link up
Username               : mike
Service Name           : classA
IP Allocation Mode     : Static
DNS Negotiation        : Enabled
Local IP               : 10.7.1.200
Echo Interval          : 30
Echo Failure           : 5
======================================================

DUAL OUTDOOR#
```

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 a 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.



Authentication

MAC Authentication : Disable

MAC Authentication Session Timeout(0-1440): 0 minutes

WEB Redirect : ● Disable ○ Enable

Warning: IF enable Web Redirect function, system will be reboot after 5 seconds...

802.1x supplicant : ● Disable ○ Enable

Username	
Password	

Local MAC Authentication :

System Default ○ Deny ● Allow

MAC Authentication Settings :

MAC Address	Permission	Update
	○ Deny ● Allow ○ Delete	Update

MAC Authentication Table :

Number	MAC Address	Permission

Ethernet Supplicant Setup – Allows the access point to act as an 802.1X supplicant so it can be authenticated through its Ethernet port with a RADIUS server on the local network. When enabled, a unique MD5 user name and password needs to be configured. (Default: Disabled)

- Enabled/Disabled – Enables/Disables the 802.1X supplicant function.
  - Username – Specifies the MD5 user name. (Range: 1-22 characters)
  - Password – Specifies the MD5 password. (Range: 1-22 characters)

WDS Supplicant Setup – Allows the access point to 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 a OAP6626A Slave unit, there is only one WDS port. For a OAP6626AM Master unit, there are 16 WDS ports. (Default: Disabled)

MAC Authentication – 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)

- Local MAC: 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.
- Radius MAC: The MAC address of the associating station is sent to a configured RADIUS server for authentication. When using a RADIUS authentication server for MAC address authentication, the server must first be configured in the Radius window (page 6-7).
- Disable: No checks are performed on an associating station’s MAC address.

Note: 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.

802.1X Setup – 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.

You can enable 802.1X as optionally supported or as required to enhance the security of the wireless network.

- 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.
- 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.

When 802.1X is enabled, the broadcast and session key rotation intervals can also be configured.

- 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 Re-authentication 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)

Local MAC Authentication – Configures the local MAC authentication database. 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.

- System Default: Specifies a default action for all unknown MAC addresses (that is, those not listed in the local MAC database).
  - 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."
- MAC Authentication Settings: Enters specified MAC addresses and permissions into the local MAC database.
  - MAC Address: Physical address of a client. Enter six pairs of hexadecimal digits separated by hyphens; for example, 00-90-D1-12-AB-89.
  - Permission: Select Allow to permit access or Deny to block access. If Delete is selected, the specified MAC address entry is removed from the database.
  - Update: Enters the specified MAC address and permission setting into the local database.
- MAC Authentication Table: Displays current entries in the local MAC database.

CLI Commands for 802.1X Suppicant Configuration – Use the **802.1X supplicant** commands to set the Ethernet and WDS user names and passwords, and to enable the feature.

```
DUAL OUTDOOR(config)#802.1X supplicant eth_user David                  7-38
DUAL OUTDOOR(config)#802.1X supplicant eth_password DEF                7-38
DUAL OUTDOOR(config)#802.1X supplicant eth                             7-38
DUAL OUTDOOR(config)#
DUAL OUTDOOR(config)#802.1X supplicant wds_user 1 David              7-38
DUAL OUTDOOR(config)#802.1X supplicant wds_password 1 ABC            7-38
DUAL OUTDOOR(config)#802.1X supplicant wds 1                         7-38
DUAL OUTDOOR(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.

```
DUAL OUTDOOR(config)#mac-authentication server local              6-72
DUAL OUTDOOR(config)#address filter default denied                 6-70
DUAL OUTDOOR(config)#address filter entry 00-70-50-cc-99-1a
denied                                                             6-71
DUAL OUTDOOR(config)#address filter entry 00-70-50-cc-99-1b allowed
DUAL OUTDOOR(config)#address filter entry 00-70-50-cc-99-1c allowed
DUAL OUTDOOR(config)#address filter delete 00-70-50-cc-99-1c       6-71
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show authentication                                   6-68

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
=========================================================
DUAL OUTDOOR#
```

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.

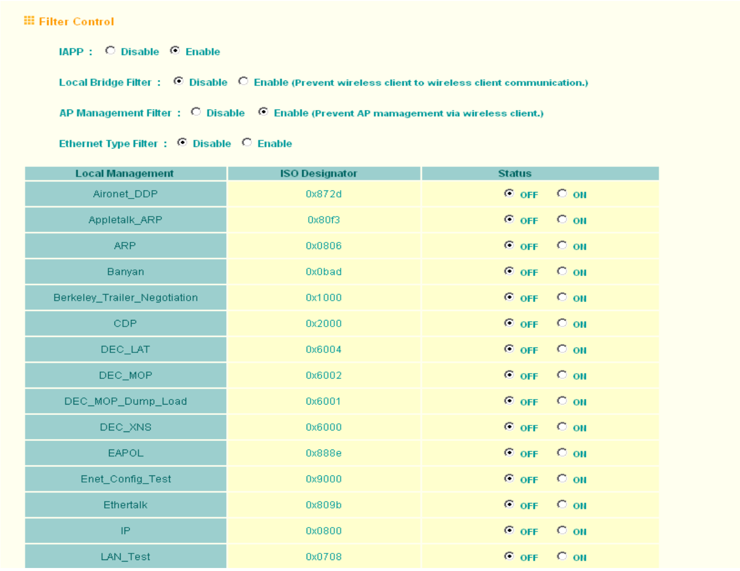
```
DUAL OUTDOOR(config)#mac-authentication server remote              6-72
DUAL OUTDOOR(config)#mac-authentication session-timeout 300        6-72
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show authentication                                   6-68

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
=========================================================
DUAL OUTDOOR#
```

CLI Commands for 802.1X Authentication – Use the **802.1X supported** command from the global configuration mode to enable 802.1X authentication. Set the session and broadcast key refresh rate, and the re-authentication timeout. To display the current settings, use the **show authentication** command from the Exec mode.

```
DUAL OUTDOOR(config)#802.1X supported                               6-65
DUAL OUTDOOR(config)#802.1X broadcast-key-refresh-rate 5            6-66
DUAL OUTDOOR(config)#802.1X session-key-refresh-rate 5              6-67
DUAL OUTDOOR(config)#802.1X session-timeout 300                     6-67
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show authentication                                    6-68

Authentication Information
=========================================================
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 300 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
=========================================================
DUAL OUTDOOR#
```

Filter Control

The wireless bridge can employ VLAN tagging support and network traffic frame filtering to control access to network resources and increase security.



Filter Control

IAPP : ○ Disable ● Enable

Local Bridge Filter : ● Disable ○ Enable (Prevent wireless client to wireless client communication.)

AP Management Filter : ○ Disable ● Enable (Prevent AP mamagement via wireless client.)

Ethernet Type Filter : ● Disable ○ Enable

Local Management	ISO Designator	Status
Aironet_DDP	0x872d	● OFF ○ ON
Appletalk_ARP	0x80f3	● OFF ○ ON
ARP	0x0806	● OFF ○ ON
Banyan	0x0bad	● OFF ○ ON
Berkeley_Trailer_Negotiation	0x1000	● OFF ○ ON
CDP	0x2000	● OFF ○ ON
DEC_LAT	0x6004	● OFF ○ ON
DEC_MOP	0x6002	● OFF ○ ON
DEC_MOP_Dump_Load	0x6001	● OFF ○ ON
DEC_XNS	0x6000	● OFF ○ ON
EAPOL	0x888e	● OFF ○ ON
Enet_Config_Test	0x9000	● OFF ○ ON
Ethertalk	0x809b	● OFF ○ ON
IP	0x0800	● OFF ○ ON
LAN_Test	0x0708	● OFF ○ ON

Native VLAN ID – The VLAN ID assigned to wireless clients that are not assigned to a specific VLAN by RADIUS server configuration. (Range: 1-64)

VLAN – Enables or disables VLAN tagging support on the wireless bridge (changing the VLAN status forces a system reboot). When VLAN support is enabled, the wireless bridge tags traffic passing to the wired network with the assigned VLAN ID associated with each client on the RADIUS server or the configured native VLAN ID. Traffic received from the wired network must also be tagged with a known VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped. When VLAN support is disabled, the wireless bridge does not tag traffic passing to the wired network and ignores the VLAN tags on any received frames.

Note: Before enabling VLANs on the wireless bridge, you must configure the connected LAN switch port to accept tagged VLAN packets with the wireless bridge's native VLAN ID. Otherwise, connectivity to the wireless bridge will be lost when you enable the VLAN feature.

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 wireless clients, thereby improving security.

A VLAN ID (1-4094) is assigned to a client after successful authentication using IEEE 802.1X and a central RADIUS server. The user VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. If a user does not have a configured VLAN ID, the access point assigns the user to its own configured native VLAN ID.

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.

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

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

When VLAN filtering is enabled, the access point must also have 802.1X authentication enabled and a RADIUS server configured. Wireless clients must also support 802.1X client software to be assigned to a specific VLAN.

When VLAN filtering is disabled, the access point ignores the VLAN tags on any received frames.

Local Bridge Filter – Controls wireless-to-wireless communications between clients through the access point. However, it does not affect communications between wireless clients and the wired network.

- Disable: Allows wireless-to-wireless communications between clients through the access point.
- Enable: Blocks wireless-to-wireless communications between clients through the access point.

AP Management Filter – Controls management access to the access point from wireless clients. Management interfaces include the web, Telnet, or SNMP.

- Disable: Allows management access from wireless clients.
- Enable: Blocks management access from wireless clients.

Ethernet Type Filter – Controls checks on the Ethernet type of all incoming and outgoing Ethernet packets against the protocol filtering table.

- Disable: Wireless bridge does not filter Ethernet protocol types.
- Enable: Wireless bridge filters Ethernet protocol types based on the configuration of protocol types in the filter table. If a protocol has its status set to “ON,” the protocol is filtered from the wireless bridge.

CLI Commands for VLAN Support – From the global configuration mode use the **native-vlanid** command to set the default VLAN ID for the Ethernet interface, then enable VLANs using the **vlan enable** command. When you change the access point’s VLAN support setting, you must reboot the access point to implement the change. To view the current VLAN settings, use the **show system** command.

```
DUAL OUTDOOR(config)#native-vlanid 3                              7-87
DUAL OUTDOOR(config)#vlan enable                                   6-130
Reboot system now? <y/n>: y
```

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.

```
DUAL OUTDOOR(config)#filter ap-manage                              6-74
DUAL OUTDOOR(config)#filter ethernet-type enable                   6-74
DUAL OUTDOOR(config)#filter ethernet-type protocol ARP             6-75
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show filters                                          6-76

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

Enabled Protocol Filters
---------------------------------------------------------
Protocol: ARP                             ISO: 0x0806
=========================================================
DUAL OUTDOOR#
```

SNMP

You can use a network management application to manage the wireless bridge via the Simple Network Management Protocol (SNMP) from a management station. To implement SNMP management, the wireless bridge 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 wireless bridge. To communicate with the wireless bridge, 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.

SNMP – Enables or disables SNMP management access and also enables the wireless bridge to send SNMP traps (notifications). SNMP management is enabled by default.

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 IP Address – Specifies the recipient of SNMP notifications. Enter the IP address or the host name. (Host Name: 1 to 20 characters)

Trap Destination Community Name – The community string sent with the notification operation. (Maximum length: 23 characters; Default: public)

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.

```
DUAL OUTDOOR(config)#snmp-server enable server                      6-42
DUAL OUTDOOR(config)#snmp-server community alpha rw                 6-41
DUAL OUTDOOR(config)#snmp-server community beta ro
DUAL OUTDOOR(config)#snmp-server host 10.1.19.23 alpha              6-43
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show snmp                                              6-54

SNMP Information
============================================
Service State  : Enable
Community (ro) : ****
Community (rw) : *****
Location       : building-1
Contact        : Paul
Traps          : Enabled
Host Name/IP   : 10.1.19.23
Trap Community : *****
=============================================

DUAL OUTDOOR#
```

Administration

Changing the Password

Management access to the web and CLI interface on the wireless bridge 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 6-18).

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 wireless bridge may be able to compromise wireless bridge and network security.

Note: Pressing the Reset button on the back of the wireless bridge for more than five seconds resets the user name and password to the factory defaults. For this reason, we recommend that you protect the wireless bridge from physical access by unauthorized persons.

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 the User Name and Password – Use the username and password commands from the CLI configuration mode.

```
DUAL OUTDOOR(config)#username bob                                      6-15
DUAL OUTDOOR(config)#password spiderman                                6-15
DUAL OUTDOOR#
```

Upgrading Firmware

You can upgrade new wireless bridge software from a local file on the management workstation, or from an FTP or TFTP server.

After upgrading new software, you must reboot the wireless bridge to implement the new code. Until a reboot occurs, the wireless bridge will continue to run the software it was using before the upgrade started. Also note that rebooting the wireless bridge with new software will reset the configuration to the factory default settings.

Note: Before upgrading your wireless bridge software, it is recommended to save a copy of the current configuration file. See “copy” on page 6-56 for information on saving the configuration file to a TFTP or FTP server.

Before upgrading new software, verify that the wireless bridge 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:

- Obtain the IP address of the FTP or TFTP server where the wireless bridge software is stored.
- If upgrading from an FTP server, be sure that you have an account configured on the server with a user name and password.

Current version – Version number of runtime code.

Firmware Upgrade Local – Downloads an operation code image file from the web management station to the wireless bridge using HTTP. Use the Browse button to locate the image file locally on the management station and click Start Upgrade to proceed.

- New firmware file: Specifies 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 is 32 characters for files on the wireless bridge. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

Firmware Upgrade Remote – 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: Specifies 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 wireless bridge. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- IP Address: IP address or host name of FTP or TFTP server.
- Username: The user ID used for login on an FTP server.
- Password: The password used for login on an FTP server.

Restore Factory Settings – Click the Restore button to reset the configuration settings for the wireless bridge 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 wireless bridge – Click the Reset button to reboot the system.

Note: If you have upgraded system software, then you must reboot the wireless bridge to implement the new operation code.

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 wireless bridge file system. To run the new software, use the **reset board** command to reboot the wireless bridge.

```
DUAL OUTDOOR#copy tftp file                                          6-56
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

DUAL OUTDOOR#dir                                                     6-58
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

DUAL OUTDOOR#reset board                                             6-10
Reboot system now? <y/n>: y
```

System Log

The wireless bridge 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.

Enabling System Logging

The wireless bridge 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 wireless bridge and network problems.

System Log Setup – Enables the logging of error messages.

Logging Host – Enables the sending of log messages to a Syslog server host.

Server Name/IP – The IP address or name of a Syslog server.

Logging Console – Enables the logging of error messages to the console.

Logging Level – Sets the minimum severity level for event logging.

The system allows you to limit the messages that are logged by specifying a minimum severity level. The following table lists the error message levels from the most severe (Emergency) to least severe (Debug). The message levels that are logged include the specified minimum level up to the Emergency level.

Error Level	Description
Emergency	System unusable
Alert	Immediate action needed
Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
Error	Error conditions (e.g., invalid input, default used)
Warning	Warning conditions (e.g., return false, unexpected return)
Notice	Normal but significant condition, such as cold start
Informational	Informational messages only
Debug	Debugging messages

Note: The wireless bridge error log can be viewed using the Event Logs window in the Status section (page 6-67).The Event Logs window displays the last 128 messages logged in chronological order, from the newest to the oldest. Log messages saved in the wireless bridge’s memory are erased when the device is rebooted.

CLI Commands for System Logging – To enable logging on the wireless bridge, 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.

```
DUAL OUTDOOR(config)#logging on                                        6-29
DUAL OUTDOOR(config)#logging level alert                               6-30
DUAL OUTDOOR(config)#logging console                                   6-30
DUAL OUTDOOR(config)#logging host 1 10.1.0.3 514                       6-29
DUAL OUTDOOR(config)#logging facility-type 19                          6-31
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show logging                                              6-32

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
=============================================

DUAL OUTDOOR#
```

Configuring SNTP

Simple Network Time Protocol (SNTP) allows the wireless bridge to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the wireless bridge enables the system log to record meaningful dates and times for event entries. If the clock is not set, the wireless bridge will only record the time from the factory default set at the last bootup.

The wireless bridge 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 wireless bridge will attempt to poll each server in the configured sequence.

SNTP Server – Configures the wireless bridge to operate as an SNTP client. When enabled, at least one time server IP address must be specified.

- Primary Server: The IP address of an SNTP or NTP time server that the wireless bridge attempts to poll for a time update.
- Secondary Server: The IP address of a secondary SNTP or NTP time server. The wireless bridge first attempts to update the time from the primary server; if this fails it attempts an update from the secondary server.

Note: The wireless bridge also allows you to disable SNTP and set the system clock manually using the CLI.

Set Time Zone – SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or 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 wireless bridge 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 by one hour.

CLI Commands for SNTP – To enable SNTP support on the wireless bridge, 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.

```
DUAL OUTDOOR(config)#sntp-server ip 10.1.0.19                      6-34
DUAL OUTDOOR(config)#sntp-server enable                            6-34
DUAL OUTDOOR(config)#sntp-server timezone +8                       6-36
DUAL OUTDOOR(config)#sntp-server daylight-saving                   6-36
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
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show sntp                                             6-37

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
=========================================================

DUAL OUTDOOR#
```

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 wireless bridge.

```
DUAL OUTDOOR(config)#no sntp-server enable                          6-34
DUAL OUTDOOR(config)#sntp-server date-time                          6-35
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
DUAL OUTDOOR(config)#
```

Wireless Distribution System (WDS)

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

To set up a wireless bridge link, you must configure the WDS forwarding table by specifying the wireless MAC address of the bridge to which you want to forward traffic. For a Slave bridge unit, you need to specify the MAC address of the wireless bridge unit at the opposite end of the link. For a Master bridge unit, you need to specify the MAC addresses of all the Slave bridge units in the network.

Mode – The wireless bridge is set to operate as a Slave or Master unit:

- Master Mode: In a point-to-multipoint network configuration, only one wireless bridge unit must be a Master unit (all others must be Slave units). A Master wireless bridge provides support for up to 16 MAC addresses in the WDS forwarding table. The MAC addresses of all other Slave bridge units in the network must be configured in the forwarding table.
- Slave Mode: A Slave wireless bridge provides support for only one MAC address in the WDS forwarding table. A Slave bridge communicates with only one other wireless bridge, either another Slave bridge in a point-to-point configuration, or to the Master bridge in a point-to-multipoint configuration.

Port Number (Master bridge only) – The wireless port identifier.

MAC Address – The physical layer address of the wireless bridge unit at the other end of the wireless link. (12 hexadecimal digits in the form “xx:xx:xx:xx:xx:xx”)

Port Status – Enables or disables the wireless bridge link.

Note: The wireless MAC address for each bridge unit is printed on the label on the back of the unit.

CLI Commands for WDS – The following example shows how to configure the MAC address of the wireless bridge at the opposite end of a point-to-point link, and then enable forwarding on the link.

```
DUAL OUTDOOR(config)#wds mac-address 1 00-12-34-56-78-9a            7-43
DUAL OUTDOOR(config)#wds enable                                     7-44
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show wds                                               7-44

      Outdoor_Mode    :     SLAVE
==================================================
  Port ID  |     Status    |    Mac-Address
==================================================
     01    |     ENABLE    |    00-12-34-56-78-9A
==================================================
DUAL OUTDOOR#
```

Bridge

The wireless bridge can store the MAC addresses for all known devices in the connected networks. All the addresses are learned by monitoring traffic received by the wireless bridge and are stored in a dynamic MAC address table. This information is then used to forward traffic directly between the Ethernet port and the corresponding wireless interface.

The Bridging page allows the MAC address aging time to be set for both the Ethernet port and the bridge radio interface. 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.

Bridge Aging Time – Changes the aging time for entries in the dynamic address table:

- Ethernet: The time after which a learned Ethernet port entry is discarded. (Range: 60-1800 seconds; Default: 100 seconds)
- Wireless 802.11a (g): The time after which a learned wireless entry is discarded. (Range: 60-1800 seconds; Default: 1800 seconds)

CLI Commands for Bridging – The following example shows how to set the MAC address aging time for the wireless bridge.

```
DUAL OUTDOOR(config)#bridge timeout 0 300                             7-46
DUAL OUTDOOR(config)#bridge timeout 2 1000                            7-46
DUAL OUTDOOR(config)#exit
DUAL OUTDOOR#show bridge                                              7-52

              Bridge  Information
=================================================
 Media Type | Age Time(sec)|
=================================================
  EtherNet  |   300        |
  WLAN_A    |  1000        |
==================================================

Bridge Id           : 32768.037fbef192
Root Bridge Id      : 32768.01f47483e2
Root Path Cost      : 25
Root Port Id        : 0
Bridge Status       : Enabled
Bridge Priority     : 32768
Bridge Hello Time   : 2 Seconds
Bridge Maximum Age  : 20 Seconds
Bridge Forward Delay: 15 Seconds
============================= Port Summary =============================
Id| Priority | Path Cost |  Fast Forward  |  Status  |      State      |
 0     128        25            Enable       Enabled      Forwarding

DUAL OUTDOOR#
```

Spanning Tree Protocol (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.

Enable – Enables/disables STP on the wireless bridge. (Default: Enabled)

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 seconds)

- Default: 15
- Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
- Maximum: 30

Hello Time – Interval (in seconds) at which the root device transmits a configuration message. (Range: 1-10 seconds)

- Default: 2
- Minimum: 1
- Maximum: The lower of 10 or [(Max. Message Age / 2) -1]

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 seconds)

- Default: 20
- Minimum: The higher of 6 or [2 x (Hello Time + 1)].
- Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

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

Port 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: 1-65535
- Default: Ethernet interface: 19; Wireless interface: 40

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.

- Default: 128
- Range: 0-240, in steps of 16

Port Fast (Fast Forwarding) – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying fast forwarding provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that fast forwarding should only be enabled for ports connected to an end-node device. (Default: Disabled)

Status – Enables/disables STP on this interface. (Default: Enabled)

CLI Commands for STP – The following example configures spanning tree paramters for the bridge and wireless port 5.

```
DUAL OUTDOOR(config)#bridge stp-bridge priority 40000              6-84
DUAL OUTDOOR(config)#bridge stp-bridge hello-time 5                6-83
DUAL OUTDOOR(config)#bridge stp-bridge max-age 38                  7-48
DUAL OUTDOOR(config)#bridge stp-bridge forward-time 20             6-83
DUAL OUTDOOR(config)#no bridge stp-port spanning-disabled 5        7-52
DUAL OUTDOOR(config)#bridge stp-port priority 5 0                  6-85
DUAL OUTDOOR(config)#bridge stp-port path-cost 5 50                6-85
DUAL OUTDOOR(config)#no bridge stp-port portfast 5                 7-51
DUAL OUTDOOR(config)#end
DUAL OUTDOOR#show bridge                                           7-52

              Bridge  Information
=================================================
 Media Type | Age Time(sec)|
=================================================
  EtherNet  |   300        |
  WLAN_A    |  1000        |
==================================================

Bridge Id           : 32768.037fbef192
Root Bridge Id      : 32768.01f47483e2
Root Path Cost      : 25
Root Port Id        : 0
Bridge Status       : Enabled
Bridge Priority     : 40000
Bridge Hello Time   : 5 Seconds
Bridge Maximum Age  : 38 Seconds
Bridge Forward Delay: 20 Seconds
============================= Port Summary =============================
Id| Priority | Path Cost |  Fast Forward  |  Status  |      State      |
 0     128        25            Enable       Enabled      Forwarding

DUAL OUTDOOR#
```

RSSI

The RSSI value displayed on the RSSI page represents a signal to noise ratio. A value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold. This value can be used to align antennas (see page 2-10) 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.

RSSI – The RSSI value for a selected port can be displayed and a representative voltage output can be enabled.

- Output Activate*:* Enables or disables the RSSI voltage output on the external RSSI connector. (Default: Enabled)
- Port Number: Selects a specific WDS port for which to set the maximum RSSI output voltage level. Ports 1-16 are available for a Master unit, only port 1 for a Slave unit. (Default: 1)
- Output Value: The maximum RSSI voltage level for the current selected WDS port. A value of zero indicates that there is no received signal or that the WDS port is disabled.

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: Indicates if the 802.11a radio is operating in normal or Turbo mode. (See "Radio Settings A" on page 6-42.)
- Distance: The approximate distance between antennas in a bridge link.

Note: There are currently no equivalent CLI commands for the RSSI controls.

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 access point 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

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

Radio Settings A (802.11a)

The 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.

Enable – Enables radio communications on the wireless interface. (Default: Enabled)

Description – Adds a comment or description to the wireless interface. (Range: 1-80 characters)

Network Name (SSID) – (Access point mode only) The name of the basic service set provided by the access point. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point. (Default: DualBandOutdoor; Range: 1-32 characters)

Note: The SSID is not configurable when the radio band is set to Bridge mode.

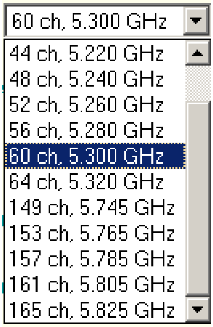
Secure Access – When enabled, the access point radio does not include its SSID in beacon messages. Nor does it respond to probe requests from clients that do not include a fixed SSID. (Default: Disable)

Turbo Mode – 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. (Default: Disabled)

Note: In normal mode, the wireless bridge provides a channel bandwidth of 20 MHz, and supports the maximum number of channels permitted by local regulations (e.g., 11 channels for the United States). In Turbo Mode, the channel bandwidth is increased to 40 MHz to support the increased data rate. However, this reduces the number of channels supported (e.g., 5 channels for the United States).

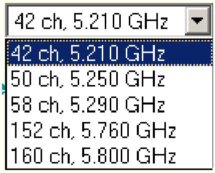
Radio Channel – The radio channel that the wireless bridge uses to communicate with wireless clients. When multiple wireless bridges are deployed in the same area, set the channel on neighboring wireless bridges at least four channels apart to avoid interference with each other. For example, in the United States you can deploy up to four wireless bridges in the same area (e.g., channels 36, 56, 149, 165). Also note that the channel for wireless clients is automatically set to the same as that used by the wireless bridge to which it is linked. (Default: Channel 60 for normal mode, and channel 42 for Turbo mode)

Normal Mode



Auto Channel Select – Enables the wireless bridge to automatically select an unoccupied radio channel. (Default: Enabled)

Turbo Mode



Transmit Power – Adjusts the power of the radio signals transmitted from the wireless bridge. 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)

Beacon Interval – The rate at which beacon signals are transmitted from the wireless bridge. The beacon signals allow wireless clients to maintain contact with the wireless bridge. They may also carry power-management information.
(Range: 20-1000 TUs; Default: 100 TUs)

Data Beacon Rate – The rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions.

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 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 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 wireless bridge. 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 wireless bridge 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 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 bridges 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)

Maximum Associations – (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)

CLI Commands for the 802.11a Wireless Interface – From the global configuration mode, enter the **interface wireless a** command to access the 802.11a radio interface. If required, configure a name for the interface using the **description** command. Use the **turbo** command to enable this feature before setting the radio channel with the **channel** command. Set any other parameters as required. To view the current 802.11a radio settings, use the **show interface wireless a** command.

```
DUAL OUTDOOR(config)#interface wireless a                           7-69
Enter Wireless configuration commands, one per line.
DUAL OUTDOOR(if-wireless a)#description RD-AP#3                     7-69
DUAL OUTDOOR(if-wireless a)#ssid r&d                                7-70
DUAL OUTDOOR(if-wireless a)#no turbo                                6-105
DUAL OUTDOOR(if-wireless a)#channel 44                              6-96
DUAL OUTDOOR(if-wireless a)#closed-system                           6-106
DUAL OUTDOOR(if-wireless a)#transmit-power full                     6-97
DUAL OUTDOOR(if-wireless a)#speed 9                                 6-95
DUAL OUTDOOR(if-wireless a)#max-association 32                      6-106
DUAL OUTDOOR(if-wireless a)#beacon-interval 150                     6-101
DUAL OUTDOOR(if-wireless a)#dtim-period 5                           6-101
DUAL OUTDOOR(if-wireless a)#fragmentation-length 512                6-102
DUAL OUTDOOR(if-wireless a)#rts-threshold 256                       6-103
DUAL OUTDOOR(if-wireless a)#exit
DUAL OUTDOOR#show interface wireless a                              6-109

Wireless Interface Information
===========================================================
----------------Identification-----------------------------
Description                : RD-AP#3
Service Type               : Access Point
SSID                       : r&d
Turbo Mode                 : OFF
Channel                    : 44
Status                     : Disable
----------------802.11 Parameters--------------------------
Transmit Power             : FULL (15 dBm)
Max Station Data Rate      : 9Mbps
Fragmentation Threshold    : 512 bytes
RTS Threshold              : 256 bytes
Beacon Interval            : 150 TUs
DTIM Interval              : 5 beacons
Maximum Association        : 32 stations
----------------Security-----------------------------------
Closed System              : ENABLED
Multicast cipher           : WEP
Unicast cipher             : WEP
WPA clients                : SUPPORTED
WPA Key Mgmt Mode          : DYNAMIC
WPA PSK Key Type           : HEX
Encryption                 : DISABLED
Default Transmit Key       : 1
Static Keys :
   Key 1: EMPTY    Key 2: EMPTY    Key 3: EMPTY    Key 4: EMPTY
Authentication Type        : OPEN
===========================================================
DUAL OUTDOOR#
```

Radio Settings G (802.11g)

The IEEE 802.11g standard operates within the 2.4 GHz band at up to 54 Mbps. Also note that because the IEEE 802.11g standard is an extension of the IEEE 802.11b standard, it allows clients with 802.11b wireless network cards to associate to an 802.11g access point.

Enable – Enables radio communications on the access point. (Default: Enabled)

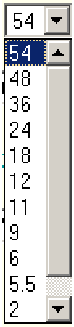
Radio Channel – The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, in the United States you can deploy up to three access points in the same area (e.g., channels 1, 6, 11). Also note that the channel for wireless clients is automatically set to the same as that used by the access point to which it is linked. (Range: 1-11 (US/Canada); Default: 1)

Auto Channel Select – Enables the access point to automatically select an unoccupied radio channel. (Default: Enabled)

Working Mode – Selects the operating mode for the 802.11g wireless interface. (Default: b & g mixed mode)

- b & g mixed mode: Both 802.11b and 802.11g clients can communicate with the access point (up to 54 Mbps).
- g only: Only 802.11g clients can communicate with the access point (up to 54 Mbps).
- b only: Both 802.11b and 802.11g clients can communicate with the access point, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps).

Maximum Station Data 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. (Default: 54 Mbps)



For a description of the remaining configuration items, see “Radio Settings A (802.11a)” on page 6-42.

CLI Commands for the 802.11g Wireless Interface – From the global configuration mode, enter the **interface wireless g** command to access the 802.11g radio interface. Set the interface SSID using the **ssid** command and, if required, configure a name for the interface using the **description** command. You can also use the **closed-system** command to stop sending the SSID in beacon messages. Select a radio channel or set selection to Auto using the **channel** command. Set any other parameters as required. To view the current 802.11g radio settings, use the **show interface wireless g** command.

```
DUAL OUTDOOR(config)#interface wireless g                     7-69
Enter Wireless configuration commands, one per line.
DUAL OUTDOOR(if-wireless g)#description RD-AP#3               7-69
DUAL OUTDOOR(if-wireless g)#ssid r&d                          7-70
DUAL OUTDOOR(if-wireless g)#channel auto                      6-96
DUAL OUTDOOR(if-wireless a)#closed-system                     6-106
DUAL OUTDOOR(if-wireless a)#transmit-power full               6-97
DUAL OUTDOOR(if-wireless g)#speed 6                           6-95
DUAL OUTDOOR(if-wireless g)#max-association 32                6-106
DUAL OUTDOOR(if-wireless g)#beacon-interval 150               6-105
DUAL OUTDOOR(if-wireless g)#dtim-period 5                     6-101
DUAL OUTDOOR(if-wireless g)#fragmentation-length 512          6-102
DUAL OUTDOOR(if-wireless g)#rts-threshold 256                 6-103
DUAL OUTDOOR(if-wireless g)#exit
DUAL OUTDOOR#show interface wireless g                             6-109

Wireless Interface Information
===========================================================
----------------Identification-----------------------------
Description                : Enterprise 802.11g Access Point
Service Type               : Access Point
SSID                       : r&d
Channel                    : 11 (AUTO)
Status                     : Enable
----------------802.11 Parameters--------------------------
Transmit Power             : FULL (14 dBm)
Max Station Data Rate      : 6Mbps
Fragmentation Threshold    : 512 bytes
RTS Threshold              : 256 bytes
Beacon Interval            : 150 TUs
DTIM Interval              : 5 beacons
Maximum Association        : 64 stations
----------------Security-----------------------------------
Closed System              : DISABLED
Multicast cipher           : WEP
Unicast cipher             : TKIP
WPA clients                : SUPPORTED
WPA Key Mgmt Mode          : DYNAMIC
WPA PSK Key Type           : HEX
Encryption                 : DISABLED
Default Transmit Key       : 1
Static Keys :
   Key 1: EMPTY   Key 2: EMPTY    Key 3: EMPTY    Key 4: EMPTY
Authentication Type        : OPEN
===========================================================
DUAL OUTDOOR#
```

Security (Bridge Mode)

Wired Equivalent Privacy (WEP) and Advanced Encryption Standard (AES) are implemented for security in bridge mode to prevent unauthorized access to network data. To secure bridge link data transmissions, enable WEP or AES encryption for the bridge radio and set at least one encryption key.

Wired Equivalent Privacy (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless bridge units. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually configured on all units in the wireless bridge network.

Setting up IEEE 802.11 Wired Equivalent Privacy (WEP) shared keys prevents unauthorized access to the wireless bridge network.

Be sure to define at least one static WEP key for data encryption. Also, be sure that the WEP keys are the same for all bridge units in the wireless network.

Data Encryption Setup – Enable or disable the wireless bridge to use either WEP or AES for data encryption. If WEP encryption is selected and enabled, you must configure at least one encryption key on the wireless bridge. (Default: Disable)

Shared Key Setup – Select 64 Bit, 128 Bit, or 152 Bit key length. Note that the same size of WEP encryption key must be set on all bridge units in the wireless network. (Default: 128 Bit)

Key Type – Select the preferred method of entering WEP encryption keys on the wireless bridge and enter up to four keys:

- Hexadecimal: Enter keys as 10 hexadecimal digits (0 to 9 and A to F) for 64 bit keys, 26 hexadecimal digits for 128 bit keys, or 32 hexadecimal digits for 152 bit keys.
- Alphanumeric: Enter keys as 5 alphanumeric characters for 64 bit keys, 13 alphanumeric characters for 128 bit keys, or 16 alphanumeric characters for 152 bit keys.

- Transmit Key Select: Selects the key number to use for encryption. Bridge units in the wireless network must have all four keys configured to the same values.

Note: Key index and type must match on all bridge units in the wireless network.

Advanced Encryption Standard (AES)

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 security standard.

The bridge radio band uses 128-bit static AES keys (hexadecimal or alphanumeric strings) that are configured for each link pair in the wireless bridge network. For a Slave bridge unit, only one encryption key needs to be defined. A Master bridge allows a different key to be defined for each wireless bridge link in the network.

Configuring AES encryption keys on the wireless bridge provides far more robust security than using WEP. Also, a unique AES key can be used for each bridge link in the wireless network, instead of all bridges sharing the same WEP keys.

Data Encryption Setup – Enable or disable the wireless bridge to use either WEP or AES for data encryption. If AES encryption is selected and enabled, you must configure one encryption key for each wireless port link on the wireless bridge. A Slave bridge supports only one wireless port link, but a Master bridge supports up to 16 links. (Default: Disable)

Key Type – Select the preferred method of entering AES encryption keys on the wireless bridge and enter a key for each bridge link in the network:

- Hexadecimal: Enter keys as exactly 32 hexadecimal digits (0 to 9 and A to F).
- Alphanumeric: Enter keys as an alphanumeric string using between 8 and 31 characters.

Note: For each wireless port link (1 to 16), the AES keys must match on the corresponding bridge unit.

CLI Commands for WEP Security – From the 802.11a interface configuration mode, use the **encryption** command to enable WEP encryption. To enter WEP keys, use the **key** command, and then set one key as the transmit key using the **transmit-key** command. To view the current security settings, use the **show interface wireless a** command.

```
DUAL OUTDOOR(config)#interface wireless a                          7-69
Enter Wireless configuration commands, one per line.
DUAL OUTDOOR(if-wireless a)#encryption wep 128                     6-118
DUAL OUTDOOR(if-wireless a)#key wep 1 128 ascii abcdeabcdeabc      6-119
DUAL OUTDOOR(if-wireless a)#transmit-key 1                         6-120
DUAL OUTDOOR(if-wireless a)#exit
DUAL OUTDOOR#show interface wireless a                             6-109

Wireless Interface Information
===========================================================
----------------Identification-----------------------------
Description                 : Enterprise 802.11a Access Point
Service Type                : WDS Bridge
SSID                        : DualBandOutdoor
Turbo Mode                  : OFF
Channel                     : 36
Status                      : Disable
----------------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 WEP ENCRYPTION
WEP Key type                : Alphanumeric
Default Transmit Key        : 1
Static Keys :
   Key 1: *****    Key 2: EMPTY    Key 3: EMPTY    Key 4: EMPTY
===========================================================
DUAL OUTDOOR#
```

Note: 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 AES Security – From the 802.11a interface configuration mode, use the **encryption** command to enable AES encryption. To enter AES keys, use the **key** command. To view the current security settings, use the **show interface wireless a** command.

```
DUAL OUTDOOR(config)#interface wireless a                           7-69
Enter Wireless configuration commands, one per line.
DUAL OUTDOOR(if-wireless a)#encryption wdsaes alphanumeric          6-118
DUAL OUTDOOR(if-wireless a)#key wdsaes 1 agoodsecretkey             6-119
DUAL OUTDOOR(if-wireless a)#exit
DUAL OUTDOOR#show interface wireless a                              6-109

Wireless Interface Information
===========================================================
----------------Identification-----------------------------
Description                 : Enterprise 802.11a Access Point
Service Type                : WDS Bridge
SSID                        : DualBandOutdoor
Turbo Mode                  : OFF
Channel                     : 36
Status                      : Disable
----------------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
===========================================================
DUAL OUTDOOR#
```

Note: The key type value entered using the **key** command must be the same as the type specified in the **encryption** command.

Security (Access Point Mode)

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 evesdropping.

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

• Wired Equivalent Privacy (WEP)	page 6-48
• IEEE 802.1X	page 6-12
• Wireless MAC address filtering	page 6-13
• Wi-Fi Protected Access (WPA)	page 6-59

The security mechanisms that may be employed 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 the following table.

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

Security Mechanism	Client Support	Implementation Considerations
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
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

Note: 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.

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.

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 same for each client in the wireless network.

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.

- Open System: Select this option if you plan to use WPA or 802.1X as a security mechanism. If you don't set up any other security mechanism on the access point, the network has no protection and is open to all users. This is the default setting.
- 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.

Note: To use 802.1X on wireless clients requires a network card driver and 802.1X client software that supports the EAP authentication type that you want to use. Windows 2000 SP3 or later and Windows XP provide 802.1X client support. Windows XP also provides native WPA support. Other systems require additional client software to support 802.1X and WPA.

Data Encryption Setup – Enable or disable the access point to use WEP shared keys for data encryption. If this option is selected, you must configure at least one key on the access point and all clients. (Default: Disable)

Note: You must enable data encryption through the web or CLI in order to enable all types of encryption (WEP, TKIP, and AES) in the access point.

Shared Key Setup – Select 64 Bit, 128 Bit, or 152 Bit key length. Note that the same size of encryption key must be supported on all wireless clients. 152 Bit key length is only supported on 802.11a radio. (Default: 128 Bit)

Key Type – Select the preferred method of entering WEP encryption keys on the access point and enter up to four keys:

- Hexadecimal: Enter keys as 10 hexadecimal digits (0 to 9 and A to F) for 64 bit keys, 26 hexadecimal digits for 128 bit keys, or 32 hexadecimal digits for 152 bit keys (802.11a radio only).
- Alphanumeric: Enter keys as 5 alphanumeric characters for 64 bit keys, 13 alphanumeric characters for 128 bit keys, or 16 alphanumeric characters for 152 bit keys (802.11a radio only).
- Transmit Key Select: Selects the key number to use for encryption. If the clients have all four keys configured to the same values, you can change the encryption key to any of the four settings without having to update the client keys.

Note: Key index and type must match that configured on the clients.

The configuration settings for WEP are summarized below:

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 6-11)
[2]: See Radius (page 6-7)

CLI Commands for static WEP Shared Key Security – From the 802.11a or 802.11g interface configuration mode, use the **authentication** command to enable WEP shared-key authentication and the **encryption** command to enable WEP encryption. Use the **multicast-cipher** command to select WEP cipher type. To enter WEP keys, use the **key** command, and then set one key as the transmit key using the **transmit-key** command. Then disable 802.1X port authentication with the **no 802.1X** command. To view the current security settings, use the **show interface wireless a** or **show interface wireless g** command.

```
DUAL OUTDOOR(config)#interface wireless g                                 7-69
Enter Wireless configuration commands, one per line.
DUAL OUTDOOR(if-wireless g)#authentication shared                         6-119
DUAL OUTDOOR(if-wireless g)#encryption 128                                6-118
DUAL OUTDOOR(if-wireless g)#multicast-cipher wep                          6-121
DUAL OUTDOOR(if-wireless g)#key 1 128 ascii abcdeabcdeabc                 6-119
DUAL OUTDOOR(if-wireless g)#transmit-key 1                                6-120
DUAL OUTDOOR(if-wireless g)#end
DUAL OUTDOOR(config)#no 802.1X                                            6-65
DUAL OUTDOOR(config)#end
DUAL OUTDOOR#show interface wireless g                                    6-109

Wireless Interface Information
===========================================================
----------------Identification-----------------------------
Description                 : Enterprise 802.11g Access Point
Service Type                : Access Point
SSID                        : DualBandOutdoor
Channel                     : 5 (AUTO)
Status                      : Disable
----------------802.11 Parameters--------------------------
Transmit Power              : FULL (20 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-----------------------------------
Closed System               : DISABLED
Multicast cipher            : WEP
Unicast cipher              : TKIP
WPA clients                 : SUPPORTED
WPA Key Mgmt Mode           : DYNAMIC
WPA PSK Key Type            : HEX
Encryption                  : 128-BIT ENCRYPTION
Default Transmit Key        : 1
Static Keys :
   Key 1: *****    Key 2: EMPTY    Key 3: EMPTY    Key 4: EMPTY
Authentication Type         : SHARED
===========================================================
DUAL OUTDOOR#
```

Note: 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 – From the 802.11a or 802.11g interface configuration mode, use the **authentication** command to select open system authentication. Use the **multicast-cipher** command to select WEP cipher type. Then set 802.1X to required with **802.1X** command, and disable MAC authentication with the **mac-authentication** command. To view the current 802.11g security settings, use the **show interface wireless g** command (not shown in example).

```
DUAL OUTDOOR(config)#interface wireless g                          7-69
Enter Wireless configuration commands, one per line.
DUAL OUTDOOR(if-wireless g)#authentication open                    6-119
DUAL OUTDOOR(if-wireless g)#encryption 128                         6-118
DUAL OUTDOOR(if-wireless g)#multicast-cipher wep                   6-121
DUAL OUTDOOR(if-wireless g)#end
DUAL OUTDOOR(config)#802.1X required                               6-65
DUAL OUTDOOR(config)#no mac-authentication                         6-72
DUAL OUTDOOR(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 following WPA components and features:

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.

Note: 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.

Advanced Encryption Standard (AES) **Support**: WPA specifies AES encryption as an optional alternative to TKIP and WEP. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP. The developing IEEE 802.11i wireless security standard has specified AES as an eventual replacement for TKIP and WEP. However, because of the difference in ciphering algorithms, AES requires new hardware support in client network cards that is currently not widely available. The access point includes AES support as a future security enhancement.

The WPA configuration parameters are described below:

Authentication Type Setup – When using WPA, set the access point to communicate as an open system to disable WEP keys.

Note: Although WEP keys are not needed for WPA, you must enable WEP encryption through the web or CLI in order to enable all types of encryption in the access point. For example, set Wired Equivalent Privacy (WEP) Setup to “Enable” on the Security page.

WPA Configuration Mode – The access point can be configured to allow only WPA-enabled clients to access the network, or also allow clients only capable of supporting WEP.

WPA Key Management – WPA can be configured to work in an enterprise environment using IEEE 802.1X and a RADIUS server for user authentication. For smaller networks, WPA can be enabled using a common pre-shared key for client authentication with the access point.

- WPA authentication over 802.1X: The WPA enterprise mode that uses IEEE 802.1X to authenticate users and to dynamically distribute encryption keys to clients.
- WPA Pre-shared Key: The WPA mode for small networks that uses a common password string that is manually distributed. If this mode is selected, be sure to also specify the key string.

Multicast Cipher Mode – Selects an encryption method for the global key used for multicast and broadcast traffic, which is supported by all wireless clients.

- 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: TKIP provides data encryption enhancements including per-packet key hashing (that is, changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.
- AES: 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.

WPA Pre-Shared Key Type – If the WPA 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, which can include spaces.

The configuration settings for WPA are summarized below:

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 web 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 6-11)
4: See Radius (page 6-7)

CLI Commands for WPA Pre-shared Key Security – From the 802.11a or 802.11g interface configuration mode, use the **authentication** command to set the access point to “Open System.” Use the WEP **encryption** command to enable all types of encryption. To enable WPA to be required for all clients, use the **wpa-clients** command. Use the **wpa-mode** command to enable the Pre-shared Key mode. To enter a key value, use the **wpa-psk-type** command to specify a hexadecimal or alphanumeric key, and then use the **wpa-preshared-key** command to define the key. Then disable 802.1X and MAC authentication. To view the current 802.11g security settings, use the **show interface wireless a** or **show interface wireless g** command (not shown in example).

```
AP(config)#interface wireless g                               7-69
Enter Wireless configuration commands, one per line.
AP(if-wireless g)#authentication open                         6-119
AP(if-wireless g)#encryption 128                              6-118
AP(if-wireless g)#wpa-clients required                        6-123
AP(if-wireless g)#wpa-mode pre-shared-key                     7-82
AP(if-wireless g)#wpa-psk-type alphanumeric                   7-83
AP(if-wireless g)#wpa-preshared-key ASCII asecret             6-123
AP(if-wireless g)#end
AP(config)#no 802.1X                                          6-65
AP(config)#no mac-authentication                              6-72
```

CLI Commands for WPA over 802.1X Security – From the 802.11a or 802.11g interface configuration mode, use the **authentication** command to set the access point to “Open System.” Use the WEP **encryption** command to enable all types of encryption. Use the **wpa-clients** command to set WPA to be required or supported for clients. Use the **wpa-mode** command to enable WPA dynamic keys over 802.1X. Set the broadcast and multicast key encryption using the **multicast-cipher** command. Then set 802.1X to required, and disable MAC authentication. To view the current 802.11g security settings, use the **show interface wireless g** command (not shown in example).

```
AP(config)#interface wireless g                                    7-69
Enter Wireless configuration commands, one per line.
AP(if-wireless g)#authentication open                              6-119
AP(if-wireless g)#encryption 128                                   6-118
AP(if-wireless g)#wpa-clients required                             6-123
AP(if-wireless g)#wpa-mode dynamic                                 7-82
AP(if-wireless g)#multicast-cipher TKIP                            6-121
AP(if-wireless g)#end
AP(config)#802.required                                            6-65
AP(config)#no mac-authentication                                   6-72
```

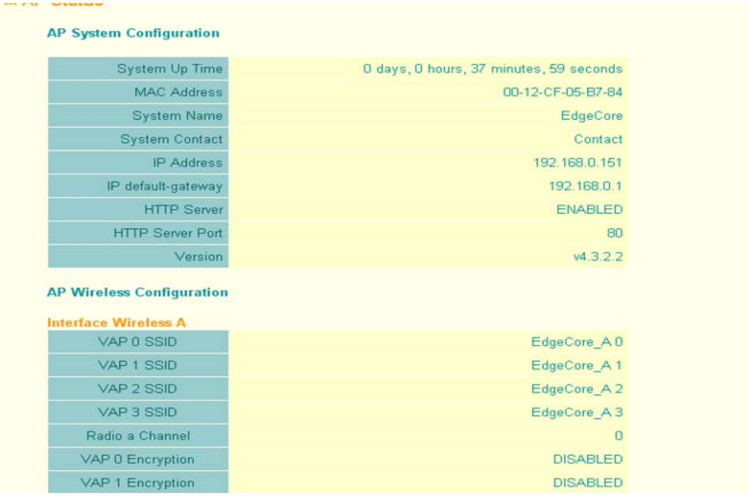
Status Information

The Status page includes information on the following items:

Menu	Description	Page
AP Status	Displays configuration settings for the basic system and the wireless interfaces	6-63
Station Status	Shows wireless clients currently associated with the access point	6-65
Event Logs	Shows log messages stored in memory	6-67

AP Status

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



AP System Configuration

System Up Time	0 days, 0 hours, 37 minutes, 59 seconds
MAC Address	00-12-CF-05-B7-84
System Name	EdgeCore
System Contact	Contact
IP Address	192.168.0.151
IP default-gateway	192.168.0.1
HTTP Server	ENABLED
HTTP Server Port	80
Version	v4.3.2.2

AP Wireless Configuration

Interface Wireless A

VAP 0 SSID	EdgeCore_A 0
VAP 1 SSID	EdgeCore_A 1
VAP 2 SSID	EdgeCore_A 2
VAP 3 SSID	EdgeCore_A 3
Radio a Channel	0
VAP 0 Encryption	DISABLED
VAP 1 Encryption	DISABLED

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

- System Up Time: Length of time the management agent has been up.
- MAC Address: The physical layer address for this device.
- System Name: Name assigned to this system.
- 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: Shows if management access via HTTP is enabled.
- HTTP Server Port: Shows the TCP port used by the HTTP interface.
- Version: Shows the version number for the runtime code.

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.

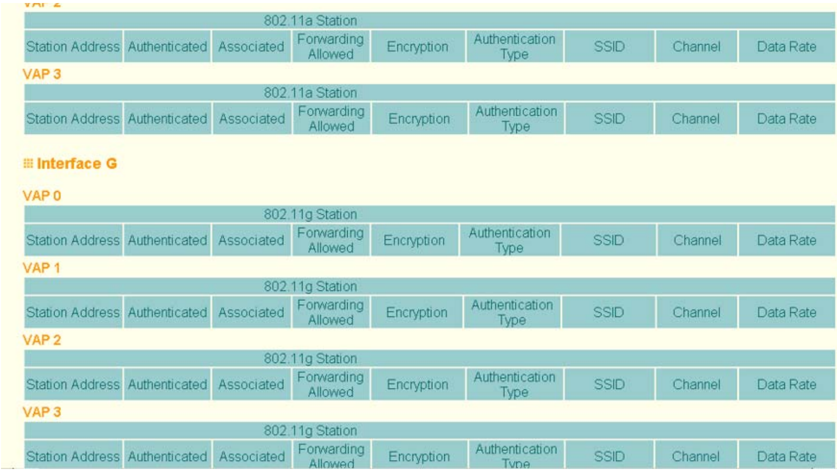
- Network Name (SSID): The service set identifier for this wireless group.
- Radio Channel: The radio channel currently used on the wireless bridge.
- Radio Encryption: The key size used for data encryption.
- Radio Authentication Type: Shows the bridge is set as an open system.
- 802.1X: Shows if IEEE 802.1X access control for wireless clients is enabled.

CLI Commands for Displaying System Settings – To view the current wireless bridge 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 6-109).

```
DUAL OUTDOOR#show system                                            6-23
System Information
============================================================
Serial Number        : .
System Up time       : 0 days, 5 hours, 2 minutes, 4 seconds
System Name          : Dual Band Outdoor AP
System Location      :
System Contact       : Contact
System Country Code  : US - UNITED STATES
MAC Address          : 00-03-7F-BE-F8-99
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     : v1.1.0.0B07
============================================================
DUAL OUTDOOR#
```

Station Status

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



802.11a Station								
Station Address	Authenticated	Associated	Forwarding Allowed	Encryption	Authentication Type	SSID	Channel	Data Rate

VAP 3

802.11a Station								
Station Address	Authenticated	Associated	Forwarding Allowed	Encryption	Authentication Type	SSID	Channel	Data Rate

Interface G

VAP 0

802.11g Station								
Station Address	Authenticated	Associated	Forwarding Allowed	Encryption	Authentication Type	SSID	Channel	Data Rate

VAP 1

802.11g Station								
Station Address	Authenticated	Associated	Forwarding Allowed	Encryption	Authentication Type	SSID	Channel	Data Rate

VAP 2

802.11g Station								
Station Address	Authenticated	Associated	Forwarding Allowed	Encryption	Authentication Type	SSID	Channel	Data Rate

VAP 3

802.11g Station								
Station Address	Authenticated	Associated	Forwarding Allowed	Encryption	Authentication Type	SSID	Channel	Data Rate

The Station Status page displays basic connection information for all associated stations. Note that this page is automatically refreshed every five seconds.

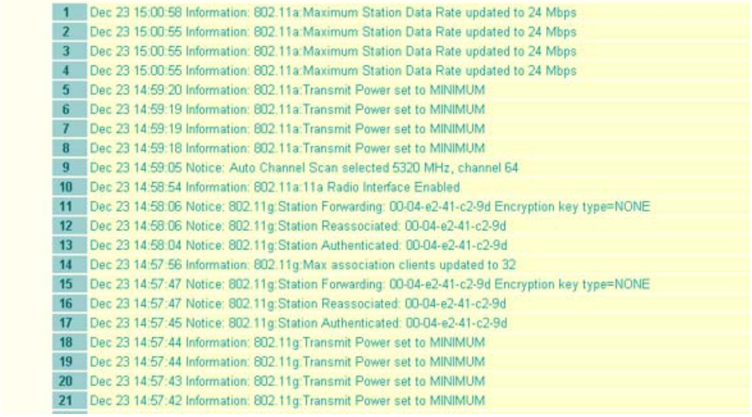
- Station Address: The MAC address of the remote wireless bridge.
- Authenticated: Shows if the station has been authenticated. The two basic methods of authentication supported for 802.11 wireless networks are “open system” and “shared key.” Open-system authentication accepts any client attempting to 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: Shows if the station has been successfully associated with the access point.
- Forwarding Allowed: Shows if the station has passed authentication and is now allowed to forward traffic.
- Key Type: Displays one of the following:
  - Disabled: The client is not using Wired Equivalent Privacy (WEP) encryption keys.
  - Dynamic: The client is using Wi-Fi Protected Access (802.1X or pre-shared key mode) or using 802.1X authentication with dynamic keying.
  - Static: The 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.

```
DUAL OUTDOOR#show station                                          6-110

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
===========================================================
DUAL OUTDOOR#
```

Event Logs

The Event Logs window shows the log messages generated by the wireless bridge and stored in memory.



```
1  Dec 23 15:00:58 Information: 802.11a:Maximum Station Data Rate updated to 24 Mbps
2  Dec 23 15:00:55 Information: 802.11a:Maximum Station Data Rate updated to 24 Mbps
3  Dec 23 15:00:55 Information: 802.11a:Maximum Station Data Rate updated to 24 Mbps
4  Dec 23 15:00:55 Information: 802.11a:Maximum Station Data Rate updated to 24 Mbps
5  Dec 23 14:59:20 Information: 802.11a:Transmit Power set to MINIMUM
6  Dec 23 14:59:19 Information: 802.11a:Transmit Power set to MINIMUM
7  Dec 23 14:59:19 Information: 802.11a:Transmit Power set to MINIMUM
8  Dec 23 14:59:18 Information: 802.11a:Transmit Power set to MINIMUM
9  Dec 23 14:59:05 Notice: Auto Channel Scan selected 5320 MHz, channel 64
10 Dec 23 14:58:54 Information: 802.11a:11a Radio Interface Enabled
11 Dec 23 14:58:06 Notice: 802.11g:Station Forwarding: 00-04-e2-41-c2-9d Encryption key type=NONE
12 Dec 23 14:58:06 Notice: 802.11g:Station Reassociated: 00-04-e2-41-c2-9d
13 Dec 23 14:58:04 Notice: 802.11g:Station Authenticated: 00-04-e2-41-c2-9d
14 Dec 23 14:57:56 Information: 802.11g:Max association clients updated to 32
15 Dec 23 14:57:47 Notice: 802.11g:Station Forwarding: 00-04-e2-41-c2-9d Encryption key type=NONE
16 Dec 23 14:57:47 Notice: 802.11g:Station Reassociated: 00-04-e2-41-c2-9d
17 Dec 23 14:57:45 Notice: 802.11g:Station Authenticated: 00-04-e2-41-c2-9d
18 Dec 23 14:57:44 Information: 802.11g:Transmit Power set to MINIMUM
19 Dec 23 14:57:44 Information: 802.11g:Transmit Power set to MINIMUM
20 Dec 23 14:57:43 Information: 802.11g:Transmit Power set to MINIMUM
21 Dec 23 14:57:42 Information: 802.11g:Transmit Power set to MINIMUM
```

The Event Logs table displays the following information:

- Log Time: The time the log message was generated.
- Event Level: The logging level associated with this message. For a description of the various levels, see “logging level” on page 6-27.
- Event Message: The content of the log message.

CLI Commands for Displaying the Event Logs – From the global configuration mode, use the **show logging** command.

```
DUAL OUTDOOR#show loggging                                          6-32

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
=============================================

DUAL OUTDOOR#
```

Chapter 7: Command Line Interface

Using the Command Line Interface

Accessing the CLI

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

Console Connection

To access the bridge through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user name is "admin" and the default password is null) When the user name is entered, the CLI displays the "Enterprise AP#" prompt.
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "exit" command.

After connecting to the system through the console port, the login screen displays:

```
Username: admin
Password:
Enterprise AP#
```

Caution: Command examples shown later in this chapter abbreviate the console prompt to "AP" for simplicity.

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 numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, if the bridge cannot acquire an IP address from a DHCP server, the default IP address used by the bridge, 192.168.1.1, consists of a network portion (192.168.1) and a host portion (1).

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

```
Enterprise AP#configure
Enterprise AP(config)#interface ethernet
Enterprise AP(if-ethernet)#ip address 10.1.0.1 255.255.255.0 10.1.0.254
Enterprise AP(if-ethernet)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the 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 will display the “Enterprise AP#” prompt to show that you are using executive access mode (i.e., Exec).
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 displays:

```
Username: admin
Password:
Enterprise AP#
```

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

Entering Commands

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 interfaces ethernet,” **show** and **interfaces** 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:

```
Enterprise AP(config)#username smith
```

Minimum Abbreviation

The CLI will accept 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 will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “configure” example, typing **con** followed by a tab will result in printing the command up to “**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 will display 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:

```
Enterprise AP#show ?
  APmanagement    Show management AP information.
  authentication  Show Authentication parameters
  bootfile        Show bootfile name
  bridge          Show bridge
  config          System snapshot for tech support
  dhcp-relay      Show DHCP Relay Configuration
  event-log       Show event log on console
  filters         Show filters
  hardware        Show hardware version
  history         Display the session history
  interface       Show interface information
  line            TTY line information
  link-integrity  Show link integrity information
  logging         Show the logging buffers
  radius          Show radius server
  rogue-ap        Show Rogue ap Stations
  snmp            Show snmp configuration
  sntp            Show sntp configuration
  station         Show 802.11 station table
  system          Show system information
  version         Show system version
Enterprise AP#show
```

The command “**show interface ?**” will display the following information:

```
Enterprise AP#show interface ?
  ethernet  Show Ethernet interface
  wireless  Show wireless interface
  <cr>
Enterprise AP#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.”

```
Enterprise AP#show s?
snmp     sntp     station  system
Enterprise AP#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 will log 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.

Using the **show history** command displays 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:

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

Exec Commands

When you open a new console session on an 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 “Enterprise AP#” for Exec mode.

```
Username: admin
Password: [system login password]
Enterprise AP#
```

Configuration Commands

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

The configuration commands are organized into four different modes:

- Global Configuration (GC) - These commands modify the system level configuration, and include commands such as **username** and **password**.
- Interface-Ethernet Configuration (IC-E) - These commands modify the Ethernet port configuration, and include command such as **dns** and **ip**.
- Interface-Wireless Configuration (IC-W) - These commands modify the wireless port configuration of global parameters for the radio, and include commands such as **channel** and **transmit-power**.
- Interface-Wireless Virtual bridge Configuration (IC-W-VAP) - These commands modify the wireless port configuration for each VAP, and include commands such as **ssid** and **authentication**.

To enter the Global Configuration mode, enter the command **configure** in Exec mode. The system prompt will change to “Enterprise AP(config)#” which gives you access privilege to all Global Configuration commands.

```
Enterprise AP#configure
Enterprise AP(config)#
```

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

```
Enterprise AP(config)#interface ethernet
Enterprise AP(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 7-1. Keystroke Commands

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 7-2. Command Groups

Command Group	Description	Page
General	Basic commands for entering configuration mode, restarting the system, or quitting the CLI	7-7
System Management	Controls user name, password, web browser management options, and a variety of other system information	7-11
System Logging	Configures system logging parameters	7-28
System Clock	Configures SNTP and system clock settings	7-33
DHCP Relay	Configures the bridge to send DHCP requests from clients to specified servers	7-38

Table 7-2. Command Groups

Command Group	Description	Page
SNMP	Configures community access strings and trap managers	7-40
Flash/File	Manages code image or bridge configuration files	7-55
RADIUS	Configures the RADIUS client used with 802.1X authentication	7-58
802.1X Authentication	Configures 802.1X authentication	7-65
MAC Address Authentication	Configures MAC address authentication	7-70
Filtering	Filters communications between wireless clients, controls access to the management interface from wireless clients, and filters traffic using specific Ethernet protocol types	7-73
WDS Bridge	Configures WDS forwarding table settings	7-77
Spanning Tree	Configures spanning tree parameters	7-83
Ethernet Interface	Configures connection parameters for the Ethernet interface	7-88
Wireless Interface	Configures radio interface settings	7-93
Wireless Security	Configures radio interface security and encryption settings	7-113
Rogue AP Detection	Configures settings for the detection of rogue bridges in the network	7-113
Link Integrity	Configures a link check to a host device on the wired network	7-127
IAPP	Enables roaming between multi-vendor bridges	7-131
VLANs	Configures VLAN membership	7-132
WMM	Configures WMM quality of service parameters	7-134

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

General Commands

Table 7-3. General Commands

Command	Function	Mode	Page
configure	Activates global configuration mode	Exec	7-8
end	Returns to previous configuration mode	GC, IC	7-8
exit	Returns to the previous configuration mode, or exits the CLI	any	7-8
ping	Sends ICMP echo request packets to another node on the network	Exec	7-9
reset	Restarts the system	Exec	7-10
show history	Shows the command history buffer	Exec	7-10
show line	Shows the configuration settings for the console port	Exec	7-11

configure

This command activates Global Configuration mode. You must enter this mode to modify most of the settings on the 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 1.

Default Setting

None

Command Mode

Exec

Example

```
Enterprise AP#configure
Enterprise AP(config)#
```

Related Commands

end (7-8)

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:

```
Enterprise AP(if-ethernet)#end
Enterprise AP(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:

```
Enterprise AP(if-ethernet)#exit
Enterprise AP#exit
CLI session with the 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

```
Enterprise AP#ping 10.1.0.19
192.168.1.19 is alive
Enterprise AP#
```

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 will always run the Power-On Self-Test.

Example

This example shows how to reset the system:

```
Enterprise AP#reset board
Reboot system now? <y/n>: y
```

show history

This command shows the contents of the command history buffer.

Default Setting

None

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

In this example, the show history command lists the contents of the command history buffer:

```
Enterprise AP#show history
 config
 exit
 show history
Enterprise AP#
```

show line

This command displays the console port’s configuration settings.

Command Mode

Exec

Example

The console port settings are fixed at the values shown below.

```
Enterprise AP#show line
Console Line Information
======================================================
  databits   : 8
  parity     : none
  speed      : 9600
  stop bits  : 1
======================================================
Enterprise AP#
```

System Management Commands

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

Table 7-4. System Management Commands

Command	Function	Mode	Page
Country Setting			
country	Sets the bridge country code	Exec	7-12
Device Designation			
prompt	Customizes the command line prompt	GC	7-14
system name	Specifies the host name for the bridge	GC	7-14
snmp-server contact	Sets the system contact string	GC	7-41
snmp-server location	Sets the system location string	GC	7-42
Management Access			
username	Configures the user name for management access	GC	7-15
password	Specifies the password for management access	GC	7-15
ip ssh-server enable	Enables the Secure Shell server	IC-E	7-16
ip ssh-server port	Sets the Secure Shell port	IC-E	7-16
ip telnet-server enable	Enables the Telnet server	IC-E	7-17
APmgmtIP	Specifies an IP address or range of addresses allowed access to the management interface	GC	7-21
APmgmtUI	Enables or disables SNMP, Telnet or web management access	GC	7-22
show APmanagement	Shows the AP management configuration	Exec	7-22

Table 7-4. System Management Commands			
Command	Function	Mode	Page
Web Server			
ip http port	Specifies the port to be used by the web browser interface	GC	7-17
ip http server	Allows the bridge to be monitored or configured from a browser	GC	7-18
ip https port	Specifies the UDP port number used for a secure HTTP connection to the bridge's Web interface	GC	7-18
ip https server	Enables the secure HTTP server on the bridge	GC	7-19
web-redirect	Enables web authentication of clients using a public access Internet service	GC	7-20
System Status			
show system	Displays system information	Exec	7-23
show version	Displays version information for the system	Exec	7-24
show config	Displays detailed configuration information for the system	Exec	7-24
show hardware	Displays the bridge's hardware version	Exec	7-28

country

This command configures the 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 7-5. Country 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
Austria	AT	France	FR	Macao	MO	Spain	ES
Azerbaijan	AZ	Georgia	GE	Macedonia	MK	Sweden	SE
Bahrain	BH	Germany	DE	Malaysia	MY	Switzerland	CH

Table 7-5. Country Codes

Country	Code	Country	Code	Country	Code	Country	Code
Belarus	BY	Greece	GR	Malta	MT	Syria	SY
Belgium	BE	Guatemala	GT	Mexico	MX	Taiwan	TW
		Honduras	HN	Monaco	MC	Thailand	TH
Belize	BZ	Hong Kong	HK	Morocco	MA	Trinidad & Tobago	TT
Bolivia	BO	Hungary	HU	Netherlands	NL	Tunisia	TN
Brazil	BR	Iceland	IS	New Zealand	NZ	Turkey	TR
Brunei Darussalam	BN	India	IN	Norway	NO	Ukraine	UA
Bulgaria	BG	Indonesia	ID	Qatar	QA	United Arab Emirates	AE
Canada	CA	Iran	IR	Oman	OM	United Kingdom	GB
Chile	CL	Ireland	IE	Pakistan	PK	United States	US
China	CN	Israel	IL	Panama	PA	Uruguay	UY
Colombia	CO	Italy	IT	Peru	PE	Uzbekistan	UZ
Costa Rica	CR	Japan	JP	Philippines	PH	Yemen	YE
Croatia	HR	Jordan	JO	Poland	PL	Venezuela	VE
Cyprus	CY	Kazakhstan	KZ	Portugal	PT	Vietnam	VN
Czech Republic	CZ	North Korea	KP	Puerto Rico	PR	Zimbabwe	ZW
Denmark	DK	Korea Republic	KR	Slovenia	SI		
Elsalvador	SV	Luxembourg	LU	South Africa	ZA		

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 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

```
Enterprise AP#country tw
Enterprise AP#
```

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: 32 characters)

Default Setting

Enterprise AP

Command Mode

Global Configuration

Example

```
Enterprise AP(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

Enterprise AP

Command Mode

Global Configuration

Example

```
Enterprise AP(config)#system name AP
Enterprise AP(config)#
```

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

```
Enterprise AP(config)#username bob
Enterprise AP(config)#
```

password

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

```
Enterprise AP(config)#password
Enterprise AP(config)#
```

ip ssh-server enable

This command enables the Secure Shell 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 bridge 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. The **show system** command displays the status of the SSH server.

Example

```
Enterprise AP(if-ethernet)#ip ssh-server enable
Enterprise AP(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

```
Enterprise AP(if-ethernet)#ip ssh-server port 1124
Enterprise AP(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

```
Enterprise AP(if-ethernet)#ip telnet-server enable
Enterprise AP(if-ethernet)#
```

ip http port

This command specifies the TCP port number used by the web browser 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

```
Enterprise AP(config)#ip http port 769
Enterprise AP(config)#
```

Related Commands

ip http server (7-18)

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

```
Enterprise AP(config)#ip http server
Enterprise AP(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 bridge’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

```
Enterprise AP(config)#ip https port 1234
Enterprise AP(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 bridge’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

```
Enterprise AP(config)#ip https server
Enterprise AP(config)#
```

web-redirect

Use this command to enable web-based authentication of clients. Use the **no** form to disable this function.

Syntax

[**no**] **web-redirect**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The web redirect feature is used to support billing for a public access wireless network. After successful association to an bridge, a client is “redirected” to an bridge login web page as soon as Internet access is attempted. The client is then authenticated by entering a user name and password on the web page. This process allows controlled access for clients without requiring 802.1X or MAC authentication.
- Web redirect requires a RADIUS server on the wired network with configured user names and passwords for authentication. The RADIUS server details must also be configured on the bridge. (See “show bootfile” on page 7-58.)
- Use the **show system** command to display the current web redirect status.

Example

```
Enterprise AP(config)#web-redirect
Enterprise AP(config)#
```

APmgmtIP

This command specifies the client IP addresses that are allowed management access to the bridge through various protocols.

Caution: 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** - Adds IP addresses within a specifiable range to the SNMP, web and Telnet groups.
- **single** - Adds an IP address to the SNMP, web and Telnet groups.
- **any -** Allows any IP address access through SNMP, web and Telnet groups.
- *IP_address* - Adds 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 bridge 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 bridge will not accept overlapping address ranges. When entering addresses for different groups, the bridge 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.

```
Enterprise AP(config)#apmgmtip multiple 192.168.1.50 255.255.255.0
Enterprise AP(config)#
```

APmgmtUI

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

Caution: 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.

```
Enterprise AP(config)#apmgmtui SNMP enable
Enterprise AP(config)#
```

show apmanagement

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

Command Mode

Exec

Example

```
Enterprise AP#show apmanagement
Management AP Information
=================================
AP Management IP Mode: Any IP
Telnet UI: Enable
WEB UI   : Enable
SNMP UI  : Enable
==================================
Enterprise AP#
```

show system

This command displays basic system configuration settings.

Default Setting

None

Command Mode

Exec

Example

```
Enterprise AP#show system
System Information
==========================================================
Serial Number         : A123456789
System Up time        : 0 days, 4 hours, 33 minutes, 29 seconds
System Name           : Enterprise Wireless AP
System Location       :
System Contact        : David
System Country Code   : US - UNITED STATES
MAC Address           : 00-30-F1-F0-9A-9C
IP Address            : 192.168.1.1
Subnet Mask           : 255.255.255.0
Default Gateway       : 0.0.0.0
VLAN State            : DISABLED
Management VLAN ID(AP): 1
IAPP State            : ENABLED
DHCP Client           : ENABLED
HTTP Server           : ENABLED
HTTP Server Port      : 80
HTTPS Server          : ENABLED
HTTPS Server Port     : 443
Slot Status           : Dual band(a/g)
Boot Rom Version      : v1.1.8
Software Version      : v4.3.2.8b03
SSH Server            : ENABLED
SSH Server Port       : 22
Telnet Server         : ENABLED
WEB Redirect          : DISABLED
DHCP Relay            : DISABLED
Proxy ARP             : DISABLED
==========================================================
Enterprise AP#
```

show version

This command displays the software version for the system.

Command Mode

Exec

Example

```
Enterprise AP#show version

Version Information
=========================================
Version: v4.3.2.8b03
Date   : Dec 20 2005, 18:38:12
=========================================
Enterprise AP#
```

show config

This command displays detailed configuration information for the system.

Command Mode

Exec

Example

```
Enterprise AP#show config

Authentication Information
===========================================================
MAC Authentication Server      : DISABLED
MAC Auth Session Timeout Value : 0 min
802.1x supplicant              : DISABLED
802.1x supplicant user         : EMPTY
802.1x supplicant password     : EMPTY
Address Filtering              : ALLOWED

System Default : ALLOW addresses not found in filter table.
Filter Table
-----------------------------------------------------------
No Filter Entries.

Bootfile Information
===================================
Bootfile : ec-img.bin
===================================

Protocol Filter Information
===========================================================
Local Bridge         :DISABLED
AP Management        :ENABLED
Ethernet Type Filter :DISABLED

Enabled Protocol Filters
-----------------------------------------------------------
No protocol filters are enabled
===========================================================
Hardware Version Information
===========================================
Hardware version R01A
===========================================

Ethernet Interface Information
========================================
IP Address          : 192.168.0.151
Subnet Mask         : 255.255.255.0
Default Gateway     : 192.168.0.1
Primary DNS         : 210.200.211.225
Secondary DNS       : 210.200.211.193
Speed-duplex        : 100Base-TX Full Duplex
Admin status        : Up
Operational status  : Up
========================================

Wireless Interface 802.11a Information
===========================================================
----------------Identification-----------------------------
Description                : Enterprise 802.11a bridge
SSID                       : VAP_TEST_11A 0
Channel                    : 0 (AUTO)
Status                     : Disable
----------------802.11 Parameters--------------------------
Transmit Power             : 100% (5 dBm)
Data Rate                  : 54Mbps
Fragmentation Threshold    : 2346 bytes
RTS Threshold              : 2347 bytes
Beacon Interval            : 100 TUs
DTIM Interval              : 1 beacon
Maximum Association        : 64 stations
Native VLAN ID             : 1
----------------Security-----------------------------------
Closed System              : DISABLED
Multicast cipher                : WEP
Unicast cipher                  : TKIP and AES
WPA clients                : REQUIRED
WPA Key Mgmt Mode          : PRE SHARED KEY
WPA PSK Key Type           : ALPHANUMERIC
Encryption                 : DISABLED
Default Transmit Key       : 1
Static Keys :
   Key 1: EMPTY     Key 2: EMPTY     Key 3: EMPTY     Key 4: EMPTY
Key Length :
   Key 1: ZERO      Key 2: ZERO      Key 3: ZERO      Key 4: ZERO
Authentication Type        : OPEN
Rogue AP Detection         : Disabled
Rogue AP Scan Interval     : 720 minutes
Rogue AP Scan Duration     : 350 milliseconds
===========================================================

Console Line Information
===========================================================
  databits   : 8
  parity     : none
  speed      : 9600
  stop bits  : 1
===========================================================
Logging Information
=====================================================
Syslog State               : Disabled
Logging Console State      : Disabled
Logging Level              : Informational
Logging Facility Type      : 16
Servers
   1: 0.0.0.0        , UDP Port:  514, State: Disabled
   2: 0.0.0.0        , UDP Port:  514, State: Disabled
   3: 0.0.0.0        , UDP Port:  514, State: Disabled
   4: 0.0.0.0        , UDP Port:  514, State: Disabled
======================================================

   Radius Server Information
========================================
IP                 : 0.0.0.0
Port               : 1812
Key                : *****
Retransmit         : 3
Timeout            : 5
Radius MAC format  : no-delimiter
Radius VLAN format : HEX
========================================

Radius Secondary Server Information
========================================
IP                 : 0.0.0.0
Port               : 1812
Key                : *****
Retransmit         : 3
Timeout            : 5
Radius MAC format  : no-delimiter
Radius VLAN format : HEX
========================================

SNMP Information
==============================================
Service State                 : Disable
Community (ro)                : ********
Community (rw)                : ********
Location                      :
Contact                       : Contact


EngineId   :80:00:07:e5:80:00:00:29:f6:00:00:00:0c
EngineBoots:2

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
```

```
      dot11InterfaceAGFail  Enabled         dot11InterfaceBFail  Enabled
   dot11StationAssociation  Enabled  dot11StationAuthentication  Enabled
 dot11StationReAssociation  Enabled     dot11StationRequestFail  Enabled
             dot1xAuthFail  Enabled       dot1xAuthNotInitiated  Enabled
          dot1xAuthSuccess  Enabled        dot1xMacAddrAuthFail  Enabled
   dot1xMacAddrAuthSuccess  Enabled         iappContextDataSent  Enabled
     iappStationRoamedFrom  Enabled         iappStationRoamedTo  Enabled
      localMacAddrAuthFail  Enabled     localMacAddrAuthSuccess  Enabled
              pppLogonFail  Enabled              sntpServerFail  Enabled
  configFileVersionChanged  Enabled         radiusServerChanged  Enabled
                systemDown  Enabled                    systemUp  Enabled

============================================

SNTP Information
==========================================================
Service State        : Disabled
SNTP (server 1) IP   : 137.92.140.80
SNTP (server 2) IP   : 192.43.244.18
Current Time         : 00 : 14, Jan 1st, 1970
Time Zone            : -5 (BOGOTA, EASTERN, INDIANA)
Daylight Saving      : Disabled
==========================================================


Station Table Information
==========================================================
if-wireless A VAP [0]   :
802.11a Channel : Auto

No 802.11a Channel Stations.
:
if-wireless G VAP [0]   :
802.11g Channel : Auto

No 802.11g Channel Stations.
:
System Information
=============================================================
Serial Number         :
System Up time        : 0 days, 0 hours, 16 minutes, 51 seconds
System Name           : Enterprise Wireless AP
System Location       :
System Contact        : David
System Country Code   : 99 - NO_COUNTRY_SET
MAC Address           : 00-12-CF-05-B7-84
IP Address            : 192.168.0.151
Subnet Mask           : 255.255.255.0
Default Gateway       : 192.168.0.1
VLAN State            : DISABLED
Management VLAN ID(AP): 1
IAPP State            : ENABLED
DHCP Client           : ENABLED
HTTP Server           : ENABLED
HTTP Server Port      : 80
HTTPS Server          : ENABLED
HTTPS Server Port     : 443
Slot Status           : Dual band(a/g)
Boot Rom Version      : v1.1.8
Software Version      : v4.3.2.8b03
```

```
SSH Server            : ENABLED
SSH Server Port       : 22
Telnet Server         : ENABLED
WEB Redirect          : DISABLED
DHCP Relay            : DISABLED
==============================================================

Version Information
=========================================
Version: v4.3.2.2
Date   : Dec 20 2005, 18:38:12
=========================================
Enterprise AP#
```

show hardware

This command displays the hardware version of the system.

Command Mode

Exec

Example

```
Enterprise AP#show hardware

Hardware Version Information
===========================================
Hardware version R01
===========================================
Enterprise AP#
```

System Logging Commands

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

Table 7-6. System Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	7-29
logging host	Adds a syslog server host IP address that will receive logging messages	GC	7-29
logging console	Initiates logging of error messages to the console	GC	7-30
logging level	Defines the minimum severity level for event logging	GC	7-30
logging facility-type	Sets the facility type for remote logging of syslog messages	GC	7-31
logging clear	Clears all log entries in bridge memory	GC	7-32
show logging	Displays the state of logging	Exec	7-32
show event-log	Displays all log entries in bridge memory	Exec	7-33

logging on

This command controls logging of error messages; i.e., sending debug or error messages to memory. The **no** form disables the logging process.

Syntax

[**no**] **logging on**

Default Setting

Disabled

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

```
Enterprise AP(config)#logging on
Enterprise AP(config)#
```

logging host

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

Syntax

logging host <**1** | **2** | **3** | **4**> <*host_name* | *host_ip_address*> [*udp_port*]
no logging host <**1** | **2** | **3** | **4**>

- **1** - First syslog server.
- **2** - Second syslog server.
- **3** - Third syslog server.
- **4** - Fourth syslog server.
- *host_name* - The name of a syslog server. (Range: 1-20 characters)
- *host_ip_address* - The IP address of a syslog server.
- *udp_port* - The UDP port used by the syslog server.

Default Setting

None

Command Mode

Global Configuration

Example

```
Enterprise AP(config)#logging host 1 10.1.0.3
Enterprise AP(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

```
Enterprise AP(config)#logging console
Enterprise AP(config)#
```

logging level

This command sets the minimum severity level for event logging.

Syntax

logging level <Emergency | **Alert** | **Critical** | **Error** | **Warning** | **Notice** | **Informational** | **Debug>**

Default Setting

Informational

Command Mode

Global Configuration