

BreezeNET PRO.11 Series

Outdoor Bridge User's Guide

(for models using AMP2440-250/500)

June, 2001

Cat. No. 213034

Revision

2

Disclaimer: The diagrams in this manual are for illustrative purposes only. They should not be confused with the transceiver operating in a standalone mode. When these diagrams are in use, the transceiver will be installed in conjunction with amp model AMP-2440-250/500 and the antennas listed in Table 1.

© 1999 by BreezeCOM Ltd. All rights reserved.

No part of this publication may be reproduced in any material form without the written permission of the copyright owner.

Trade Names

BreezeNET and BreezeLINK are trade names of BreezeCOM Ltd. Other brand and product names are registered trademarks or trademarks of their respective companies.

Statement of Conditions

The information contained in this manual is subject to change without notice. BreezeCOM Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranty

In the following warranty text, "the Company" shall mean:

- BreezeCOM Inc., for products located in the USA.
- BreezeCOM Ltd., for products located outside the USA.

This BreezeNET product is warranted against defects in material and workmanship for a period of one year. During this warranty period the Company will, at its option, either repair or replace products that prove to be defective.

For warranty service or repair, the product must be returned to a service facility designated by the Company. Authorization to return products must be obtained prior to shipment. The buyer shall pay all shipping charges to the Company and the Company shall pay shipping charges to return the product to the buyer.

The Company warrants that the firmware designed by it for use with the unit will execute its programming instructions when properly installed on the unit. The Company does not warrant that the operation of the unit or firmware will be uninterrupted or error-free.

Limitation of Warranty

The foregoing warranty shall not apply to defects resulting from improper or inadequate maintenance by the buyer, buyer supplied interfacing, unauthorized modification or misuse, operation outside of the environmental specifications for the product, or improper site preparation or maintenance. No other warranty is expressed or implied. The Company specifically disclaims the implied warranties of merchantability and fitness for any particular purpose.

Electronic Emission Notices

This device complies with Part 15 of the FCC rules, ETSI 300-328, UL, UL/C, TUV/GS, and CE.

Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment when installed as directed. This equipment should be installed and operated with the minimum distance between any persons body and the antenna as shown below:

Antenna Type	Gain (dBi)	Gain Numeric	Amp Peak output Power (mW)	Minimum RF Exposure Separation Distance (cm)
Uni 24	24	251.2	250	70.7
Uni 21	21	125.9	250	50.1
Uni 18	18	63.1	250	35.4
Uni 16	16	39.8	250	28.1
Uni 16	16	39.8	500	39.8
Uni 13	13	20.0	500	28.2
Omni 12	12	15.8	250	20.0
Omni 8	8	6.3	500	20.0
Omni 6	6	4.0	500	20.0

WARNING: It is the responsibility of the professional installer to ensure that when using the outdoor antenna kits in the United States (or where FCC rules apply), only these antenna configurations shown in the table in section 1.4 are used. The use of any antenna other than those listed is expressly forbidden in accordance to FCC rules CFR47 part 15.204.

Information to User

Any changes or modifications of equipment not expressly approved by the manufacturer could void the user's authority to operate the equipment and the company's warranty.

CONTACTING BREEZECOM TECHNICAL SUPPORT

Should you need assistance beyond the scope of this guide, please contact your local BreezeCOM reseller or distributor. If they cannot solve your problem, feel free to contact the BreezeCOM Technical Support Department. The support representatives can assist you in solving any problems that cannot be solved by your reseller.

When requesting support, please have the following items available:

- Configuration of the system, including models of the BreezeCOM equipment used.
- Antenna type and cable lengths.
- Site information such as, possible radio path problems (trees, machines, and buildings).
- Distance between devices.
- Configuration, statistic counters, and error messages, as seen on the monitor.
- Description of problems encountered.

To contact BreezeCOM Technical Support, refer to the Technical Support page of the BreezeCOM website: www.breezecom.com

TABLE OF CONTENTS

1. Introduction To The BreezeNET PRO.11 Series.....	1-4
1.1. How to Use This Guide	1-4
1.2. BreezeNET PRO.11 Series Features	1-5
1.3.1. Access Point.....	1-6
1.3.4. Workgroup Bridge	1-7
1.4. BreezeNET PRO.11 Functional Description.....	1-9
2. Basic Installation.....	2-1
2.1. Basic Installation Checklist	2-1
2.2. Check the Package List.....	2-1
2.3. Position the Unit	2-2
2.3.1. Additional Considerations When Positioning the Access Point...	2-3
2.4. Connect the Unit to the Power Supply	2-3
2.5. Connect the Unit to the Ethernet Port.....	2-4
2.6. Check Unit Functionality using LED indicators	2-5
2.6.1. Station (SA-10, SA-40) and Bridge (WB-10) LEDs	2-5
2.6.2. Access Point LEDs	2-6
2.6.3. Verifying the Ethernet Connection.....	2-6
3. Device Setup and Management	3-1
3.1. Accessing and Using Local Terminal Management.....	3-1
3.2. Configuration Screens	3-2
3.3. Main Menu	3-4
3.4. System Configuration Menu.....	3-5
3.4.1. Station Status	3-5
3.4.2. IP and SNMP Parameters	3-6
3.4.3. Wireless LAN (WLAN) Parameters.....	3-7
3.4.4. Bridging	3-9
3.4.5. Station Control.....	3-10
3.4.6. Security	3-11
3.5. Advanced Settings Menu.....	3-12
3.5.1. Translation Mode (read-only).....	3-13
3.5.2. Roaming (read-only).....	3-13
3.5.3. Performance	3-13
3.5.4. Radio.....	3-15
3.5.5. Rate	3-16
3.5.6. AP Redundancy Support (read-only).....	3-16
3.5.7. Maintenance.....	3-16
3.6. Site Survey Menu	3-17

3.6.1.	System Counters	3-18
3.6.2.	Survey Software.....	3-22
3.6.3.	Event Log.....	3-22
3.6.4.	Display Neighboring AP's.....	3-22
3.6.5.	Using the Site Survey Software.....	3-23
3.6.6.	Using the Rx Packets per Frequency Histogram	3-26
3.7.	Access Control Menu	3-27
4.	Planning and Installing Wireless LANs	5-2
4.1.	System Configurations	5-2
4.1.1.	Single Cell Configuration.....	5-3
4.1.2.	Overlapping Cell Configuration	5-7
4.1.3.	Multicell Configuration	5-9
4.1.4.	Multi-hop Configuration (Relay).....	5-11
4.3.	Outdoor Installation Considerations.....	5-13
4.3.1.	Site Selection Factors	5-13
4.3.2.	Rooftop Installation	5-14
4.3.3.	Antennas for Outdoor Applications.....	5-14
4.3.4.	Antenna Seal.....	5-16
4.3.5.	Cell Size.....	5-16
4.3.6.	Link Distance.....	5-17
4.3.7.	Using Outdoor Range Tables.....	5-17
4.5.	Precautions.....	5-18
4.5.1.	Professional Installers Only	5-18
4.5.2.	Transmit Antenna Gain.....	5-18
4.5.3.	Spurious Radio Frequency Emissions	5-18
4.5.4.	Lightning Protection	5-19
4.5.5.	Rain Proofing.....	5-19
6.	Upgrade Procedure	6-1
7.	System Troubleshooting.....	7-1
7.1.	Troubleshooting Guide.....	7-1
7.2.	Checking Counters	7-3
7.2.1.	WLAN Counters.....	7-3
7.2.2.	Ethernet Counters	7-3
8.	Appendix	
8.1.	Supported MIBs and Traps.....	9-1
8.1.1.	Supported MIBs.....	9-1
8.1.2.	Supported Traps.....	9-2

8.2. Technical Specifications.....	9-3
8.2.1. Specifications for BreezeNET PRO.11 Units.....	9-3
8.2.5. Specifications for AL 1 Lightning Arrestor.....	9-5
8.3. Wireless LAN Concepts.....	9-6
8.4. Radio Signal Propagation.....	9-12
8.4.1. Introduction.....	9-12
8.4.2. RF Terms and Definitions.....	9-13
8.5. IEEE 802.11 Technical Tutorial.....	9-20
8.5.1. Architecture Components.....	9-20
8.5.2. IEEE 802.11 Layers Description.....	9-21
8.5.3. The MAC Layer.....	9-22
8.5.4. How Does a Station Join an Existing Cell (BSS)?.....	9-28
8.5.5. Roaming.....	9-28
8.5.6. Keeping Synchronization.....	9-29
8.5.7. Security.....	9-29
8.5.8. Power Saving.....	9-30
8.5.9. Frame Types.....	9-31
8.5.10. Frame Formats.....	9-31
8.5.11. Most Common Frame Formats.....	9-36
8.5.12. Point Coordination Function (PCF).....	9-38
8.5.13. Ad-hoc Networks.....	9-38

1. INTRODUCTION TO THE BREEZENET PRO.11 SERIES

This chapter explains how to use this guide, presents the members of the **BreezeNET PRO.11 Series**, describes the benefits of **BreezeNET PRO.11** Wireless LANs, and lists the product specifications.

1.1. How to Use This Guide

This User's Guide contains instructions for overall planning and setting up your wireless LAN, and provides details of how to install each unit, and how to install antennas and accessories.

This guide contains the following chapters:

- **Chapter 1 Introduction** – Explains how to use this guide and presents the members of the **BreezeNET PRO.11 Series**.
- **Chapter 2 Basic Installation** – Details how to install most **BreezeNET PRO.11 Series** units.
- **Chapter 3 Device Setup and Management** – Describes how to use the local terminal to setup, configure, and manage **BreezeNET PRO.11 Series** units.
- **Chapter 4 Planning and Installing Wireless LANs** – Provides guidelines and restrictions regarding antenna selection and installation, and includes outdoor antenna range tables.
- **Chapter 6 Upgrade Procedure** – Explains how to perform future upgrades for **BreezeNET PRO.11 Series** units using a TFTP application.
- **Chapter 7 System Troubleshooting** – Contains a troubleshooting guide that provides answers to some of the more common problems which may occur when installing and using **BreezeNET PRO.11 Series** products.
- **Chapter 8 Appendix** – This appendix lists MIBs, and traps supported by **BreezeNET PRO.11 Series** products, lists product and attachment specifications, provides an overview of the concepts related to wireless LANs, discusses the concepts and applications of radio signal propagation relevant to wireless LANs, and introduces the new 802.11 standard.

1.2. BreezeNET PRO.11 Series Features

Following is a partial list of the features in the **BreezeNET PRO.11 Series**:

- **IEEE 802.11 Compliant** – All **BreezeNET PRO.11 Series** units are fully compliant with the final IEEE 802.11 specification for wireless LANs, and thus support interoperability with other 802.11 compliant vendors.
- **Fully integrated product family** – One high-performance Access Point for all products in the series.
- **Increased Throughput** – Up to 2 Mbps data throughput; the best figure in the market!
- **Translation Bridging** – Support for both translation and transparent bridging as defined in the IEEE 802.1.h and RFC 1042 standards.
- **Seamless Roaming** – Network connection is maintained while roaming between overlapping coverage areas. Transmission and reception can be continued while moving at high speeds with no data packet loss or duplication.
- **Load Sharing** – Traffic is equally distributed among all Access Points in the area.
- **Redundancy** – In co-located cell environments, upon failure of an Access Point, stations will switch to other available Access Points.
- **LED Display** – Power, Network Activity, and WLAN Load or Signal Quality LEDs indicate the current status of the unit.
- **Upgrading** – Simple, quick, and free software upgrades via TFTP.
- **Future-proof Investment** – All “infrastructure” items in the PRO.11 Series line offer Flash updates.

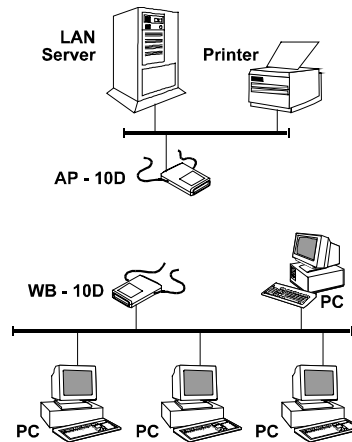
1.2.1. Access Point

The Access Point is fully compliant with the IEEE 802.11 wireless LAN standard.

The **BreezeNET** Access Point is a wireless hub that provides access for wireless workstations into wired Ethernet LANs. It also contains a wireless coordinating function which enables workstations equipped with a Station Adapter (Station Adapter, Bridge) to communicate with one another inside the cell coverage area (even if they are not in direct line of sight) via the Access Point. Any two wireless stations in two different cells can communicate through their Access Points.

Disclaimer: This diagram is for illustrative purposes only. It should not be confused with the transceiver operating in a standalone mode.

When this diagram is in use, the transceiver will be used in conjunction with amp model AMP-2440-250/500 and the antennas listed in this manual.



Mobile workstations, such as laptops and hand-held devices, can *roam* between Access Points that belong to the same Extended Service Set (ESS). In an Extended Service Set, all Access Points have the same ESSID. When the access points are set up so that their coverage areas overlap, users can roam seamlessly from cell to cell. This means that there is no interruption of network connection when moving from one coverage area to the other through the overlap and is completely transparent to the user and the applications. The Station Adapters decide when a mobile user becomes disassociated from one access point and associated with another. This process is fully transparent, requires no user intervention and involves no loss of data packets.

Position multiple access points in locations where heavy network traffic is expected to create a multicell and increase the aggregate throughput capacity in areas where it is needed most. The system implements a Load

Balancing algorithm to divide the stations equally between the available co-located Access Points.

The **BreezeNET** Access Point contains an embedded SNMP agent enabling effective management by BreezeVIEW or any standard SNMP management station. Software upgrades can be downloaded by TFTP protocol via the wired LAN or wireless LAN.

1.2.2. Workgroup Bridge

The **BreezeNET** Workgroup Bridge is a high-speed, wide-range wireless LAN bridge that provides connectivity to remote Ethernet networks.

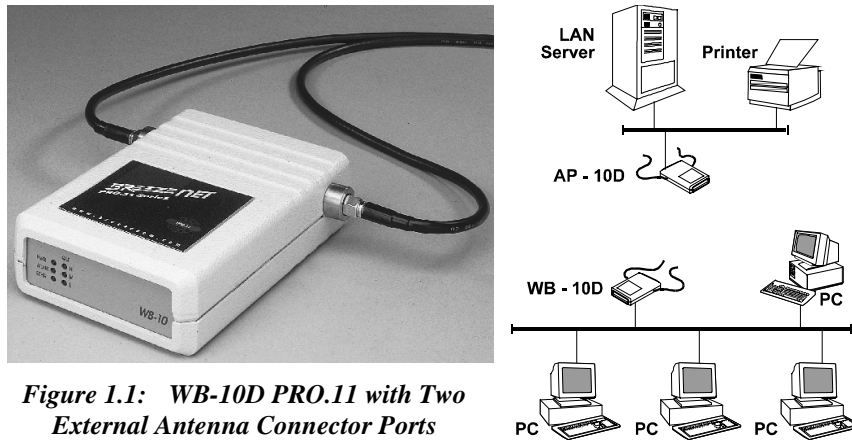


Figure 1.1: WB-10D PRO.11 with Two External Antenna Connector Ports

Disclaimer: This diagram is for illustrative purposes only. It should not be confused with the transceiver operating in a standalone mode. When this diagram is in use, the transceiver will be used in conjunction with amp model AMP-2440-250/500 and the antennas listed in this manual.

The Workgroup Bridge communicates with the **BreezeNET** Access Points of the remote LANs effectively creating an extended wireless network spanning sites situated up to 6 miles apart (in Europe this range is limited by ETSI regulations to 2.5 Km.). In this way a central Ethernet LAN may be connected with one or more branch office LANs.

In addition, an *island* consisting of a Workgroup Bridge together with an Access Point can work as a relay. Transmissions from the central LAN and from the remote LAN are relayed via the island located between them. This configuration effectively doubles bridge range.

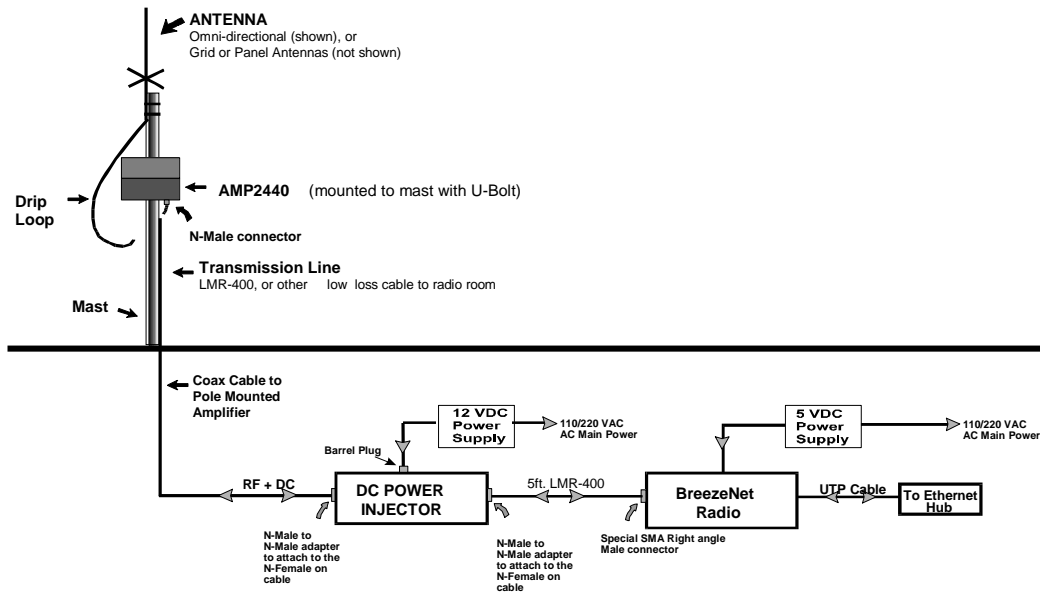
Workstations that can be connected to the wireless LAN include PCs, X-Terminals, Digital, SUN, HP, IBM, and Apple computers, and any other device that supports Ethernet. The unit is transparent to the workgroup devices' hardware, software, and network operating system.

The **BreezeNET** Workgroup Bridge contains an embedded SNMP agent and software downloading capabilities enabling effective management. Software upgrades are downloaded using TFTP protocol via the Ethernet ports or via the wireless LAN and Access Point.

1.3. Extending Range with the AMP2440

To extend the range of the AP10-D or WB-10D, the AMP2440-250 or AMP2440-500 is used. These devices amplify the RF output and receive power to allow long range connections or connections with longer cable runs. The diagram below shows a typical installation of the BreezeNet and AMP2440. (See the addendum at the end of this manual for instructions on how to install the AMP2440).

BREEZECOM AMPLIFIER INSTALLATION DETAILS



* Filter is required in the United States when the 24dB grid dish antenna is used in order to comply with FCC emission requirements.

1.4. Antenna Selection

The AMP2440 and the BreezeNET radio modem must be professionally installed. Table (1) shows the FCC approved configuration of the AMP2440, BreezeNET Radio and antenna configurations.

WARNING: It is the responsibility of the installer to ensure that when used in the United States (or where FCC rules apply), only these configurations are used. The use of any antenna other than those listed below is expressly forbidden in accordance to FCC rules CFR47 part 15.204.

1.4.1.1 Table (1) FCC Type Acceptance Configurations

Radio Equipment	UNI-24 24 dBi Grid	UNI-21 21 dBi Grid	UNI-18 18 dBi Grid	UNI-16 16 dBi Panel	UNI-13 13 dBi Panel	Omni-12 12 dBi Omni	Omni-8 8 dBi Omni	Omni-6 6 dBi Omni
BreezeNET PRO.11 with Amp2440-250	X	X	X	X		X		
BreezeNET PRO.11 with Amp2440-500				X	X		X	X

*: External filter (P/N: SPF-1) is required in the United States with the 24dBi grid antenna to comply with FCC spurious emission requirements. Install this between the amplifier and the antenna.

1.5. BreezeNET PRO.11 Functional Description

BreezeNET PRO.11 units add wireless functionality to existing Ethernet LANs.

1.5.1. Quick Review of Ethernet

Standard Ethernet LAN stations are wired to a common bus. When one of the stations sends a message, it assigns a destination address to the message and sends the message on the bus. All stations on the bus “hear” the message, but only the station with the proper address processes the message.

1.5.2. Startup Procedure

When wireless units (other than AP-10) start up, they scan the frequencies for an AP-10. If an active AP-10 is in range, the units synchronize with it. The addresses associated with the units are registered in the AP-10 (the registration process is different for each unit type). From then on, the units can send and receive messages to and from the wired LAN.

1.5.3. AP-10 Access Point

The AP-10 Access Point is connected to a wired Ethernet LAN, and it keeps a list of known stations on its wireless side. When an AP-10 “hears” a message that is destined for a wireless station, the AP-10 forwards the message wirelessly to the station. If the message has a destination address that the AP-10 does not recognize, the AP-10 ignores the message.

The AP-10 is constantly “listening” for wireless messages as well. When the AP-10 “hears” a wireless message destined for another wireless unit, it relays the message directly to the wireless unit without forwarding the message to the wired LAN. When the AP-10 “hears” a wireless message whose destination it does not recognize (since it does not keep a list of known stations on its wired side), it forwards the message to the wired LAN. Messages cannot be sent directly between wireless stations without an AP-10 to relay the message.

1.5.4. SA-10 Station Adapter

The SA-10 station adapter is connected to a station's network card. When the station sends a message, the SA-10 wirelessly forwards it to the AP-10. And when the AP-10 receives a message destined for the station, it wirelessly forwards the message to the SA-10.

The first time the station sends a message, the station's address is registered in the AP-10. The AP-10 keeps only the first address for each SA-10, so the SA-10 will not work properly if connected to more than one station.

1.5.5. SA-40 Station Adapter

The SA-40 station adapter has four connectors for up to four stations and works just like the SA-10. As each station connected to the SA-40 sends its first message, each address is registered in the AP-10. The AP-10 keeps only up to four addresses for each SA-40, so the SA-40 will not work properly if connected to more than four stations.

1.5.6. WB-10 Wireless Bridge

As opposed to the SA-10 and SA-40 that connect directly to stations, the WB-10 wireless bridge connects to a wired Ethernet LAN (Hub). When a station on the WB-10's LAN sends a message that is not destined for a local station, the WB-10 wirelessly forwards the message to the AP-10. And when the AP-10 receives a message destined for a station on the WB-10's LAN, the AP-10 wirelessly forwards it to the WB-10. In this way, the WB-10 and AP-10 work together like a standard network bridge.

The first time each station on the WB-10's LAN sends a message, the station's address is registered in the WB-10 and the AP-10. The WB-10 and AP-10 can hold all the addresses necessary to support an entire LAN connected to a WB-10.

2. BASIC INSTALLATION

The **BreezeNET PRO.11 Series** is a plug-and-play solution, and the units begin to function when the following basic installation is complete. However, you can adapt the system to your particular needs using the local terminal (see Chapter 3).

For a description of various overall system configurations, refer to Chapter 4.

2.1. Basic Installation Checklist

Standard installation involves the following steps:

- Check the Package List.
- Position the unit and the antenna in the best location.
- Connect the power supply to the unit.
- Connect the Ethernet port to the unit.
- Check unit functionality using the LED indicators.

2.2. Check the Package List

When you first open the package, verify that the unit is complete with the following components:

- The unit, complete with two RF connectors for use with external antennas (“D” models).
- Quick Installation Guide/Card.
- 5V DC power supply transformer.
- Mounting bracket for wall or ceiling installations and torque key for antenna connectors (supplied with "D" models).

The AP-10 PRO.11 Access Point comes with the following additional components:

- The **BreezeNET PRO.11 Series** User's Guide.
- A monitor connector cable for connecting the units to a monitor in order to perform Local Terminal Management functions (see section 3.1).
- Proprietary MIB disk for performing remote unit configuration and monitoring via SNMP (see section 8.1.1).

Open the packaging carefully and make sure that none of the items listed above are missing. Do not discard packaging materials. If, for any reason, the unit is returned, it must be shipped in its original package.

2.3. Position the Unit

BreezeNET PRO.11 wireless LAN products are robust, trouble-free units, designed to operate efficiently under a wide range of conditions. The following guidelines are provided to help you position the units to ensure optimum coverage and operation of the wireless LAN.

Metal Furniture

Position the units clear of metal furniture and away from moving objects such as metal fans or doors.

Microwave Ovens

For best performance, position the units clear of radiation sources that emit in the 2.4 GHz frequency band, such as microwave ovens.

Antennas

For models with integrated antennas, make sure the antennas are extended upward vertically in relation to the floor. For models with external antennas, connect the external antennas and RF cable. For information about external antenna installation, refer to section 4.2

*Outdoor Installation Considerations.***Heat Sources**

Keep the units well away from sources of heat, such as radiators, air-conditioners, etc.

2.3.1. Additional Considerations When Positioning the Access Point

When positioning the AP-10 PRO.11 and AP-10DE Access Points, take into account the following additional considerations.

Height

Install the Access Point at least 1.5m above the floor, clear of any high office partitions or tall pieces of furniture in the coverage area. The Access Point can be placed on a high shelf, or can be attached to the ceiling or a wall using a mounting bracket.

Central Location

Install the Access Point in a central location in the intended coverage area. Good positions are:

- In the center of a large room.
- In the center of a corridor.
- At the intersection of two corridors.

Many modern buildings have partitions constructed of metal or containing metal components. We recommend that you install the Access Points on the corridor ceilings. The radio waves propagated by the **BreezeNET PRO.11** LAN are reflected along the metal partitions and enter the offices through the doors or glass sections.

2.4. Connect the Unit to the Power Supply

The unit operates on a power input of 5V DC, (1200mA , 1500mA peak) supplied by the power transformer included with the unit.

- Plug the output jack of the power transformer into the DC input socket on the unit. This socket may be located on the rear or side panel of the unit.
- Connect the supplied power transformer to a power outlet - 110/ 220VAC.

2.5. Connect the Unit to the Ethernet Port

- Connect one end of a an Ethernet 10BaseT cable (not supplied) to the RJ-45 port on the rear panel of the unit (marked UTP).
- Connect the other end of the connector cable to the Ethernet outlet:
 - When connecting an SA-10 or SA-40 to a PC, use a *straight* cable.
 - When connecting an AP-10 or WB-10 to a LAN, use a *straight* cable.
 - When connecting an AP-10 or WB-10 to a PC, use a *crossed* cable.
 - When connecting an AP-10 to a WB-10, use a *crossed* cable.

2.6. Check Unit Functionality using LED indicators

Check the unit functionality by using the LEDs on the front panel. The following tables describe the front panel LEDs for Stations (SA-10, SA-40) and Bridges (WB-10), and for Access Points.

2.6.1. Station (SA-10, SA-40) and Bridge (WB-10) LEDs

Name	Description	Functionality
PWR	power supply	On – After successful power up Off – Power off
WLNK	WLAN Link	On – Unit is synchronized or associated with an AP Off – Unit is not synchronized or associated with an AP
ETHR	Ethernet activity	On – Reception on Ethernet port Off – No reception on Ethernet port
QLT	Quality of reception	<p>LOAD ○ H very low quality reception or ○ M not synchronized with Access Point ○ L less than -81 dBm</p> <p>LOAD ○ H low quality reception ○ M (usually enabling 1 Mbps traffic) ● L from -81 to -77 dBm</p> <p>LOAD ○ H medium quality reception ● M (usually enabling 2 Mbps traffic) ● L from -77 to -65 dBm</p> <p>LOAD ● H high quality reception ● M (usually enabling 3 Mbps traffic) ● L greater than -65 dBm</p>

2.6.2. Access Point LEDs

Name	Description	Functionality
PWR	power supply	On – After successful power up Off – Power off
INFR	radio interference	Off – No interference Blinking – Interference Present
ETHR	Ethernet activity	On – Reception of data from Ethernet LAN that is forwarded to WLAN (in reject unknown mode) Off – No reception of data from Ethernet LAN that is forwarded to WLAN
LOAD	WLAN load Number of associated stations	<p>LOAD ○ H no stations ○ M ○ L</p> <p>LOAD ○ H ○ M 1-8 stations ● L</p> <p>LOAD ○ H ● M 9-16 stations ● L</p> <p>LOAD ● H ● M 17 or more stations ● L</p>

2.6.3. Verifying the Ethernet Connection

Once you have connected the unit to an Ethernet outlet, verify that the ETHR LED on the front panel is blinking. The ETHR LED should blink whenever the unit receives LAN traffic.

At the other end of the Ethernet link, verify that the LINK indicator is ON. For APs the LINK indicator is located on the attached hub port, and for Station Adapters the LINK indicator is located on the NIC.

3. DEVICE SETUP AND MANAGEMENT

This chapter explains how to access the local terminal program, and how to use the terminal program to setup, configure, and manage most **BreezeNET PRO.11 Series** units.

The **BreezeNET PRO.11 Series** is a plug-and-play solution and operates immediately after physical installation without any user intervention. However, you can adapt the system to your particular needs using the local terminal. In addition, all products in the series contain an SNMP agent and are configurable remotely via the network.

Note: Reset the unit after making configuration changes so that the changes will take effect.

3.1. Accessing and Using Local Terminal Management

To access Local Terminal Management:

1. Use the Monitor cable (supplied with the Access Point) to connect the MON jack on the rear panel of the unit to the COM port of your ASCII ANSI terminal or PC.
2. Run a terminal emulation program (such as HyperTerminal™).
3. Set up communication parameters to the following:
 - Baud Rate: 9600
 - Data Bits: 8
 - Stop Bits: 1
 - Parity: None
 - Flow Control: NONE
 - Connector: Connected COM port.
4. Press Enter. The main menu appears.

To use Local Terminal Management:

1. Press an option number to open/activate the option. You may need to press Enter in some cases.
2. Press Esc to exit a menu or option.
3. Reset the unit after making configuration changes.

3.2. Configuration Screens

Listed below are the menus, sub-menus, and parameters/options in the terminal program. Default values are listed where applicable. Numbers in the table below indicate how to reach each option. For example, to reach the *1.2.1 IP Address* option, start at the main menu, press 1, then 2, and then 1.

Menu	Sub-Menu	Parameter/Option	Default Values
1. System Configuration	1.1 Station Status	<ul style="list-style-type: none"> • Unit's Mode • Unit's H/W Address • Unit's WLAN Addr (<i>SA-10/40, WB-10</i>) • Station Status (<i>SA-10-40, WB-10 Only</i>) • Total Number of Associations since last reset (<i>SA-10-40, WB-10 Only</i>) • Current Number of Associations (AP) • Maximum Number of Associations since last reset (AP) • Current Number of Authentications (AP) • Maximum Number of Authentications since last reset (AP) 	
	1.2 IP and SNMP Parameters	1.2.1 IP Address 1.2.2 Subnet Mask 1.2.3 Default Gateway Address 1.2.4 SNMP Traps 1.2.5 Display Current Values	Not set Not set Not set Enabled
	1.3 Wireless LAN (WLAN) Parameters	1.3.1 Hopping Sequence (<i>AP Only</i>) 1.3.2 Hopping Set (<i>AP Only</i>) 1.3.3 ESSID 1.3.4 Maximum Data Rate 1.3.5 Transmit Antenna 1.3.6 Mobility 1.3.7 Load Sharing 1.3.8 Preferred AP (<i>SA-10/40, WB-10 Only</i>) 1.3.A Display Current Values	1 (FCC standard) 1 (FCC standard) ESSID1 3Mbps Use 2 Antennas* Low Disabled** Not set
	1.4 Bridging	1.4.1 LAN-WLAN Bridge Mode (<i>AP Only</i>) 1.4.2 Intelligent Bridging Period (<i>AP Only</i>) 1.4.3 IP Filtering 1.4.4 Tunneling 1.4.5 Broadcast Relaying 1.4.6 Unicast Relaying	Reject Unknown 15 sec Disabled Both Enabled Enabled

Menu	Sub-Menu	Parameter/Option	Default Values
	1.5 Station Control	1.5.1 Reset Unit 1.5.2 Load Factory Defaults	
	1.6.Security (Not activated)	1.6.1 Authentication Algorithm 1.6.2 Default Key ID 1.6.3 Preauthentication A. WEP Default Key #1 B. WEP Default Key #2 C. WEP Default Key #3 D. WEP Default Key #4	Open System Key #1 Disabled User defined User defined User defined User defined
2. Advanced Settings	2.1 Translation Mode		Enabled
	2.2 Roaming	2.2.1 Max Number of Scanning 2.2.2 Roaming Decision Window 2.2.3 Roaming Decision Numerator 2.2.4 Roaming Decision RSSI Threshold 2.2.5 Jogging Decision RSSI Threshold 2.2.6 Number of Beacons for Disconnect Decision 2.2.7 Number of Probe Responses Neighboring Beacon Rate	70 10 6 60 65 4 Sent every 40 dwell times
	2.3 Performance	2.3.1 Dwell Time (<i>AP Only</i>) 2.3.2 RTS Threshold 2.3.3 Max Number of Re-Transmissions 2.3.4 Number of Dwells to Re-Transmit 2.3.5 Max Multicast Rate 2.3.6 Power Saving (Not activated) 2.3.7 DTIM Period (Not activated) 2.3.8 IP Stack 2.3.9 Acknowledge Delay	128 milliseconds 120 bytes 1 2 1 Mbps Disabled 4 Enabled Regular
	2.4 Radio	2.4.1 Hopping Standard 2.4.2 Display Site Proprietary Sequences 2.4.3 Power Level 2.4.4 Carrier Sense Level 2.4.5 Carrier Sense Difference Level	US FCC User defined High 50 14
	2.5 Rate	2.5.1 Multi – Rate Support 2.5.2 Multi – Rate Decision window Size	Enabled 3
	2.6 AP Redundancy Support	Enter New AP Redundancy Support Decision Period (in seconds)	Disabled
	2.7 Maintenance	2.7.1 Auto Calibration 2.7.2 Wait for association Address 2.7.3 Japan Call sign	Enabled Wait for update
3. Site Survey	3.1 System Counters	3.1.1 Display Ethernet and WLAN Counters 3.1.2 Display Rate Counters 3.1.3 Display Rx Packets per Frequency 3.1.4 Reset All Counters 3.1.5 Power Saving Counters	
	3.2 Survey Software	3.2.1 Operation Mode (Rx/Tx) 3.2.2 Start Statistics	Rx

Menu	Sub-Menu	Parameter/Option	Default Values
		3.2.3 Stop Statistics	
	3.3 Event Log	3.3.1 Display Event Log 3.3.2 Erase Event Log 3.3.3 Event Storage Policy	From level warning up
	3.4 Display Neighboring AP's		
4. Access Control		4.1 Change Access Rights 4.2 Change Installer Password 4.3 Show Current Access Right	

* Option 1.3.5 Transmit Antenna has the default value Use #2 for the SA-40 unit only.

** Option 1.3.7 Load Sharing has the default value Enabled for the AP-10 unit only.

3.3. Main Menu

PRO.11 Series

Unit Model (SA-10, SA-40, WB-10, AP-10)

```

BreezeNET PRO.11 Series (SA-10)
Version : 4.3.10
Date: 15 Feb 1999 23:49:56

BreezeNET Monitor
=====
1 - System Configuration
2 - Advanced Settings
3 - Site Survey
4 - Access Control

Select option >
    
```

Software Version

Figure 3.1: Main Menu

3.4. System Configuration Menu

```
BreezeNET PRO.11 Series (SA-10)
Version : 4.3.10
Date: 15 Feb 1999 23:49:56

System Configuration menu
=====
1 - Station Status
2 - IP and SNMP Parameters
3 - Wireless LAN Parameters
4 - Bridging
5 - Station Control
6 - Security

Select option >
```

Figure 3.2: System Configuration Menu

3.4.1. Station Status

Station Status is a read-only sub-menu that displays the current values of the following parameters:

- **Unit Mode** – Identifies the unit’s function. For example, if the unit is an Access Point, “AP” appears in this field. If the unit is a Station Adapter (SA-10, SA-40) or a WB-10, "SA" appears in this field.
- **Unit H/W Address** – Displays the unit’s unique IEEE MAC address.
- **Unit WLAN Address (SA or WB)** – The address by which the unit associates. For the SA-10, this is the address of the PC. For the SA-40 and WB-10, this is the address of the hardware. This field does not appear when the unit is an AP.
- **Station Status (SA or WB)** – Current status of the station. There are three options:
 - *Scanning* - The station is searching for an AP with which to associate.

- *Sync Waiting for Address* - (this option is relevant only to the SA-10). The station is synchronized with an AP but has not yet learned its WLAN MAC address. The AP does not forward packets to the station when it is in this mode.
- *Associated* - The station is associated with an AP and has adopted the attached PC MAC address (for SA-10) or uses the unit's H/W address (SA-40 and WB-10), and is receiving packets from the LAN.
- **AP Address (Station Only)** – MAC Address of the AP with which the unit is currently associated.
- **Total Number of Associations since last reset** – Total number of stations currently associated with an AP.
- **Current Number of Associations (AP Only)** – Total number of stations currently associated with an AP.
- **Maximum Number of Associations since last reset (AP Only)** – For stations, this indicates the total number of associations and disassociations with various AP's. This is usually an indication of roaming. When the unit is an AP, this field indicates how many stations are currently associated with this particular AP.
- **Current Number of Authentications (AP Only)** – The current number of stations that are authenticated to this AP, including stations that are “pre-authenticated” and not associated to this AP.
- **Maximum Number of Authentications since last reset (AP Only)** – The number of authentications (and “preauthentications”) to this AP; since it was last reset. This number includes stations that were disauthenticated for different reasons.

3.4.2. IP and SNMP Parameters

All BreezeNET PRO.11 units contain IP Host software. This software is used for testing the unit for SNMP management functions and for downloading software upgrades using the TFTP protocol.

- **IP Address** – IP address of the unit.
- **Subnet Mask** – Subnet mask of the unit.
- **Default Gateway Address** – Gateway address of the unit.

- **SNMP Traps** – Whether this unit sends SNMP traps. If enabled, when an event occurs, a trap is sent to the defined host address (see section 8.1.2 for a list of traps). You can configure the host address to which the traps are sent through SNMP management.
- **Display Current Values** – Displays information concerning the current status of all IP-related items.

3.4.3. Wireless LAN (WLAN) Parameters

The WLAN Parameters Menu contains the following options:

- **Hopping Sequence (AP Only)** – Hopping sequence of the unit.

A hopping sequence is a pre-defined series of channels (frequencies) that are used in a specific, pseudo-random order as defined in the sequence. The unit “hops” from frequency to frequency according to the selected sequence. When more than one AP is co-located in the same area (even if they are not part of the same network) it is recommended to assign a different hopping sequence to each AP.

Hopping sequences are grouped in three hopping sets. The hopping set selected in the Hopping Set screen (see next parameter) determines which hopping sequences are available in this screen. When setting up multiple APs in the same site, always choose hopping sequences from the same hopping set. This reduces the possibility of collisions on the WLAN.

This parameter is set only in AP-10 PRO.11 Access Point. It is not accessible from any other **BreezeNET PRO.11** unit. All other stations learn it from the Access Point during the association process. Different co-located WLAN segments should use different hopping sequences.

- **Hopping Set (AP Only)** – Hopping set (between 1 and 3) of the unit. Hopping sequences are grouped in several hopping sets. The hopping set selected in this screen determines which hopping sequences are available in the Hopping Sequence screen (see previous parameter). Always use the same hopping set per site. Following is the list of hopping sequences and sets for each country.

The default value for all countries is:

Hopping Sequence=1, Hopping Set=1.

- **ESSID** – ESSID of the unit (up to 32 printable ASCII characters). The ESSID is a string used to identify a WLAN. This ID prevents the unintentional merging of two co-located WLANs. A station can only associate with an AP that has the same ESSID. Use different ESSIDs to segment the WLAN network and add security.

Note: The ESSID is case-sensitive.

- **Maximum Data Rate** – Maximum data rate of the unit. **BreezeNET PRO.11** units operate at 1 Mbps, 2 Mbps or 3 Mbps. The unit adaptively selects the highest possible rate for transmission. Under certain conditions (compatibility reasons or for range/speed trade-off) you may decide to limit the use of higher rates.
- **Transmit Antenna** – Which antennas are used for transmission. During reception, a **BreezeNET PRO.11** unit dynamically selects the antenna where reception is optimal. In contrast, *before* transmission the unit selects the antenna from which it will transmit. It usually uses the antenna last used for successful transmission. In models with external antennas, sometimes only a single antenna is used. In this case, Transmit Antenna should be configured to transmit only from that single antenna. Similarly, models using a booster or an LNA use only a single antenna for transmission. There are three possibilities for configuration:
 - 0 Use Two Antennas
 - 1 Use Antenna No. 1 only
 - 2 Use Antenna No. 2 only
- **Mobility** – **BreezeNET PRO.11** stations optimize their roaming algorithms according to the mobility mode parameter. For example, a stationary station is more tolerant of bad propagation conditions. It assumes that this is a temporary situation and is not caused by the station changing position. Initiating a roaming procedure in such a case would be counter-productive. In general, Wireless stations can be used in one of three mobility modes:
 - **High** – For stations that may move at speeds of over 30 km per hour.

- **Medium** – For stations that may move at speeds of over 10 km per hour, but not over 30 km per hour.
- **Low** – For stations that will not move at speeds of over 10 km per hour. *Low* is the default value. In most cases this is the best choice.
- **Load Sharing** – When installing a Wireless LAN network in a high-traffic environment; you can increase the aggregate throughput by installing multiple APs to create co-located cells. When load sharing is enabled, the wireless stations distribute themselves evenly among the APs to best divide the traffic between the APs.
- **Preferred AP** – AP MAC (Ethernet) address of the preferred AP. You can configure a station to prefer a specific AP unit. When the station powers up, it will associate with the preferred AP even if the signal from that AP is lower than the signal from other APs. The station will roam to another AP only if it stops receiving beacons from the preferred AP.
- **Display Current Values** – This read-only status screen displays current WLAN parameters. Press any key to return to the WLAN Parameters Menu.

3.4.4. Bridging

The Bridging Menu contains the following options:

- **LAN to WLAN Bridging Mode (AP Only)** – The options are:
 - *Reject Unknown* – Type 0 to allow transmission of packets only to stations that the AP knows to exist in the Wireless LAN (behind the Wireless Bridge).
 - *Forward Unknown* – Type 1 to allow transmission of all packets except those sent to stations that the AP recognizes as being on its wired Ethernet side. When connecting very large networks; it is recommended to set this parameter to *forward unknown*.
- **Intelligent Bridging Period (AP Only)** – Intelligent bridging enables smooth roaming of WB-10 units. When intelligent bridging is enabled, the AP goes into a special bridging mode for a fixed amount of time whenever a wireless bridge (WB) roams into its area. This mode causes the AP to forward packets destined for the stations behind the WB-10. Even though, they are known or were learned from the wired side

(except that no learning of the wired LAN will take place). Afterwards, the AP will switch back to *Reject Unknown* bridging mode.

This procedure prevents packets destined for stations behind the bridge from getting lost. The value of this parameter is the length of time in seconds that the AP will remain in special mode.

- **IP Filtering** – Whether IP filtering is enabled for the unit. Enable IP Filtering to filter out any other protocol (such as IPX) if you want that only IP traffic will pass through the WLAN.
- **Tunneling** – Whether the unit performs Appletalk or IPX tunneling.
 - *Disable Appletalk Tunneling.* This parameter allows to disable or enable (default) Appletalk tunneling; if the network contains a mix of Ethertalk1 (ET1) and Ethertalk2 (ET2) stations to ensure smooth communications. Be sure to set all units to the same tunneling setting.
 - *Disable IPX Tunneling.* This parameter allows to disable or enable (default) IPX tunneling; if the IPX protocol is running over your network. Be sure to set all units to the same tunneling setting.
- **Broadcast Relaying (AP Only)** – When Broadcast Relaying is enabled, Broadcast packets originated in WLAN devices are transmitted by the AP back to the WLAN devices, as well as to the LAN. If it is disabled, these packets are sent only to the local wired LAN and are not sent back to the WLAN. Disable Broadcast Relaying only if you know that all Broadcast messages from the WLAN will be destined to the wired LAN.
- **Unicast Relaying** – When Unicast Relaying is enabled, Unicast packets originated in WLAN devices can be transmitted back to the WLAN devices. If this parameter is disabled, these packets are not sent to the WLAN even if they are intended for devices on the WLAN. Disable Unicast Relaying only if you know that all Unicast messages from the WLAN will be destined to the local wired LAN.

Note: Notice that some of the most common internet applications use peer-to-peer traffic, such as “chat”, ICQ and even internet browsing between a client and a server which are connected wirelessly on the same subnet. Disabling Broadcast or Unicast relaying will cause such applications to become unavailable.

3.4.5. Station Control

The Station Control Menu contains the following options:

- **Reset Unit** – Resets the BreezeNET PRO.11 unit and applies any changes made to the system parameters.
- **Set Factory Defaults** –When this option is implemented, system parameters revert back to the original factory default settings. There are two options:
 - *Full* – All parameters revert to defaults except for the Hopping Standard and Japan Call Sign (if applicable).
 - *Partial* – All parameters revert except for the Hopping Standard and Japan Call Sign (if applicable), IP Address, SubNet Mask, Default Gateway, Hopping Sequence, Hopping Set, ESSID, Transmit Antenna, Acknowledge Delay, Preferred AP, IP Filtering, Hopping Standard, Power Level, Auto Calibration.

3.4.6. Security

Security options are not activated yet.

The security mechanism involves configuring four different modules:

- **Authentication Algorithm** – This module operates in two modes:
 - *Open System (Default)*. There is no privacy implemented by authentication. After synchronization, a station will send a request for authentication and immediately receive a “successful authentication” message from the AP.(2 frames)
 - *Shared Key authentication (for users with access keys)*. This option will activate the WEP cryptographic authentication. After synchronization, a station will send a request for authentication, the AP will answer with a “challenge text” (ASCII characters), the station will encrypt this text using RC4 (not yet implemented) with the encryption key in use and send this text back to the AP, the AP will decrypt the received message and if it matches the original text it will send a “successful authentication” message. (4 frames).

The association process will begin only after a successful authentication (in either system).

- **Default Key ID** – In order to authenticate, the value of the key used by the station and the AP must be identical. During the authentication process a station must notify the AP which key it used to encrypt the challenge text. The station will do this by passing the number of the current default key it uses. The AP and station must have the same keys (values).

- **Preauthentication** – During the authentication process the AP is notifying the other AP's connected to the Ethernet backbone to preauthenticate the station that has been authenticated to this AP. It is recommended to use this feature when there is plenty of roaming between the AP's. Preauthentication must be activated on both the AP's and the Station.
- **WEP Key#1-4** – These 4 Access Keys must be configured before they can be used. In this screen you may enter the encryption key. The key is made of 10 Hex (0-9,A-F) characters. In order to change the unit to work in shared key authentication all four keys must be entered. Entering zeros (0000000000) which is the default for this parameter will cause the unit to work in open system authentication.

3.5. Advanced Settings Menu

```
BreezeNET PRO.11 Series (SA-10)
Version : 4.3.10
Date: 15 Feb 1999 23:49:56

Advanced menu
=====
1 - Translation Mode
2 - Roaming
3 - Performance
4 - Radio
5 - Rate
6 - AP Redundancy Support
7 - Maintenance

Select option >
```

Figure 3.3: Advanced Settings Menu

The following sections describe the important parameters and relevant information in the Advanced Settings Menu. All menu options can be viewed by the Installer; However, the modification of certain parameters from this menu, require the Technician access rights level.

3.5.1. Translation Mode (read-only)

The translation of Ethernet packets can be *enabled* (default) or *disable*.

3.5.2. Roaming (read-only)

The Roaming menu contains parameters related to when and how the unit roams from one AP to another. The following windows can be accessed from the Roaming menu:

- Max. Number of Scanning
- Roaming Decision Window
- Roaming Decision Numerator
- Roaming Decision RSSI Threshold – *At what signal strength the unit roams to another AP*
- Joining Decision RSSI Threshold – *At what signal strength the unit associates with an AP*
- Number of Beacons for Disconnect Decision
- Number of Probe Responses
- Neighboring Beacon Rate
- Neighboring AP's – *Currently known number of AP's*

3.5.3. Performance

The Performance menu contains parameters regarding unit performance:

- **Dwell Time (AP Only)** – The time spent on a radio channel before hopping to the next channel in the sequence. The default value is 128ms.
- **RTS Threshold** (read-only) – Minimum packet size to require an RTS. For packets smaller than this threshold, an RTS packet is not sent and the packet is transmitted directly to the WLAN. The threshold is 120 bytes. A station wanting to transmit a packet, first transmits a short control packet called **RTS** (Request To Send), which includes the source, destination, and the duration of the following transaction (i.e. the packet and the respective **ACK**). The destination station responds (if the medium is free) with a response control Packet called **CTS** (Clear to Send), which includes the same duration information.
- **Max. Number of Re-Transmissions** (read-only) – If a packet was received with errors or not received at all, the station will not transmit an ACK (acknowledgement) packet. The station that initiated the first transmission will try to re-transmit the packet. The number of times the unit will try to re-transmit this packet is determined by two parameters in

this menu, *Max. Number of Re-Transmissions* and *Number of Dwells to Re-Transmit*. This parameter can be presented as a counter. This counter is decreased each time a re-transmission occurs. It will be the minimum number of times a packet will be re-transmitted.

- **Number of Dwells to Re-Transmit** (read-only) – A re-transmission will be performed after a set number of Dwells. This parameter works in conjunction with the Max Number of Re-Transmissions parameter.
- **Max Multicast Rate** (read-only) – Multicast and Broadcast transmissions are not yet acknowledged, the chance of error increases. Therefore by default, the unit will always transmit broadcasts, multicasts and control frames in the minimum possible rate, 1Mbps.
- **Power Saving** – *This option is not activated yet.*

There are three modes:

- *Disable* (Active Mode): The station is Active all the time, uses full power.
- *Enable* (Power Save Mode): In this mode the station has two states: **Awake state**, uses full power. **Doze (sleep) state**, uses approximately 5% power.
- *Enable and test PM bit*. In this mode the station will test every frame and check if the power management bit is enabled.

Power Management Mechanism:

Stations inform AP about their Power Management Mode (Active or Power Save). Stations in Power Save Mode are usually in sleep state. A station will enter awake state in order to transmit data and also from time to time in known intervals (DTIM period). AP's maintain a table indicating the Power Save mode of each associated station. Data destined for Active Mode stations is sent immediately by AP. Data destined for Power Save Mode stations is buffered by AP. Every Beacon includes TIM (Traffic Identification Map). TIM identifies the stations (by SID) of data buffered in the AP, waiting to be retrieved. If a station recognizes its address in the TIM, the station will send a PS-POLL (Power Save Poll) to the AP. In response to this, the AP will forward a data frame buffered for that station.

Aging: If a data frame is buffered in the AP more than 50 seconds, it will be deleted along with all other frames buffered for that station.

This process is done every 2 seconds.

Notice that although power save mode is set in the AP it will not effect the APs' power consumption, but only the handling and management.

- **DTIM Period** (read-only) – This is the number of dwells between broadcast transmissions of messages for stations in power saving mode.

Note: This option is not activated yet.

- **IP Stack** – By default this parameter is enabled. If it is disabled, it will improve performance, but IP support will not be available.
- **Acknowledge Delay** – Acknowledge delay is designed to increase the performance in links **LONGER THAN 20 KM**. This parameter increases the ACK timeout in the units, and therefore allows a more efficient operation. When a BreezeNET unit transmits a certain packet, it waits for a pre defined time interval (ACK Timeout) for an ACK packet to be received. If the ACK is not received during that interval, the unit will assume the transmission has failed, and will retransmit the packet. In links longer than 20 km, that ACK timeout is not long enough for the ACK to arrive to the other side on time, and therefore unnecessary retransmissions are made, causing the performance to drop. This parameter increases the ACK timeout and allows the ACK to arrive to the other side on time, in links longer than 20 km.

Note: Acknowledge delay **must be enabled on both sides of the link**, when the distance is greater than 20 km. If used in links shorter than 20 km, a significant performance drop may occur.

3.5.4. Radio

The Radio menu contains the following major parameters:

- **Hopping Standard** (read-only) – The *Hopping Standard* is a set of rules regarding the radio transmission standard allowed in each country. Units will work together only if set to the same hopping standard.
- **Power level** – Output power level at which the unit is transmitting. There are two possibilities, Low (4dBm) or High (17 dBm) at the antenna connector.
- **Carrier Sense Level** (read-only) – Before transmission a station will check if the media is free of other transmissions. This parameter is a threshold in RSSI units that determines the sensitivity of the Carrier

Sense mechanism. Signals with a lower RSSI are considered “noise” and are disregarded by the unit.

- **Carrier Sense Difference Level** (read-only) - Carrier Sense Difference Level refers to a sudden rise of the signal level. This parameter is the minimum rise in RSSI units to be considered a Carrier Sense positive result, in which case the unit will not attempt to transmit. It is recommended **not** to change this parameter

3.5.5. Rate

The Rate menu contains the following relevant parameters:

- **Multi-Rate Support** (read-only) – When this parameter is enabled, the unit will automatically switch to the best transmission rate at any given time.
- **Multi-Rate Decision Window Size** (read-only) – This parameter indicates the number of packets to be used for multi-rate decisions. It is recommended **not** to change the value of this parameter.

3.5.6. AP Redundancy Support (read-only)

When the AP identifies the Ethernet wire connection has been disconnected over a defined time period; it stops transmitting. The default mode is disabled (the AP continues transmitting even when the link is discontinued).

3.5.7. Maintenance

The Maintenance menu contains the following major parameters and information:

- **Auto Calibration** – When the unit is started, it performs an internal self-test. Part of this test is automatic calibration of the DC Offset and deviation pattern. Auto Calibration is not supported in the “DE” models, and it therefore must be disabled for “DE” units.
- **Wait for Association Address (SA only)** – For the SA-10, the Association address is the MAC address of the NIC (Network interface Card) card that the station is connected to through the Ethernet UTP port (usually the Ethernet card of the PC). The station uses the Association Address as its identification in the Wireless Cell (WLAN address). When a station is first connected to an ethernet port, it waits for the

Association Address update over the Ethernet. You can also have the device use its own MAC address (Use Mine) for testing purposes, in which case there will not be a proper network connection.

3.6. Site Survey Menu

```
BreezeNET PRO.11 Series (SA-10)
Version : 4.3.10
Date: 15 Feb 1999 23:49:56

Site Survey menu
=====
1 - System Counters
2 - Survey Software
3 - Event Log
4 - Display Neighboring AP's

Select option >
```

Figure 3.4: Site Survey Menu

The Site Survey Menu gives access to the sub-menus necessary to perform a *Site Survey* that helps you position your units and align their antennas, as well as perform troubleshooting.

The following sections first describe the sub-menus in the Site Survey menu, and then explain step-by-step how to perform a Site Survey. The Site Survey menu contains four sub-menus:

- System Counters
- Survey Software
- Event Log
- Display Neighboring AP's

3.6.1. System Counters

```
BreezeNET PRO.11 Series (AP-10)
Version : 4.3.10
Date: 15 Feb 1999 23:49:56

System Counters menu
=====
1 - Display Ethernet and WLAN Counters
2 - Display Rate Counters
3 - Display Rx packets per frequency
4 - Reset All Counters
5 - Power Saving Counters

Select option >
```

Figure 3.4b: Systems Counters Menu

The System counters are a simple yet very efficient tool to monitor, interpret and analyze the Wireless LAN performance. The counters contain statistics concerning Wireless and Ethernet frames.

The submenu contains the following options:

- **Display Ethernet and WLAN Counters** – Choose this option to display the current value of the Ethernet and Wireless counters.

Ethernet Counters

Ethernet counters display statistics about the unit's Ethernet port activity.

The unit receives Ethernet frames from its UTP port and forwards them to its internal bridge, which decides whether or not to transmit them to the Wireless LAN. The units have a smart hardware filter mechanism which filters most of the frames on the LAN, and hardware filtered frames are not counted.

On the other side, frames which were received from the wireless LAN and some frames generated by the unit (answers to SNMP queries and pings which reached to the unit via the UTP port), will be transmitted to the UTP port.

Available Counters:

- **Total Received frames** – The total number of frames received from the UTP port. This counter includes both bad and good frames.

- **Received Bad Frames** – The number of frames with errors received from the UTP port. High values (more than just a few) indicate a problem in the UTP connection such as a bad UTP cable or hub port.
- **Received good frames** – The number of good frames (i.e. frames with no errors) received from the UTP port.
- **Forwarded to the bridge** – The number of received frames that were forwarded to the unit's internal bridge. This counter should be equal to the number of good frames unless the internal bridge is overloaded.
- **Missed Frames** – Frames that the unit recognized but failed to read due to internal bridge overload. This counter should equal zero unless the internal bridge is overloaded.
- **Transmitted to Ethernet** – The number of frames transmitted by the unit to the UTP port. These mainly include frames that have been received from the Wireless side, but also includes frames generated by the unit itself.

Wireless LAN Counters

Wireless counters display statistics about the unit's Wireless LAN activity.

Transmission to the wireless media includes data frames received from the UTP ports, as well as self generated control and management frames. When a data frame is transmitted, the unit will wait for an *acknowledge* from the receiving side. If an *acknowledge* is not received, the unit will retransmit the frame until it gets an acknowledge (there are no retransmissions for control frames). If the unit has retransmitted a frame for the maximum number of retransmissions (refer to section 3.5.3) it will stop re-transmitting the frame and drop this frame.

Available Counters:

- **Total Transmitted Frames** – The number of frames transmitted to the wireless media. The count includes the first transmission of data frames (without retransmissions), and the number of control and management frames.

Notice that an AP continuously transmits a control frame called *beacon* in every frequency to which it hops, in order to publish its existence and keep its associated stations synchronized. Thus, the total

transmitted frames counter will get high values even if the AP-10 is not connected to an active LAN.

- **Total Transmitted Frames (Bridge)** - The total number of data frames transmitted to the wireless media (i.e. frames that were received from the UTP port and forwarded to the internal bridge which decided to transmit them to the wireless media).
- **Total Transmitted Data Frames** – This counter is similar to the above but counts only data frames. In most **BreezeNET PRO.11** units, the number of total transmitted frames and total transmitted frames (bridge) are identical. In the case of the AP, due to the inclusion of beacon frames, this number will be higher than that for Total transmitted frames.
- **Frames Dropped (too many retries)** – The number of frames which were dropped since they were retransmitted for the maximum number of allowed retransmissions and weren't acknowledged.
- **Total Transmitted Fragments** – The total number of transmitted frames. The count includes data, control and management frames, and the number of retransmissions of data frames (for example, if the same data frame is retransmitted ten times, the count will increase ten times).
- **Total Retransmitted Fragments** – The total number of retransmissions of data frames (for example, if the same data frame is retransmitted ten times then the count will increase ten times). In a point-to-point application, this counter should relatively correspond to the number of bad fragments received on the other side.
- **Total Tx Errors** – The number of transmit errors that have occurred. Currently this counter also includes normal situations where a fragment has not been transmitted because the dwell time has elapsed.
- **Internally Discarded** – The number of frames that the AP discarded due to a buffer overflow. Frame discard will occur mainly when the wireless conditions are bad and the unit is busy re-transmitting frames and doesn't have time for handling new frames.
- **Power Saving Aged** – The AP buffers frames for stations in a power saving sleep mode. This counter counts the number of frames dropped by the AP because a station did not wake up for a long time.

- **Power Saving Free Entries** – Number of free buffers (one frame each) available for power save management. These buffers hold messages for stations that only periodically make contact with the AP due to power considerations.
- **Total Received Frames** - The number of frames received from the wireless media. The count includes data and control frames (including beacons received from AP's).
- **Total Received Data Frames** – The number of data frames received from the wireless media.
- **Total Received Fragments** – The total number of frames received, including data, control and duplicate data frames (see *duplicates and dwell timeouts* parameter below).
- **Bad Fragments Received** – The number of frames received from the WLAN with errors. In a point-to-point application, this counter should relatively correspond to the number of retransmitted fragments on the other side.
- **Duplicates and Dwell timeouts** – When a unit receives a frame; it sends an *acknowledgement* for it. If the acknowledge is lost, than it receives a second copy of the same frame, since the other side thinks this frame was not received. Although duplicate frames are count, only the first copy of the frame is forward to the UTP port.

- **Display Rate Counters** – Displays contents of packets at each rate. The AP displays counters per station.
- **Display Rx Packets per Frequency** - Histogram of the number of frames received on each channel. This graph is explained fully in section 3.6.6 , *Using the Rx Packets per Frequency Histogram*.
- **Reset Counters** - Choose this option to reset all the counters. After choosing this option, you will be requested to type 1 for confirmation or 0 to cancel the reset.
- **Power Saving Counters** – Displays the power saving per station, the number of transmitted frames and the number of discarded frames. This applies only to AP's.

3.6.2. Survey Software

The Survey Software sub-menu enables you to align antennas and to assess the radio signal quality of a point-to-point link. The sub-menu includes the following options:

- **Operation Mode** – When running a Site Survey, set the units on either side of the link to either receive (option 1) or transmit (option 2) packets (one unit should be set to transmit and the other to receive). Option 0 (Idle mode) is not active at present.
- **Start Statistics** – Press **2** and then press any digit to start Site Survey.
- **Stop Statistics** – Press **3** and then press any key to stop update of Site Survey statistics.

3.6.3. Event Log

- **Display Event Log** - The last four error messages that the unit displayed since the last *Factory Defaults* reset. The Event log stores events in four levels of error notifications: *Message*, *Warning*, *Error*, and *Fatal*.
- **Erase Event Log** – Erase a specific event log.
- **Event Storage Policy** – Defines storage level for the event log.

The following are the levels which events are stored in log:

- 0 - Store all events (beginning at message level)
- 1 - Store all events from warning level up
- 2 - Store all events from error level up
- 3 - Store fatal events only

3.6.4. Display Neighboring AP's

Displays neighboring AP's on the same ESS. The information displayed in this option refers to the CURRENT or NEIGHBOR AP that the station can hear. The following information is displayed.

- The MAC Address of the AP described.
- **Good or bad frames:** The number of frames, out of the total number of frames received from the current AP, that are considered “good or bad”. A frame is considered good or bad; if it was received in an RSSI level higher or lower than the value set at the “Roaming Decision RSSI Threshold” parameter (see “Roaming” on section 3.5.2).

- **Total:** The number of frames set as the “Roaming Decision Window” - 10 in the example shown above (see “Roaming” on section 3.5.2).
- **avr RSSI:** The average RSSI level of the total number of frames (only includes the frames received without errors).
- **bcn cnt:** (Beacon Count) - How many dwells have passed since the last beacon has been received.
- **Load:** The number of stations currently associated with the described AP. This parameter will be displayed only when “Load Sharing” (page 24) is Enabled.

3.6.5. Using the Site Survey Software

To use the Site Survey Software:

1. Roughly, align the antennas on either side of the link before starting the Site Survey procedure.
2. Verify that the Ethernet cables are disconnected from both units.
3. Press **1** to go to the Operation mode screen. Set the units on either side of the link to either receive (option 1) or transmit (option 2) packets (one unit should be set to transmit and the other to receive).
4. Start the survey by selecting option (2) in the Survey Software menu in both units. When performing a site survey from a station to an AP (transmitting from the station to the AP), always begin with the station (select option (2) on the station).
5. On the transmit side, a screen appears displaying a table with the number of packets and the frequency at which each packet was transmitted (refer to Figure 3.5). This list is updated continuously. Select option (3) to stop sending packets.

```
BreezeNET PRO.11 Series (AP-10)
Version : 4.3.10
Date: 15 Feb 1999 23:49:56

# Tx Packets Channel
0 37
1 10
2 7
3 30
4 28
5 44
6 35
7 12
8 48
9 76
10 42
```

Figure 3.5: Transmit Statistics

6. On the receive side of the link, the screen displays a table showing the packet number received, the antenna port that was selected for the reception, the Received Signal Strength Indicator (RSSI) for each antenna, the bit error rate, the frequency at which each packet was transmitted, the data rate at which the packet was transmitted, and the quality of the signal (refer to Figure 3.6). Use only the RSSI reading from the selected antenna.

```
BreezeNET PRO.11 Series (AP-10)
```

```

Version : 4.3.10
Date: 15 Feb 1999 23:49:56

#Pack Ant RSSI1 RSSI2 Bit_Err Freq Rate Quality
58 1 108 91 0 19 3 #####
59 2 110 112 0 42 3 #####
60 2 86 88 0 14 3 #####...
61 2 109 112 0 46 3 #####
62 1 109 107 0 24 3 #####
63 1 108 106 0 22 3 #####
64 1 112 108 0 33 3 #####
65 1 111 107 0 25 3 #####
66 1 111 111 0 41 3 #####
67 2 111 110 0 79 3 #####
68 1 115 111 0 64 3 #####
69 1 115 111 0 65 3 #####
70 2 111 111 0 56 3 #####
71 2 110 111 0 55 3 #####
    
```

Figure 3.6: Receive Statistics

- The RSSI is given in arbitrary units. Use the following graph (Figure 3.7) to correlate RSSI to dBm.

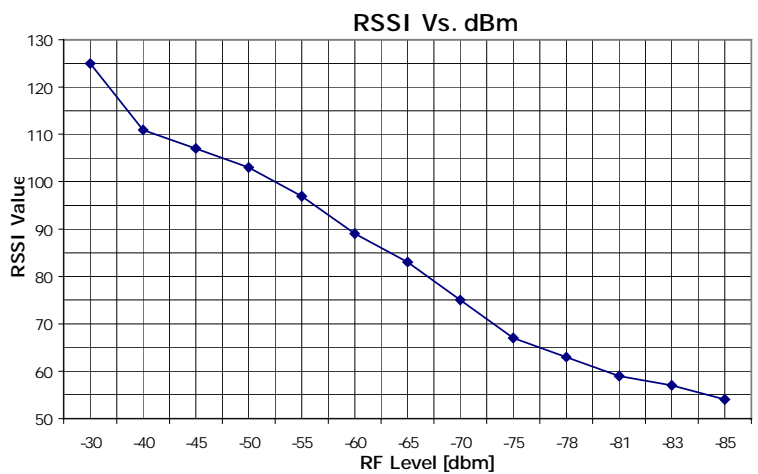


Figure 3.7: RSSI to dBm Graph

- Re-align the antennas until the maximum received signal strength is obtained. As you align the antennas, you will see that the RSSI (received signal strength indicator) continually increases until it reaches a certain level after which the RSSI begins to decrease. This is the maximum attainable RSSI level indicating optimum receive antenna alignment.

interference. Frequencies with low numbers of packets received probably have more interference than other frequencies.

3.7. Access Control Menu

Access Control functions enable the System Administrator or Installer to limit the access to the Local Terminal Maintenance setup and configuration menus.

```
BreezeNET PRO.11 Series (AP-10)
Version : 4.3.10
Date: 15 Feb 1999 23:49:56

Access Control menu
=====
1 - Change Access Rights
2 - Change Installer Password
S - Show Current Access Right

Select option >
```

Figure 3.9: Access Control Menu

The Access Control menu includes the following options:

- **Change Access Rights** – This screen determines the level of access rights to the **BreezeNET PRO.11** unit's setup and configuration menus. When the unit is first installed, the default setting is option (1), Installer and the default password is "user":
 - *User* – The Local Terminal Management menus are read-only for a user who does not possess the correct password. The ESSID and security parameters are hidden by asterisks (*) at this level.
 - *Installer* – The installer has access to configure all required parameters in the system configuration menu, as well as some of the advanced settings. Access is password-protected. After

configuration, the installer should change access rights to option (0), User. The installer can also change the installer password (see next parameter).

- *Technician* – Only a Certified BreezeCOM Engineer possessing the correct password can select this option to configure all the parameters and settings.

- **Change Installer Password** – Type in the new password according to the directions on screen. This screen changes the installer password to prevent unauthorized persons from making any changes in system configuration and setup. The password is limited to eight printable ASCII characters. This option is not available at User level.
- **Show Current Access Right** – This read-only screen presents the current access right configuration.

*Important: If you change the Installer password **do not forget it**, or you will be unable to change the unit's access rights.*

4. PLANNING AND INSTALLING WIRELESS LANs

This chapter describes various possible system configurations, lists points to consider when performing indoor and outdoor installations, presents guidelines and restrictions regarding external antenna installation. It also describes some antennas that work well with **BreezeNET PRO.11** units.

4.1. System Configurations

This chapter describes various wireless LAN configurations, and how to set them up:

- **Single Cell Configuration** – The wireless LAN consists of an Access Point and the wireless workstations associated with it.
- **Overlapping Cell Configuration** – The wireless LAN consists of two or more adjacent Access Points whose coverage slightly overlaps.
- **Multicell Configuration** – The wireless LAN consists of several Access Points installed in the same location. This creates a common coverage area that increases aggregate throughput.
- **Multi-Hop Configuration** – The wireless LAN contains AP-WB pairs that extend the range of the wireless LAN.

Many wireless LANs contain several of these configurations at different points in system. The Single Cell configuration is the most basic, and the other configurations build upon it.

4.1.1. Single Cell Configuration

A basic **BreezeNET** cell consists of an Access Point and the wireless workstations associated with it. You can convert most workstations (PCs, X-Terminals, Apple, Digital, SUN, HP, IBM and others) that are equipped with an Ethernet network interface card (NIC) to wireless workstations simply by connecting a **BreezeNET** SA-10 PRO.11 Station Adapter.

There are three types of Single Cell Configuration:

- Point-to-Point
- Point-to-Multipoint
- Mobile Applications

Each type is explained in the following sections.

4.1.1.1 Point-to-Point

Point-to-Point installations (refer to Figure 5.1) require directional antennas at either end of the link. To select the best antenna for a specific application, consider the following factors:

- Distance between sites
- Required throughput
- Clearance between sites
- Cable length.

Refer to the range tables (section 4.2.7) to determine the best combination of antennas for your application.

4.1.1.2 Point-to-Multipoint

Point-to-Multipoint applications consist of one or more APs at the central site and several remote stations and bridges (SA-10, SA-40, WB-10). In this case, use an Omni antenna with the Access Point because of its 360° radiated pattern. In the United States, the Omni-8 antenna (which also has a 360° radiated pattern but has a wider range) can also be used. The Omni-8 antenna comes with 20ft. of low loss cable and a mast mount bracket for rooftop installations.

The remote units should use directional antennas aimed in the direction of the AP's antenna(s).

4.1.1.3 Mobile Applications

In mobile applications, station orientation changes continuously. In order to maintain connectivity throughout the entire coverage area, most mobile applications require omni-directional antennas for both Access Points and wireless stations. In a motor vehicle, for example, you can install an SA-10 in the cabin, and mount the antennas on the roof.

4.1.1.4 Extending the LAN with WLAN Bridging

The figures below demonstrate how the WB-10 can be used to extend a regular network with a wireless link.

Disclaimer: This diagram is for illustrative purposes only. It should not be confused with the transceiver operating in a standalone mode. When this diagram is in use, the transceiver will be used in conjunction with amp model

AMP-2440-250/500 and the antennas listed in this manual.

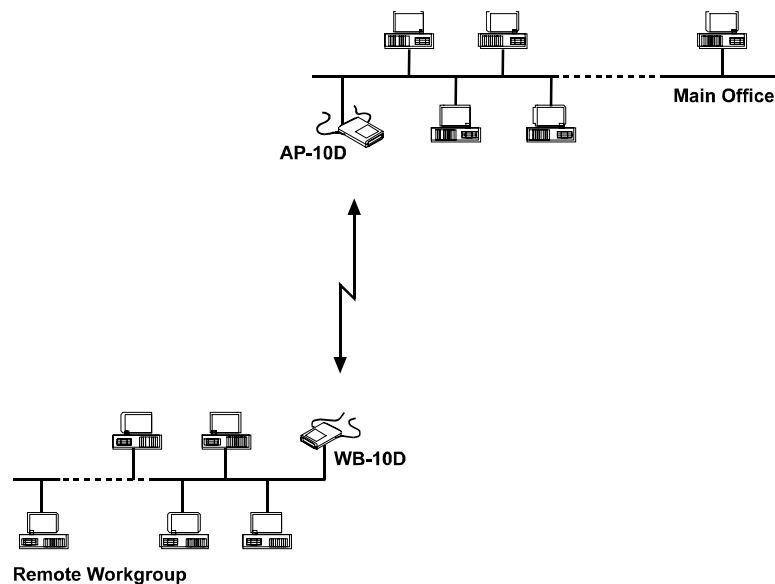


Figure 5.1: Connecting Remote Offices to Main Office Network

The WB-10 PRO.11 also enables connectivity between a wireless LAN and individual workstations or workgroups located outside the LAN. The WB-10 PRO.11 enables these wireless stations in its coverage area to communicate with the wireless LAN and gain access to all of the network resources such as file servers, printers and shared databases.

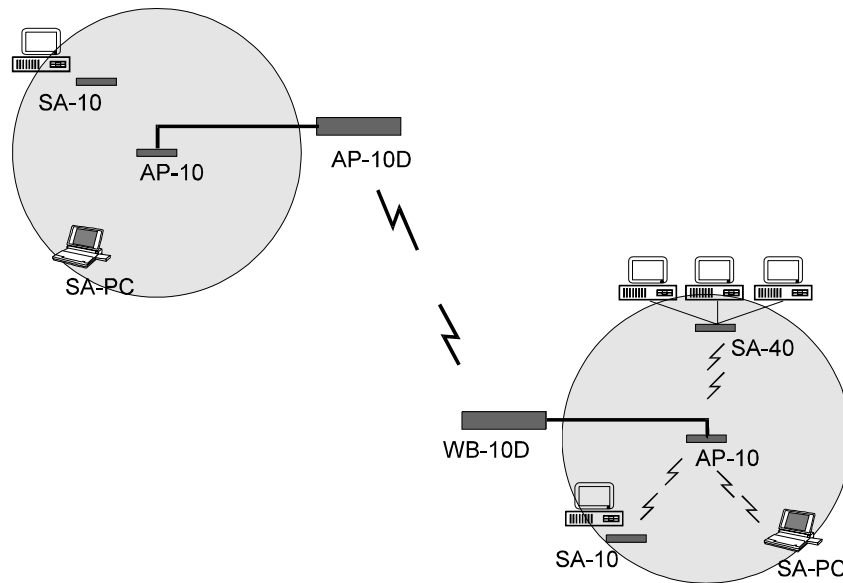


Figure 5.2: Wireless Bridging Between Two or More Wireless LAN Segments

4.1.1.5 Setting Up a Single BreezeNET Cell

To set up a single BreezeNET cell:

1. Install the Access Point (refer to section 2, *Basic Installation*). Be sure to position the Access Point as high as possible.

Note: It is not necessary at this point to connect the Access Point to an Ethernet backbone, since Access Points continuously transmit signals (beacon frames) whether they are connected to an Ethernet backbone or not.

2. Install a Station Adapter (refer to section 2, *Basic Installation*).
3. Check the LED indicators of the front panel of the Station Adapter, to check signal strength.
4. Make any necessary adjustments, for example:

- Adjust the antennas
 - Adjust the location of the Station Adapter
 - Adjust the location of the Access Point
5. Proceed to setup the other workstations.

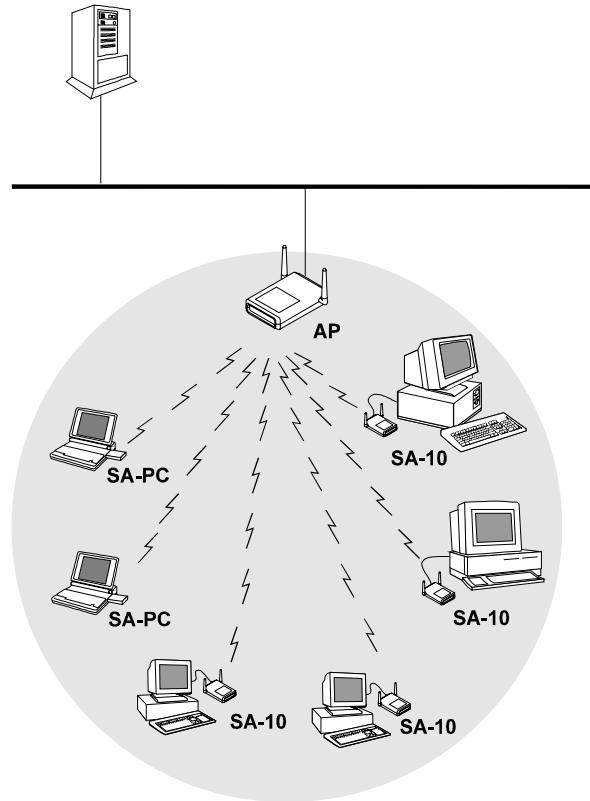


Figure 5.3: Single Cell Configuration

Disclaimer: This diagram is for illustrative purposes only. It should not be confused with the transceiver operating in a standalone mode. When this diagram is in use, the transceiver will be used in conjunction with amp model AMP-2440-250/500 and the antennas listed in this manual.

4.1.2. Overlapping Cell Configuration

When two adjacent Access Points are positioned close enough to each other, a part of the coverage area of Access Point #1 overlaps that of Access Point #2. This overlapping area has two very important attributes:

- Any workstation situated in the overlapping area can associate and communicate with either Access Point #1 or Access Point #2.
- Any workstation can move seamlessly through the overlapping coverage areas without losing its network connection. This attribute is called, *Seamless Roaming*.

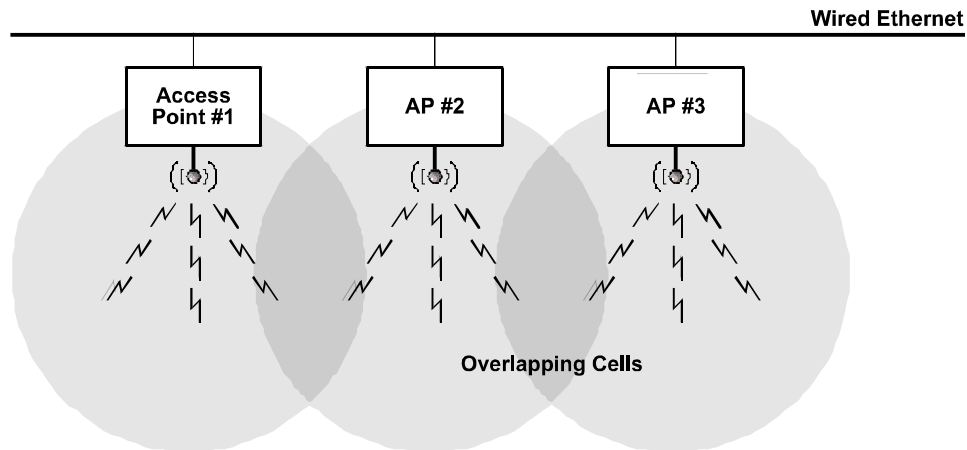


Figure 5.4: Three Overlapping Cells

To set up overlapping BreezeNET cells:

1. Install an Access Point (refer to section 2, *Basic Installation*). Be sure to position the Access Point as high as possible.
2. Install the second Access Point so that the two are positioned closer together than the prescribed distance (refer to section **Error!** **Reference source not found.**).
3. To allow roaming, configure all Access Points and stations adapters to the same ESSID.
4. To improve collocation and performance, configure all Access Points to different hopping sequences of the same hopping set.

5. Install a Station Adapter or SA-PCR Card on a workstation.
6. Position the wireless workstation approximately the same distance from the two Access Points.
7. Temporarily disconnect the **first** Access Point from the power supply. Verify radio signal reception from the first Access Point. View the LED indicators of the front panel of the Station Adapter, or the Site Survey application of the SA-PCR Card, to check signal strength of the first Access Point.
8. Disconnect the **second** Access Point from the power supply and re-connect the first Access Point. View the LED indicators of the front panel of the Station Adapter, or the Site Survey application of the SA-PCR Card, to check signal strength of the second Access Point.
7. If necessary, adjust the distance between the Access Points so the coverage areas overlap.
8. Continue setting up overlapping cells until the required area is covered.

***Note:** It is not necessary at this point to connect the Access Points to an Ethernet backbone, since Access Points continuously transmit signals (beacon frames) whether they are connected to an Ethernet backbone or not.*

4.1.3. Multicell Configuration

Areas congested by many users and a heavy traffic load may require a multicell structure. In a multicell structure, several Access Points are installed in the same location. Each Access Point has the same coverage area, thereby creating a common coverage area that increases aggregate throughput. Any workstation in the overlapping area can associate and communicate with any Access Point covering that area.

To set up a BreezeNET multicell:

1. Calculate the number of Access Points needed as follows: Multiply the number of active users by the required throughput per user, and divide the result by 1.5Mbps (net throughput supported by collocated Access Points). Consider the example of 5 active stations, each requiring 0.5 Mbps throughput. The calculation is $(5 * .5) / 1.5 = 1.6$. Two Access Points should be used. This method is accurate only for the first few Access Points.

The aggregate throughput of the common coverage area is equal to the number of co-located Access Points, multiplied by the throughput of each individual Access Point, minus a certain amount of degradation caused by the interference among the different Access Points.

2. Install several Access Points in the same location a few meters from each other so they cover the same area. Be sure to position the Access Points as high as possible.
3. To allow roaming and redundancy, configure all Access Points and stations adapters to the same ESSID.
4. To improve collocation and performance, configure all Access Points to different hopping sequences of the same hopping set.
5. Install Station Adapters or SA-PCR Cards on workstations.
6. Make sure that the *Load Sharing* option is activated. Stations will automatically associate with an Access Point that is less loaded and provides better signal quality.

Note: It is not necessary at this point to connect the Access Points to an Ethernet backbone, since Access Points continuously transmit signals (beacon frames) whether they are connected to an Ethernet backbone or not.

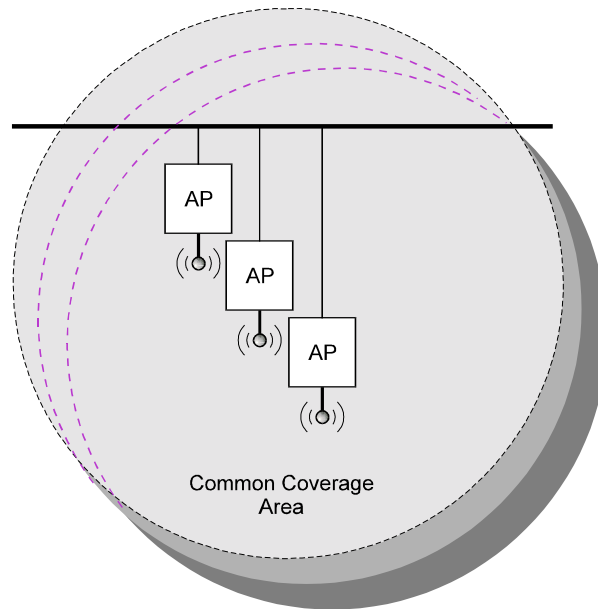


Figure 5.5: Multicell Configuration

4.1.4. Multi-hop Configuration (Relay)

When you want to connect two sites between which a line-of-sight does not exist, an AP-WB pair can be positioned at a third location where line-of-sight exists with each of the original locations. This third location then acts as a relay point.

In areas where a wired LAN backbone is not available, another AP can be added to the AP-WB relay to distribute a wireless backbone. In this way, the range of a wireless system can be extended.

System configuration is as follows:

To set up a BreezeNET multi-hop cell:

1. Install an AP at the main office (refer to section 2, *Basic Installation*).
2. Install a WB at the remote site (refer to section 2, *Basic Installation*).
3. Install an AP-WB pair in a high location that has a clear line of sight to both the main office and the remote site. Many AP-WB pairs can form a chain.
4. When an AP and WB communicate over the wireless LAN, set them both to the same ESSID. For example, set the AP of the main office and the WB of the first AP-WB relay pair to the same ESSID. Also, set the AP of the last AP-WB relay and the WB of the remote site to the same ESSID; this ESSID should be different from the first ESSID.

Another option is to use one ESSID, and to set the *Preferred AP* parameter of each WB to its paired AP (refer to section 3.4.3). This option allows stations to roam between the sites.

5. As usual, make sure that the *hopping sequence* of the Access Points are different.

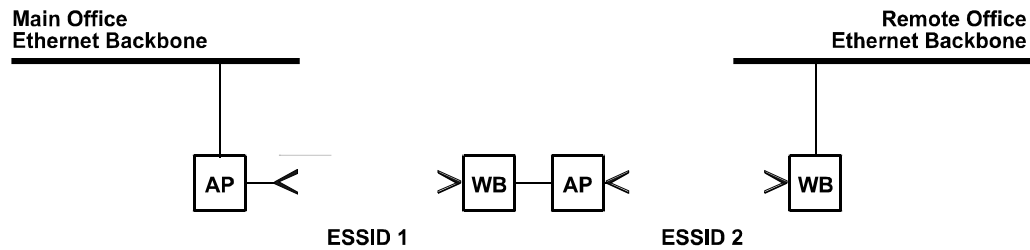


Figure 5.6: Multihop Configuration

6. If desired, an additional AP may be added at the main office and remote site, and between each AP-WB pair to provide wireless LANs at those points (see illustration).

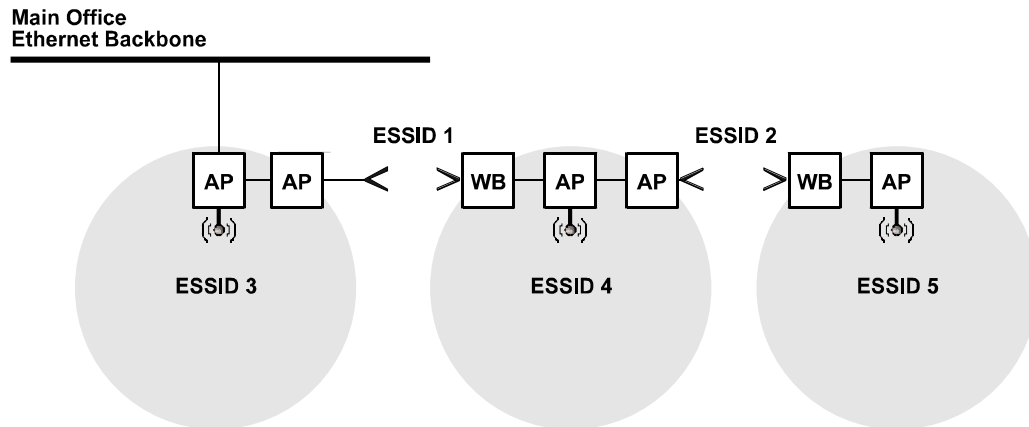


Figure 5.7: Advanced Multihop Configuration

7. Install Station Adapters or SA-PCR Cards on workstations (refer to section 2, *Basic Installation*).

4.2. Outdoor Installation Considerations

This chapter describes various considerations to take into account when planning an outdoor installation including site selection, antenna alignment, antenna diversity, antenna polarization, antenna seal, and cell size.

4.2.1. Site Selection Factors

When selecting a location for external antennas, remember to take into consideration the following guidelines:

- Minimum distance between sites
- Maximum height above the ground
- Maximum line of sight clearance
- Maximum separation between antennas (diversity option)

Path of Clearest Propagation

A propagation path is the path that signals traverse between the antennas of any two bridges. The “line” between two antenna sites is an imaginary straight line which may be drawn between the two antennas. Any obstacles in the path of the “line” degrade the propagation path. The best propagation path is, therefore, a clear line of sight with good clearance between the “line” and any physical obstacle.

Physical Obstacles

Any physical object in the path between two bridges can cause signal attenuation. Common obstructions are buildings and trees. If a bridge’s antenna is installed indoors, the walls and/or windows between the two sites are physical obstructions. If the antenna is positioned outdoors, any buildings or other physical structure such as trees, mountains or other natural geographic features higher than the antenna and situated in the path between the two sites can constitute obstructions.

Install indoor antennas as close as possible to a window (or wall if a window is not accessible) facing the required direction. Avoid metal obstacles such as metal window frames or metal film anti-glare windows in the transmission path. Install outdoor antennas high enough to avoid any obstacles which may block the signal.

Minimal Path Loss

Path loss is determined mainly by several factors:

- Distance between sites
Path loss is lower and system performance better when distances between sites are shorter.
- Clearance
Path loss is minimized when there exists a clear line of sight. The number, location, size, and makeup of obstacles determine their contribution to path loss.
- Antenna height
Path loss is lower when antennas are positioned higher. Antenna height is the distance from the imaginary line connecting the antennas at the two sites to “ground” level. “Ground” level in an open area is the actual ground. In dense urban areas, “ground” level is the average height of the buildings between the antenna sites.

4.2.2. Rooftop Installation

Warning: Rooftop antenna installations are extremely dangerous! Incorrect installation may result in death, serious injury and/or damage. Such installations should be performed by professional antenna installers only!

Rooftop installations offer several advantages:

- Increased antenna range.
- Less obstacles in path.
- Improved performance due to greater height.
- Reduced multipath problems.

4.2.3. Antennas for Outdoor Applications

The **BreezeNET PRO.11 Series** can be used in point-to-point or point-to-multipoint configurations.

4.2.3.1 Point-to-Point

A point-to-point link is based on the use of one Access Point with external antennas and one adapter (SA-10/40D, WB-10D). The AP and the WB must be equipped with one or two directional antennas. The necessary antenna gain depends on the required range and performance.

4.2.3.2 Point-to-Multipoint

Setting up a point-to-multipoint link requires the use of an AP-10D equipped with omni-directional antennas and a remote WB-10D (or SA-10/40D) equipped with high-gain directional antennas.

4.2.3.3 Antenna Alignment

Low gain antennas do not require alignment due to their very wide radiation pattern. High gain antennas have a narrow beamwidth necessitating an alignment procedure in order to optimize the link.

Check antenna alignment by using the LED indicators on the front panel of whichever adapter is used in the link (WB-10D or SA-10/40D). These LED indicators provide indication of reception quality.

To perform antenna alignment:

1. Assemble antennas according to the assembly instructions included with the antenna set.
2. Mount the antennas as high as possible.
3. Connect the coaxial cable to the AP at the main site.
4. Connect the coaxial cable to the WB (or SA) at the remote site.
5. Power on the AP and the WB (or SA).
6. Synchronize the units by aligning the antennas manually until the WLNK indicator LED on the front panel of the wireless Bridge and/or Station Adapter illuminates.
7. Align antennas at the main and remote sites until maximum signal quality is obtained. (Check QLT LEDs on the front panel of the Station Adapter and the wireless Bridge.)

If the received signal quality is lower than expected for this antenna/range combination, change antenna height and verify RF cables connections.

4.2.3.4 Antenna Diversity

In applications where no multipath propagation is expected, a single antenna is sufficient to ensure good performance levels. However, in cases where multipath propagation exists, BreezeCOM recommends that two antennas be used. This takes advantage of space diversity capabilities. By using two antennas per unit, the system can select the best antenna on a per-packet basis (every several milliseconds).

Multipath propagation is to be expected when there are potential reflectors between the main and remote sites. These reflectors may be buildings or moving objects such as airplanes and motor vehicles. If this is the case, the radio signal does not travel in a straight line, but is reflected or deflected off of the object, creating multiple propagation paths.

When installing a single antenna, modify the *transmit antenna* option to either antenna 1 or antenna 2, according to the antenna being used (refer to section 3.4.3). Note: Only antennas from Table 1 FCC Type Acceptance Configurations can be used.

4.2.3.5 Antenna Polarization

Antenna polarization must be the same at either end of the link. In most applications, the preferred orientation is vertical polarization. Above-ground propagation of the signal is better when it is polarized vertically. To verify antenna polarization, refer to the assembly instructions supplied with the antenna set.

4.2.4. Antenna Seal

When using outdoor antennas, you must seal the antenna connectors against rain. Otherwise the antennas are not suitable for use in outdoor installations.

4.2.5. Cell Size

Cell size is determined by the maximum possible distance between the Access Point and the Station Adapter, usually related to point-to-multipoint installations using external antennas. For open outdoor areas with an unobstructed line of sight between the Access Point and the BreezeNET

PRO.11 workstation, the suggested maximum distance between Access Point and workstation is:

Standard AP-10 PRO.11700m (2000 ft.)

4.2.6. Link Distance

Link distance is the maximum distance between the AP and the station adapter, usually related to point-to-point installations using external antennas. For open outdoor areas with an unobstructed line of sight between the Access Point and the wireless bridge, the suggested maximum distance is:

AP-10D PRO.11 with external antennasup to 10Km (7 miles) in the USA

Note: *The maximum distance of 10Km/7 miles is achieved using 24 dBi antennas.*

4.2.7. Using Outdoor Range Tables

Outdoor installations must have a clear line-of-sight. Solid obstacles such as buildings or hills prevent the establishment of a link. Partial obstacles such as trees or traffic can reduce range. Extending coaxial cables can cause an increase in assembly signal loss and a reduction in range.

The ranges in the following tables are attained under good propagating conditions when using the standard cables supplied in the antenna set. Actual ranges may vary due to specific multipath and interference conditions.

For specific range guidelines and information about extending cables, consult your local dealer or BreezeCOM central offices.

Ranges are subject to change without notice.

4.3. Precautions

4.3.1. Professional Installers Only

Caution: *Detached antennas, whether installed indoors or out, should be installed ONLY by experienced antenna installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities.*

Failure to do so may void the BreezeNET Product Warranty and may expose the end user to legal and financial liabilities. BreezeCOM and its resellers or distributors are not liable for injury, damage or violation of government regulations associated with the installation of detached antennas.

4.3.2. Transmit Antenna Gain

Regulations regarding maximum antenna gains vary from country to country. It is the responsibility of the end user to operate within the limits of these regulations and to ensure that the professional installer is aware of these regulations, as well. The FCC in the United States and ETSI in Europe limit effective transmit power to 36dBm (USA) and 20dBm (Europe). The maximum total assembly gain of antennas and cables in this case equals 19dBi (USA) and 3dBi (Europe).

Violation of government regulations exposes the end user to legal and financial liabilities. BreezeCOM and its resellers and distributors shall not be liable for expense or damage incurred as a result of installations which exceed local transmit gain limitations.

4.3.3. Spurious Radio Frequency Emissions

The regulations referred to in the previous section also specify maximum “out-of-band” radio frequency emissions. Install a filter as close as possible to the BreezeNET PRO.11 “D” model unit connector.

4.3.4. Lightning Protection

Lightning protection is designed to protect people, property and equipment by providing a path to ground for the lightning's energy. The lightning arrester diverts the strike energy to ground through a deliberate and controlled path instead of allowing it to choose a random path. Lightning protection for a building is more forgiving than protection of electronic devices. A building can withstand up to 100,000 volts, but electronic equipment may be damaged by just a few volts.

Lightning protection entails connecting an antenna discharge unit (also called an arrester) to each cable as close as possible to the point where it enters the building. It also entails proper grounding of the arrestors and of the antenna mast (if the antenna is connected to one).

The lightning arrester should be installed and grounded at the point where the cable enters the building. The arrester is connected to the unit at one end and to the antenna at the other end.

The professional installer you choose must be knowledgeable about lightning protection. The installer must install the lightning protector in a way that maximizes lightning protection. BreezeCOM offers the following high-quality lightning arrester assembly:

BreezeNET AL 1 Lightning Arrester - Part No. 872905 5 ft (1.5m), "N" Male to "N" Female.

4.3.5. Rain Proofing

12, 18, and 24 dBi antennas must be sealed against rain at the point the cable enters the pole before they are suitable for external use.

5. ACCESSORY INSTALLATION

This chapter introduces some of the accessories available for specific installations, and describes how to install them.

5.4. AL 1 Lightning Arrestor

The AL 1 Lightning Arrestor is used to protect transmitters and receivers from transients originating from lightning or EMP.

The AL 1 is gas tube-based and is not radioactive. The gas discharge tube can sustain several transients if the time period between transients is sufficient to allow the tube to cool down.

For technical specifications, refer to section 8.2.2, *Specifications for AL 1 Lightning Arrestor*.

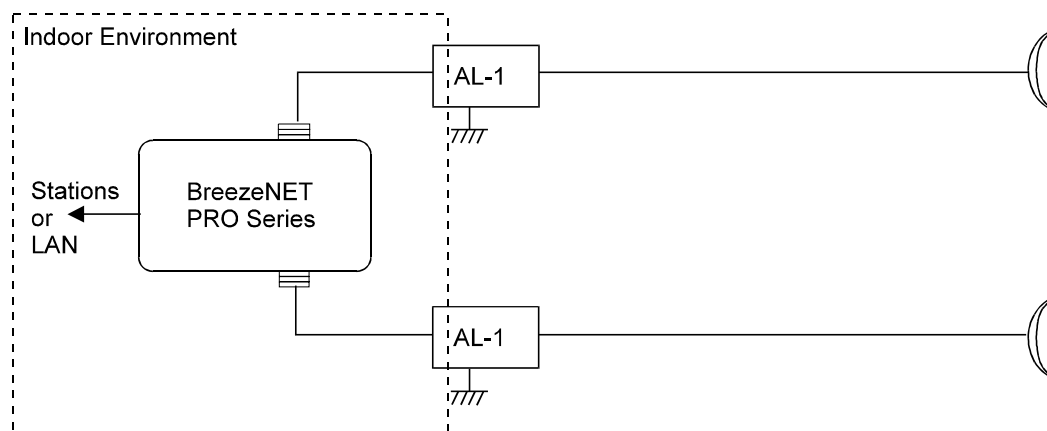


Figure 6.4: AL-1 Connection Block Diagram

One of the female-type N connectors is mounted directly through a hole in the shelter wall and held in place with a lockwasher and nut.

6. UPGRADE PROCEDURE

Firmware upgrades to the unit's flash memory is done by a simple download procedure using a TFTP application. Before beginning an upgrade, *be sure you have the correct files and latest instructions*. Upgrade packages can be obtained at the BreezeCOM web site: www.breezecom.com.

In general terms, upgrading includes the following steps:

1. Set up an IP connection to the device. You can verify working connection using the Ping command.
2. Run TFTP software and connect to the device.
3. Use TFTP to download the erase file to the device Use the tables below to determine the specific file to use, according to the unit's current version. This causes the flash memory to be cleared. **Do not reset the device now.**
4. Use TFTP to download the software file to the device. Use the tables below to determine the specific file to use, according to the unit's current version.
5. The unit resets itself and comes up with the new upgraded version.

Table 7.1: Upgrade Files

Current Version of Unit	Flash Erase File Name	Software Download File Name	
		AP-10	SA-10, SA-40, WB-10
3.2, 3.38, 3.42, 3.50	download	eanaf	eansf
3.52, 4.204	erase	eanafb	eansfb
3.62, 4.211, 4.310	erase_fw	ap_fw	sawb_fw

The *current* version and type of the unit determine the files used for upgrade. For example, when upgrading an AP-10 from version 3.52 to version 4.310, use the *erase* and *eanafb* files.

When upgrading a SA-10 from version 3.62 to version 4.310, use the *erase_fw* and *sawb_fw* files.

When upgrading an AP-10 from version 4.211 to version 4.310, use the *erase_fw* and *ap_fw* files.

7. SYSTEM TROUBLESHOOTING

The following troubleshooting guide provides answers to some of the more common problems which may occur when installing, and using **BreezeNET PRO.11 Series** products. If problems not mentioned in this guide should arise, checking the Ethernet and WLAN counters may help (see section 3.6.1). If the problem persists, please feel free to contact your local distributor or the BreezeCOM Technical Support Department.

8.1. Troubleshooting Guide

Problem and Indication	Possible Cause	Corrective Action
No Power to Unit. PWR LED is off.	<ol style="list-style-type: none"> 1. Power cord is not properly connected. 2. Power supply is defective. 	<ol style="list-style-type: none"> 1. Verify power cord is properly connected to the BreezeNET unit and to the power outlet. 2. If this is not the cause, replace the power supply.
Failure to establish wireless link. WLNK LED is off and unit resets every few minutes.	<ol style="list-style-type: none"> 1. Power supply to units may be faulty 2. The units may not have the same ESSID as the AP-10. 	<ol style="list-style-type: none"> 1. Verify power to units (AP and SA/ WB). 2. Verify that all units in the network have the same ESSID as the AP (ESSID must be identical in all units in the network): 3. Verify wireless link: <ul style="list-style-type: none"> • Set AP and unit (SA or WB) side by side. • Power on each unit and see if a wireless link is established (even "D" models without their external antennas should establish a link if placed side by side with the AP). • If the units fail to associate, reset units to factory default values reset unit (see section 3.4.5). The units should now establish a wireless link.
Failure to establish wireless link ("D" models/external antennas)	<ol style="list-style-type: none"> 1. Power supply to units may be faulty. 2. Cables may be improperly connected 3. There may be some problem with antenna installation. 	<ol style="list-style-type: none"> 1. Verify power to units. 2. Verify that all cables are connected securely. 3. Refer to previous section and verify wireless link between the units. 4. Verify that the antenna(s) are properly installed (see relevant section in this manual): <ul style="list-style-type: none"> • Check antenna alignment. • Verify that antenna polarization is the same at both ends. • Verify that the range matches specifications. • Verify line-of-sight/antenna alignment/antenna height.
Wireless link established, but there is no Ethernet activity (AP and WB units).	<ol style="list-style-type: none"> 1. Ethernet hub port or UTP cable is faulty. 2. Ethernet port in unit is faulty. 	<ol style="list-style-type: none"> 1. Check that the LINK LED is on and solid at the hub port. If this is not the case, the port is inactive. Try another port on the hub or another UTP cable. 2. Verify that Ethernet port in unit is working. Ping unit to verify Ethernet connection. 3. Verify that you are using a cross-over UTP cable (pins 1

Problem and Indication	Possible Cause	Corrective Action
		& 3, 2 & 6) if connected directly to workstation, or a straight-through cable if connected to a hub. 4. Check ETHR LED indicator in unit and Ethernet counters in Monitor to verify Ethernet activity.
Wireless link established, but there is no Ethernet activity (SA-10 and SA-40 units).	1. Ethernet port on Network Interface card is faulty. 2. Ethernet port of unit is faulty. 3. UTP cable is faulty.	1. Verify that the LINK LED is lit and solid at the NIC port. If this is not the case, the port is inactive. Try using another UTP cable or another workstation. 2. Ping the unit to check the Ethernet port. If you cannot ping the unit, this may indicate failure of cable, Ethernet port of unit or Ethernet port of workstation's NIC. Change UTP cable and retry. If you still cannot ping the unit, exchange units and try to ping the new unit using the same NIC and cable.
No network detected at Station Adapter (SA-10, SA-40) workstation.	1. Workstation networking is improperly configured. 2. UTP cable connection is faulty. 3. Failure to pass Ethernet packets.	1. Reset both Access Point and Station Adapter. <ul style="list-style-type: none"> • Re-establish network connection. • Verify proper workstation network configuration. 2. Try to ping the remote network. Failure to detect the network may indicate a failure to pass Ethernet packets. 3. Verify UTP cable connection. Solid LINK LED in workstation NIC indicates proper Ethernet connection. 4. Check monitor messages for errors or other indications of problems. 5. Check station counters to verify increase in Ethernet counters which indicates Ethernet activity.
High quality signal but throughput is poor.	1. Too much interference or multipath propagation. 2. Ethernet port of the unit may be faulty.	1. Move the unit or the antennas out of the range of interference. <ul style="list-style-type: none"> • Check counters to see if more than 10% of total transmitted frames are retransmitted fragments. • Check if more than 10% of total received data frames are bad fragments. 2. Verify Ethernet port activity by checking Ethernet counters.
Link signal quality low or not as good as expected (indoor installation).	1. Possible multipath or structural interference.	Reposition the unit outside range of possible interference. <ul style="list-style-type: none"> • Check for heavy metal structures (e.g. elevators, racks, file cabinets) near unit. • Check counters for excessive retransmissions or received bad fragments. • Site may require higher gain antennas. • site may require a multicell structure (multiple AP units) due to multipath/structural interference.
Link signal quality low or not as good as expected (outdoor installation).	There may be a problem with certain aspects of outdoor installation considerations (see relevant section in <i>this manual</i>).	Refer to section 4.2, <i>Outdoor Installation Considerations</i> : <ul style="list-style-type: none"> • Verify that there is a clear line-of-site. • Verify antenna height. • Verify antenna polarization. • Verify antenna alignment. • Check length of cable between antenna and unit (an overly long extension cable may adversely affect performance).
Unit associates with the wrong	In a multicell structure with	For a unit to associate with a specific Access Point, assign

Problem and Indication	Possible Cause	Corrective Action
Access Point.	overlapping cells, the units may not associate with the closest Access Point.	a unique ESSID to the Access Point and to all the units you want to include in that wireless network.
Reduced performance in a multi-AP configuration.	The APs in the same coverage area have not been assigned unique hopping sequences.	Assign a unique hopping sequence to each AP in the coverage area. Each AP must have a unique hopping sequence regardless of ESSID.
Rx / Tx calibration error messages.	Auto Calibration is enabled for a "DE" unit.	Disable Auto Calibration for the unit (refer to section 3.5).

8.2. Checking Counters

Checking counters is also a good way to pinpoint any problems that may occur in the **BreezeNET** wireless LAN. Counters can be checked from the monitor. See section **Error! Reference source not found.**

8.2.1. WLAN Counters

When checking WLAN counters, total retransmitted fragments should be below 10% of total transmitted (bridge) frames. If total retransmitted fragments are above 10%, this indicates errors in data transmission. Too many retransmissions may be an indication of interference between the transmitting and receiving units. Also, the ratio between Frames Dropped (too many retries) and Total Transmitted Frames (Bridge) should not exceed 1:40 (2.5%)

Received bad fragments should be no more than 10% of the total received data frames. If more than 10% of the total received data frames are bad fragments, this may indicate that there is a problem with the wireless link.

Refer to the Troubleshooting guide (section 7) above for possible corrective action.

8.2.2. Ethernet Counters

When checking the Ethernet counters, received bad frames should be zero (0). If this is not the case, this may indicate a problem with the Ethernet connection. Verify Ethernet port link at hub, workstation, and unit. Assign a unique IP address to the unit and ping.

8. APPENDIX

This appendix includes the following sections:

- **Supported MIBs and Traps** – Lists MIBs and traps supported by *BreezeNET PRO.11 Series* products.
- **Technical Specifications** – Lists product and attachment specifications.
- **Wireless LAN Concepts** – Provides an overview of the concepts related to wireless LANs.
- **Radio Signal Propagation** – Discusses the concepts and applications of radio signal propagation relevant to wireless LANs.
- **IEEE 802.11 Technical Tutorial** – Introduces the new 802.11 standard.

8.1. Supported MIBs and Traps

This chapter lists MIBs and traps supported by *BreezeNET PRO.11 Series* products.

8.1.1. Supported MIBs

All products in the *BreezeNET PRO.11 Series* as well as the Extended Range Access Point (AP-10 DE) and Workgroup Bridge (WB-10 DE) contain an embedded SNMP (Simple Network Management Protocol) agent. All functions can be accessed from the Management Information Base (MIB) using an SNMP application.

BreezeNET PRO.11 Series agents support the following MIBs:

- MIB-II (RFC1213)
- BRIDGE-MIB (RFC1286)
- BreezeCOM Private MIB

The BreezeCOM Private MIB can be viewed by opening the MIB file on the provided diskette.

8.1.2. Supported Traps

The following traps are implemented by BreezeNET PRO.11 units. All BreezeNET PRO.11 units with enabled Trap Sending will send traps to the network's designated managers. The traps can be viewed and filtered using SNMPc.

To enable/disable Trap Sending for a device, use the *IP and SNMP Parameters* menu (see section 3.4.2).

The following table lists the traps implemented by BreezeCOM PRO.11 units:

Trap	Variables	Description
brzAProamingIn	brzTrapSTAMacAddr	A station has roamed into this AP coverage area. The trap contains the MAC address of the associated station.
brzAPAssociated	brzTrapSTAMacAddr	A new station is associated with this AP. The trap contains the MAC address of the associated station.
brzAPdisassociated	brzTrapSTAMacAddr	A station has disassociated itself from this AP. The trap contains the MAC address of the associated station.
brzAPaging	brzTrapSTAMacAddr	A station association was aged out and removed from this AP. The trap contains the MAC address of the aged-out station.
brzAProamedout	brzTrapSTAMacAddr	A station has roamed out of this AP's range. The trap contains the MAC address of the station that roamed out.
brzSTAassociated	brzLastAPMacAddr brzTrapAPMac brzTrapLastRssiQuality brzTrapRssiQuality	A station has become associated with, or roamed to, a new AP. The trap contains the MAC address and average RSSI level of the new AP (<i>TrapAPMac</i> and <i>TrapRssiQuality</i> variables). If the station has been roaming, the MAC address of the old AP and the RSSI level prior to roaming are also provided (<i>LastAPMacAddr</i> and <i>LastRssiQuality</i> variables). For an association, the second address appears as all zeros.
brzWlanStatus	brzTrapToggle brzTrapMacAddress	The wireless media condition has changed. An ON value is sent when the wireless LAN quality for a station or AP drops below the WLAN trap threshold. An OFF value is sent if the quality improves beyond the threshold. The current value of wireless LAN quality is also sent.
brzWlanStatusOfStation	brzTrapToggle brzTrapMacAddress	The quality of the wireless connection to the AP has changed. An ON value is sent when the connection goes lower than the predetermined threshold. An OFF value is sent when the quality improves above the threshold. The <i>brzTrapMacAddress</i> variable contains the MAC address of the applicable station.
brzGeneral	brzTrapIndex brzTrapText	For future use.

8.2. Technical Specifications

8.2.1. Specifications for BreezeNET PRO.11 Units

The following table provides the technical specifications for all products in the *BreezeNET PRO.11 Series*.

Technical Specifications	AP-10 PRO.11, SA-10/40 PRO.11, WB-10 PRO.11	
Wired LAN interface		
Compliant with	Ethernet / IEEE 802.3 CSMA/CD standard	
Physical Interface	10BaseT	
Network Operating Systems supported	All	
Network protocols supported	All	
Wireless LAN interface		
Compliant with	IEEE 802.11 CSMA / CA Wireless LAN standard	
Physical interface – two antennas	Integrated or External	
Radio Specifications		
Type	Frequency Hopping Spread Spectrum (FHSS)	
Frequency range	2.4 GHz – 2.4835 GHz (ISM band) (different ranges available for countries using other bands)	
Dwell time	32, 64, 128 ms	
Transmitted power: - integrated antennas	Up to 100 mW (20dBm) EIRP	
Transmitted power: - external antennas	D models: - High Power (at the connector): 17dBm (50mW) - Low Power (at the connector): 4dBm (25 mW)	
	DE models: At the connector: 0.01mW (-2dBm)	
Sensitivity - @ 1 Mbps - @ 2 Mbps - @ 3 Mbps	- 81 dBm - 75 dBm - 67 dBm	
Modulation	Multilevel GFSK	
Demodulation Technology	DSP-based with adaptive equalization	
Antenna Diversity	Two antennas, selected for use on a packet basis	
Frequency Accuracy	+/- 10 PPM	
Approvals of Compliance	FCC part 15, ETS 300-328, UL, UL/C, TUV/GS, CE	

Technical Specifications	Access Points AP-10 PRO.11	Station Adapters SA-10/40 PRO.11	Ethernet Bridges WB-10 PRO.11	
Configuration and Management				
Configuration and Setup	Via Local Monitor port (serial RS-232)			
SNMP management	MIB II, Bridge MIB, WLAN MIB, and private MIB			
- SNMP agents				
- Access via	Wired LAN, Wireless LAN			
Site Survey	Via Local Monitor port (serial RS-232) Via SNMP			
Front Panel Display LED indicators	- Power on - Wired LAN activity - Wireless LAN synchronization - Wireless LAN signal quality/Load			
S/W upgradeable	Through TFTP download			
System Considerations				
Range (Access Point to Station)	Depends on rate and antenna cable length/quality. (Accurate values must be calculated for specific installations.) Refer to section 4.2.7, <i>Using Outdoor Range Tables</i> .			
- Range - unobstructed with integrated antennas	2000 ft. (600m)			
- Range - unobstructed with external antennas (models D and DE)	USA FCC - up to 6 miles Europe ETSI - up to 2.5 km Europe ETSI (DE model only) - up to 5 km Non-Regulated - 30 km and above			
- Range - Office Environment	Up to 500 ft. (150m)			
Maximum no. of APs per wired LAN	Unlimited			
Maximum no. of co-located (overlapping) cells (Access Points)	15			
Data Rate	- over the air - nominal net - aggregate			
	1, 2, or 3 Mbps Up to 2 Mbps Over 5 Mbps with overlapped cells			
High Speed roaming	up to 60 mph (90 kph)			
Load sharing support	yes (with WIX™)			
Dynamic rate selection based on radio medium quality	Yes			

Technical Specifications	Access Points AP-10 PRO.11	Station Adapters SA-10/40 PRO.11	Ethernet Bridges WB-10 PRO.11	
Electrical				
External Power Supply	100V - 250V, 50-60Hz, 0.5A			
Input Voltage	5Vdc			
Power Consumption	1.5A (peak) 1.2A (average)			
Dimensions (without antennas and power supply)	5.1" x 3.4" x 1.35" (13cm x 8.6cm x 3cm)			
Weight (without antennas and power supply)	0.9 lb. (0.4 kg.)			
Environmental				
Operating Temperature	32° F - 105° F (0° C - 40° C)			
Operating Humidity	5% - 95% non-condensing			

Note: All specifications are subject to change without notice.

8.2.2. Specifications for AL 1 Lightning Arrestor

Turn on voltage	75V
Insertion loss	0.3dB typical
DC path from input to output	existing
Operating Temperature	-55° C to +70° C
Dimensions	67.5mm x 25mm x 25mm (2.7" x 1" x 1")
Connectors	<ul style="list-style-type: none"> • Antenna Port: N-type, Female • Equipment Port: N-type, Female
Operating Environment	Indoor/Outdoor
Grounding	One of the female-type N connectors is mounted directly through a hole in the shelter wall and held in place with a lockwasher and nut.

Note: All specifications are subject to change without notice.

8.3. Wireless LAN Concepts

Wireless LAN technology is becoming increasingly popular for a wide variety of applications. After evaluating the technology, users are convinced of its reliability, more than satisfied with its performance, and are ready to use it for large-scale and complex wireless networks.

Originally designed for indoor office applications, today's wireless LANs can be used for both indoor client-server and peer-to-peer networks as well as for outdoor point-to-point and point-to-multipoint remote bridging applications.

Wireless LANs are designed to be modular and very flexible. They can also be optimized for different environments. For example, point-to-point outdoor links are less susceptible to interference and can have higher performance if designers increase the "dwell time" and disable the "collision avoidance" and "fragmentation" mechanisms described later in this section.

Topology

Wired LAN Topology

Traditional LANs (Local Area Networks) link PCs and other computers to one another and to file servers, printers and other network equipment using cables or optic fibers as the transmission medium.

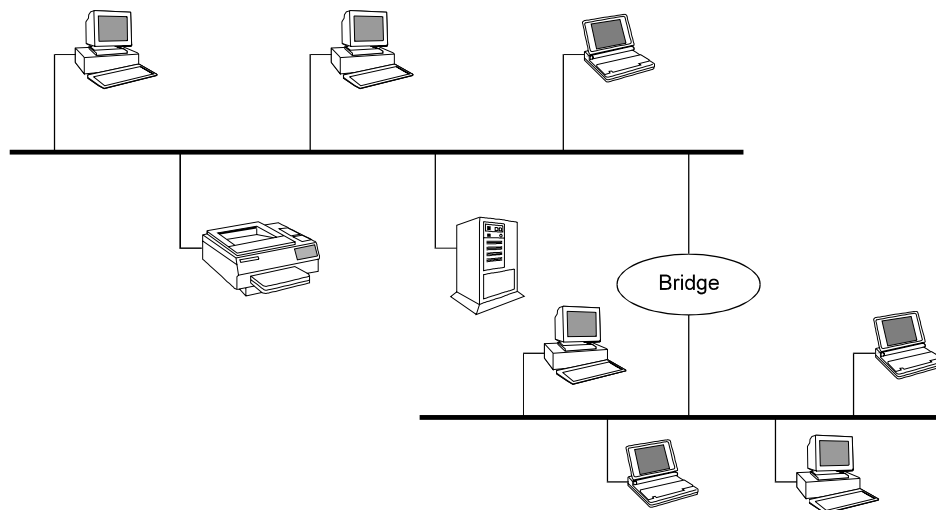


Figure 9.1: Wired LAN Topology

Wireless LAN Topology

Wireless LANs allow workstations to communicate and to access the network using radio propagation as the transmission medium. Wireless LANs can be connected to existing wired LANs as an extension, or can form the basis of a new network. While adaptable to both indoor and outdoor environments, wireless LANs are especially suited to indoor locations such as office buildings, manufacturing floors, hospitals and universities.

The basic building block of the wireless LAN is the Cell. This is the area in which wireless communication takes place. The coverage area of a cell depends on the strength of the propagated radio signal and the type and construction of walls, partitions and other physical characteristics of the indoor environment. PC-based workstations, notebook and pen-based computers can move freely in the cell.

Disclaimer: This diagram is for illustrative purposes only. It should not be confused with the transceiver operating in a standalone mode. When this diagram is in use, the transceiver will be used in conjunction with amp model AMP-2440-250/500 and the antennas listed in this manual.

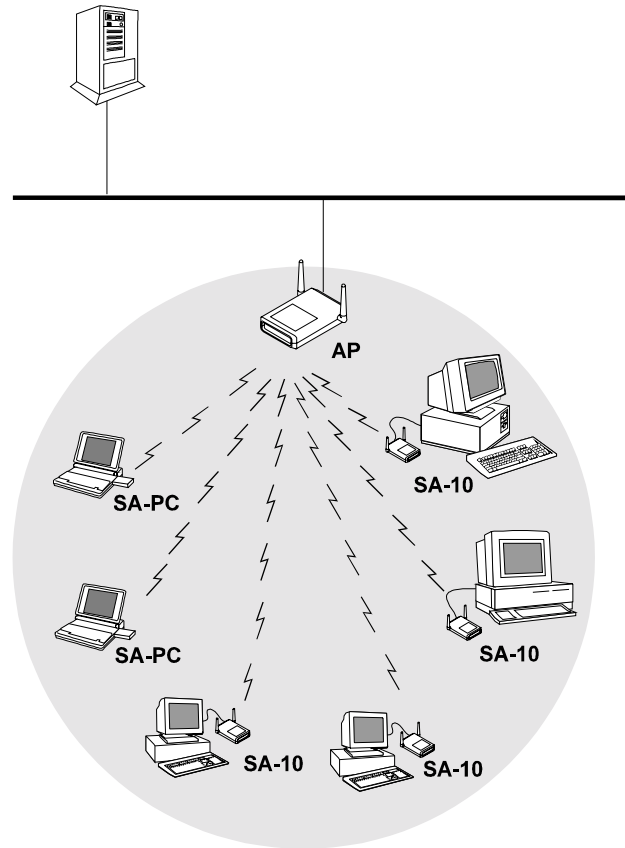


Figure 9.2: The Basic Wireless LAN Cell

Each wireless LAN cell requires some communications and traffic management. This is coordinated by an Access Point (AP) which communicates with each wireless station in its coverage area. Stations also communicate with each other via the AP, so communicating stations can be hidden from one another. In this way, the AP functions as a relay, extending the range of the system.

The AP also functions as a bridge between the wireless stations and the wired network and the other wireless cells. Connecting the AP to the backbone or other wireless cells can be done by wire or by a separate

wireless link, using wireless bridges. The range of the system can be extended by cascading several wireless links, one after the other.

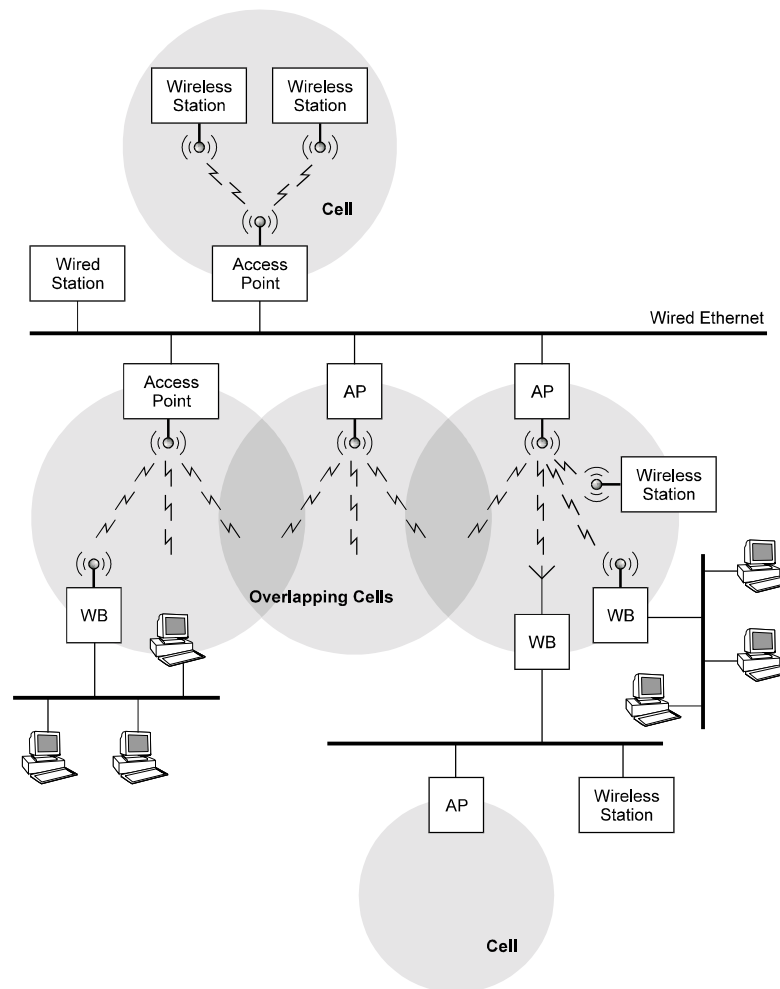


Figure 9.3: Wireless LAN Connectivity

Roaming

When any area in the building is within reception range of more than one Access Point, the cells' coverage is said to overlap. Each wireless station automatically establishes the best possible connection with one of the Access Points. Overlapping coverage areas are an important attribute of the wireless LAN setup, because this enables seamless roaming between overlapping cells.

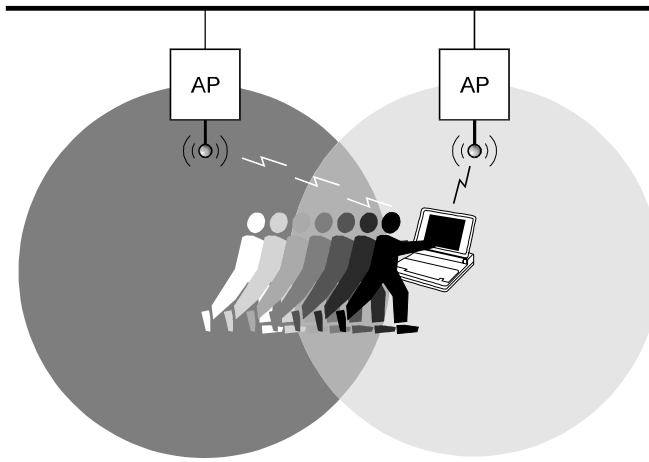


Figure 9.4: Roaming Through Overlapping Cells

Roaming allows mobile users with portable stations to move freely between overlapping cells, constantly maintaining their network connection. Roaming is seamless: a work session can be maintained while moving from one cell to another. Multiple Access Points can provide wireless coverage for an entire building or campus. When the coverage area of two or more APs overlap, the stations in the overlapping area can establish the best possible connection with one of the APs, continuously searching for the best AP. In order to minimize packet loss during switchover, the “old” and “new” APs communicate to coordinate the process.

Load Balancing

Congested areas with many users and heavy traffic load per unit may require a multi-cell structure. In a multi-cell structure, several co-located APs “illuminate” the same area creating a common coverage area which increases aggregate throughput. Stations inside the common coverage area automatically associate with the AP that is less loaded and provides the best signal quality. The stations are equally divided between the APs in order to equally share the load between all APs. Efficiency is maximized because all APs are working at the same low level load. Load balancing is also known as load sharing.

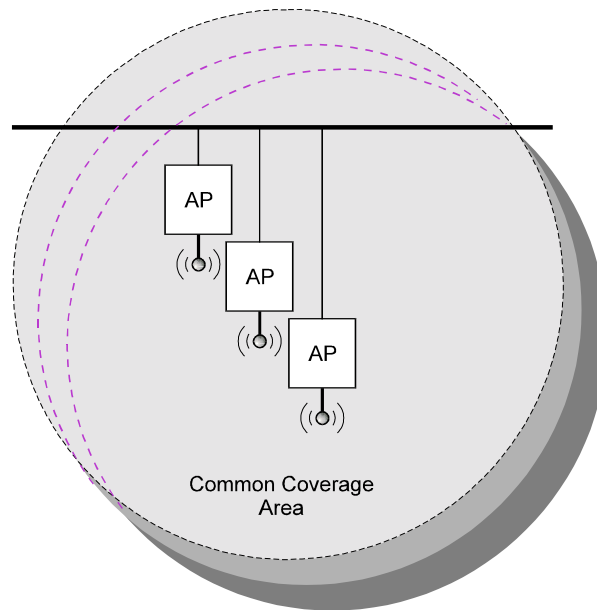


Figure 9.5: The Common Coverage Area of a Multi-cell Structure

Dynamic Rate Switching

The data rate of each station is automatically adjusted according to the received signal quality. Performance (throughput) is maximized by increasing the data rate and decreasing re-transmissions. This is very important for mobile applications where the signal quality fluctuates rapidly, but less important for fixed outdoor installations where signal quality is stable.

Media Access

When many users are located in the same area, performance becomes an issue. To address this issue, wireless LANs use the Carrier Sense Multiple Access (CSMA) algorithm with a Collision Avoidance (CA) mechanism in which each unit senses the medium before it starts to transmit.

If the medium is free for several microseconds, the unit can transmit for a limited time. If the medium is busy, the unit will back off for a random time before it senses again. Since transmitting units compete for air time, the protocol should ensure equal fairness between the stations.

Fragmentation

Fragmentation of packets into shorter fragments adds protocol overhead and reduces protocol efficiency when no errors are expected, but reduces the time spent on re-transmissions if errors are likely to occur. No fragmentation or longer fragment length adds overhead and reduces efficiency in case of errors and re-transmissions (multi-path).

Collision Avoidance

To avoid collisions with other incoming calls, each station transmits a short RTS (Request To Send) frame before the data frame. The Access Point sends back a CTS (Clear To Send) frame with permission to start the data transmission. This frame includes the time that this station is going to transmit. This frame is received by all the stations in the cell, notifying them that another unit will transmit during the following Xms, so they can not transmit even if the medium seems to be free (the transmitting unit is out of range).

Channelization

Using Frequency Hopping Spread Spectrum (FHSS), different hopping sequences are assigned to different co-located cells. Hopping sequences are designed so different cells can work simultaneously using different channels.

Since hopping sequences and hopping timing of different cells cannot be synchronized (according to FCC regulations), different cells might try to use the same channel occasionally. Then, one cell uses the channel while the other cell backs off and waits for the next hop. In the case of a very noisy environment (multiples and interference), the system must hop quickly. If the link is quiet and clean, it is better to hop slowly, reducing overhead and increasing efficiency.

8.4. Radio Signal Propagation

8.4.1. Introduction

This section explains and simplifies many of the terms relating to antennas and RF (Radio Frequency) used when dealing with an RF installation system.

The following diagram depicts a typical radio system:

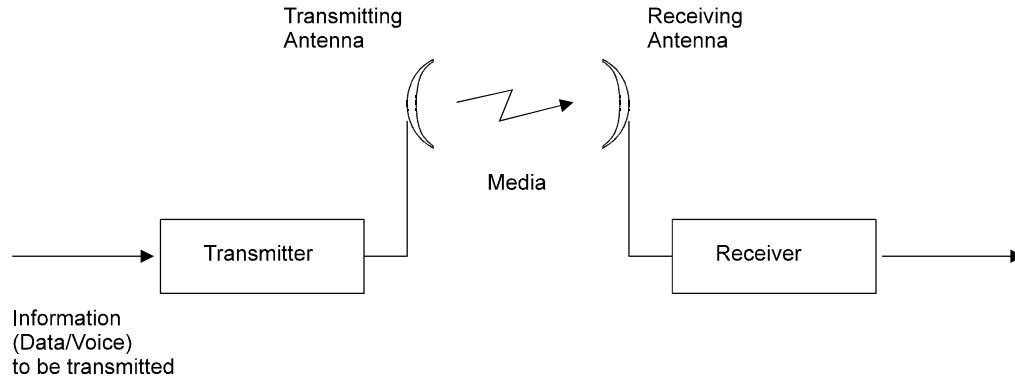


Figure 9.6: A Typical Radio System

A radio system transmits information to the transmitter. The information is transmitted through an antenna which converts the RF signal into an electromagnetic wave. The transmission medium for electromagnetic wave propagation is free space.

The electromagnetic wave is intercepted by the receiving antenna which converts it back to an RF signal. Ideally, this RF signal is the same as that originally generated by the transmitter. The original information is then demodulated back to its original form.

8.4.2. RF Terms and Definitions

dB

The dB convention is an abbreviation for decibels. It is a mathematical expression showing the relationship between two values.

RF Power Level

RF power level at either the transmitter output or the receiver input is expressed in Watts. It can also be expressed in dBm. The relation between dBm and Watts can be expressed as follows:

$$P_{\text{dBm}} = 10 \times \text{Log } P_{\text{mw}}$$

For example: 1 Watt = 1000 mW; $P_{dBm} = 10 \times \text{Log } 1000 = 30 \text{ dBm}$
 100 mW; $P_{dBm} = 10 \times \text{Log } 100 = 20 \text{ dBm}$

For link budget calculations, the dBm convention is more convenient than the Watts convention.

Attenuation

Attenuation (fading) of an RF signal is defined as follows:

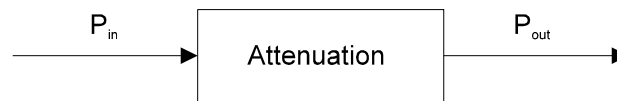


Figure 9.7: Attenuation of an RF signal

P_{in} is the incident power level at the attenuator input

P_{out} is the output power level at the attenuator output

Attenuation is expressed in dB as follows:

$$P_{dB} = -10 \times \text{Log} (P_{out}/P_{in})$$

For example: If, due to attenuation, half the power is lost ($P_{out}/P_{in} = 1/2$),
 attenuation in dB is $-10 \times \text{Log} (1/2) = 3_{dB}$

Path Loss

Loss of power of an RF signal travelling (propagating) through space. It is expressed in dB. Path loss depends on:

- The distance between transmitting and receiving antennas
- Line of sight clearance between the receiving and transmitting antennas
- Antenna height

Free Space Loss

Attenuation of the electromagnetic wave while propagating through space. This attenuation is calculated using the following formula:

$$\text{Free space loss} = 36.5 + 20 \times \text{Log}(F_{\text{MHz}}) + 20 \times \text{Log}(D_{\text{Mile}})$$

F is the RF frequency expressed in Mhz.

R is the distance between the transmitting and receiving antennas.

At 2.4 GHz, this formula is: $105+20 \times \text{Log}(D_{\text{Mile}})$

Antenna Characteristics

Isotropic Antenna

A hypothetical, lossless antenna having equal radiation intensity in all directions. Used as a zero dB gain reference in directivity calculation (gain).

Antenna Gain

A measure of directivity. It is defined as the ratio of the radiation intensity in a given direction to the radiation intensity that would be obtained if the power accepted by the antenna was radiated equally in all directions (isotropically). Antenna gain is expressed in dBi.

Radiation Pattern

A graphical representation in either polar or rectangular coordinates of the spatial energy distribution of an antenna.

Side Lobes

The radiation lobes in any direction other than that of the main lobe.

Omni-directional Antenna

Radiates and receives equally in all directions in azimuth. The following diagram shows the radiation pattern of an omnidirectional antenna with its side lobes in polar form.

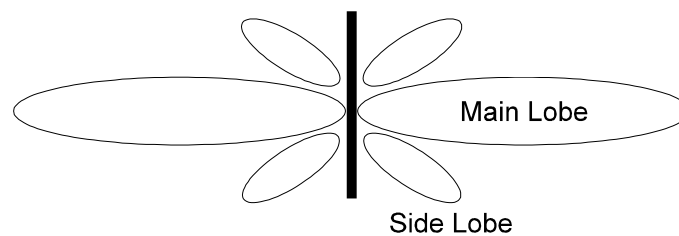


Figure 9.8: Side View

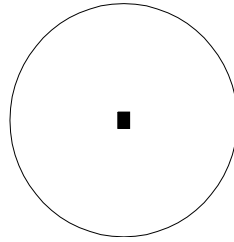


Figure 9.9: Top View

Directional Antenna

Radiates and receives most of the signal power in one direction. The following diagram shows the radiation pattern of a directional antenna with its side lobes in polar form:

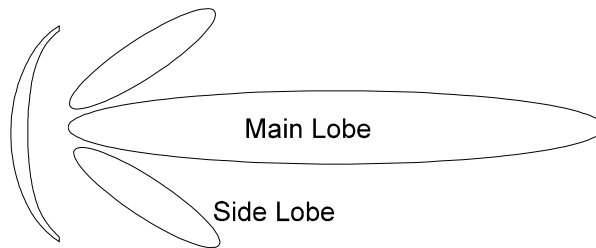


Figure 9.10: Radiation Pattern of Directional Antenna

Antenna Beamwidth

The directiveness of a directional antenna. Defined as the angle between two half-power (-3 dB) points on either side of the main lobe of radiation.

System Characteristics

Receiver Sensitivity

The minimum RF signal power level required at the input of a receiver for certain performance (e.g. BER).

EIRP (Effective Isotropic Radiated Power)

The antenna transmitted power. Equal to the transmitted output power minus cable loss plus the transmitting antenna gain.

P_{out}	Output power of transmitted in dBm
Ct	Transmitter cable attenuation in dB
Gt	Transmitting antenna gain in dBi
Gr	Receiving antenna gain in dBi
L	Path loss in dB
Cr	Receiver cable attenuation is dB
Pr	Received power level at receiver input in dBm
Sr	Receiver sensitivity is dBm

$$Pr = P_{out} - Ct + Gt - L + Gr - Cr$$

$$EIRP = P_{out} - Ct + Gt$$

Example:

Link Parameters:

Frequency: 2.4 Ghz

$P_{out} = 17$ dBm (50 mW)

Tx and Rx cable length (Ct and Cr) = 50ft. cable type LMR-400 (6.8 dB/100ft)

Tx and Rx antenna gain (Gt and Gr) = 18 dBi

Distance between sites = 5 miles

Receiver sensitivity (Sr) = -74 dBm

$Pr \geq Sr$

Link Budget Calculation

$$\text{EIRP} = P_{\text{out}} - C_t + G_t = 31.6 \text{ dBm}$$

$$L = 36.5 + 20 \times \text{Log}(F_{\text{Mhz}}) + 20 \times \text{Log}(D_{\text{Mile}}) \cong 118 \text{ dB}$$

$$P_r = \text{EIRP} - L + G_r - C_r = -72 \text{ dBm}$$

In conclusion, the received signal power is above the sensitivity threshold, so the link should work. The problem is that there is only a 2 dB difference between received signal power and sensitivity. Normally, a higher margin is desirable due to fluctuation in received power as a result of signal fading.

Signal Fading

Fading of the RF signal is caused by several factors:

- Multipath

The transmitted signal arrives at the receiver from different directions, with different path lengths, attenuation and delays. The summed signal at the receiver may result in an attenuated signal.

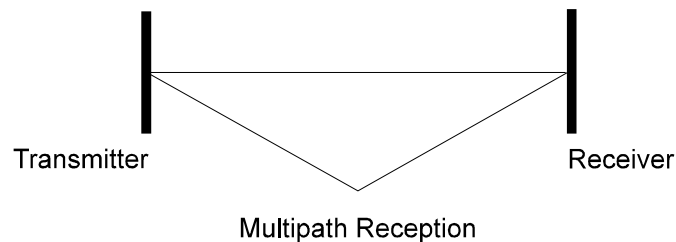


Figure 9.11: Multipath Reception

- Bad Line of Sight

An optical line of sight exists if an imaginary straight line can connect the antennas on either side of the link.

Radio wave clear line of sight exists if a certain area around the optical line of sight (Fresnel zone) is clear of obstacles. A bad line of sight exists if the first Fresnel zone is obscured.

- Link Budget Calculations
- Weather conditions (Rain, wind, etc.)

At high rain intensity (150 mm/hr), the fading of an RF signal at 2.4 GHz may reach a maximum of 0.02 dB/Km

Wind may cause fading due to antenna motion

- Interference

Interference may be caused by another system on the same frequency range, external noise, or some other co-located system.

The Line of Sight Concept

An optical line of sight exists if an imaginary straight line can be drawn connecting the antennas on either side of the link.

Clear Line of Sight

A clear line of sight exists when no physical objects obstruct viewing one antenna from the location of the other antenna.

A radio wave clear line of sight exists if a defined area around the optical line of sight (Fresnel Zone) is clear of obstacles.

Fresnel Zone

The Fresnel zone is the area of a circle around the line of sight.

The Fresnel Zone is defined as follows:

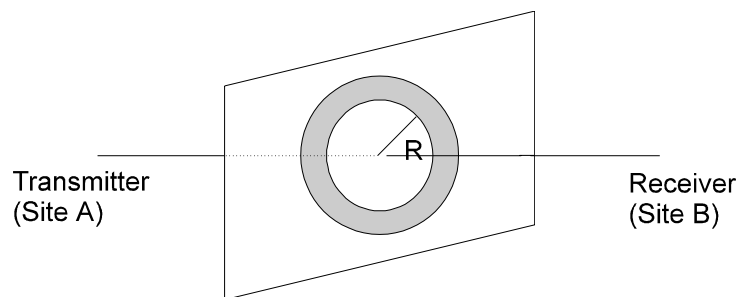


Figure 9.12: Fresnel Zone

$$R = \frac{1}{2} \sqrt{(\lambda x D)}$$

R: radius of the first Fresnel zone

λ : wavelength

D: distance between sites

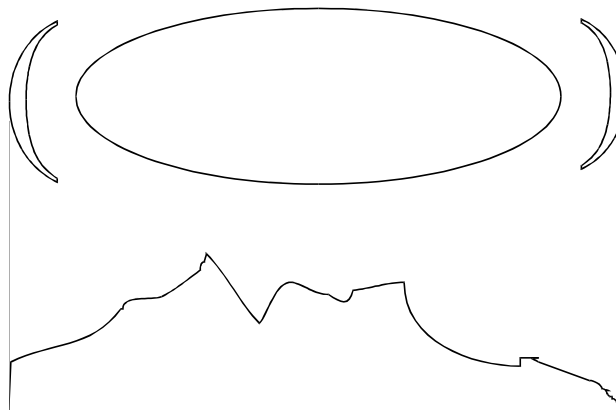


Figure 9.13: Fresnel Zone Clear of Obstacles

When at least 80% of the first Fresnel Zone is clear of obstacles, propagation loss is equivalent to that of free space.

8.5. IEEE 802.11 Technical Tutorial

The purpose of this chapter is to give technical readers a basic overview of the new IEEE 802.11 Standard, enabling them to understand the basic concepts, principles of operation, and the reasons behind some of the features and/or components of the Standard.

The document does not cover the entire Standard and does not provide enough information for the reader to implement an 802.11-compliant device (for this purpose the reader should refer to the Standard itself).

8.5.1. Architecture Components

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells. Each cell (called **Basic Service Set**, or **BSS**, in the 802.11 nomenclature) is controlled by a Base Station (called **Access Point** or, in short, **AP**).

Although a wireless LAN may be formed by a single cell, with a single Access Point, (and as will be described later, it can also work without an Access Point), most installations will be formed by several cells, where the

Access Points are connected through some kind of backbone (called **Distribution System** or **DS**). This backbone is typically Ethernet but, in some cases, might be wireless itself.

The whole interconnected wireless LAN, including the different cells, their respective Access Points and the Distribution System, is seen as a single 802 network to the upper layers of the OSI model and is known in the Standard as the **Extended Service Set (ESS)**.

The following diagram shows a typical 802.11 LAN including the components described above:

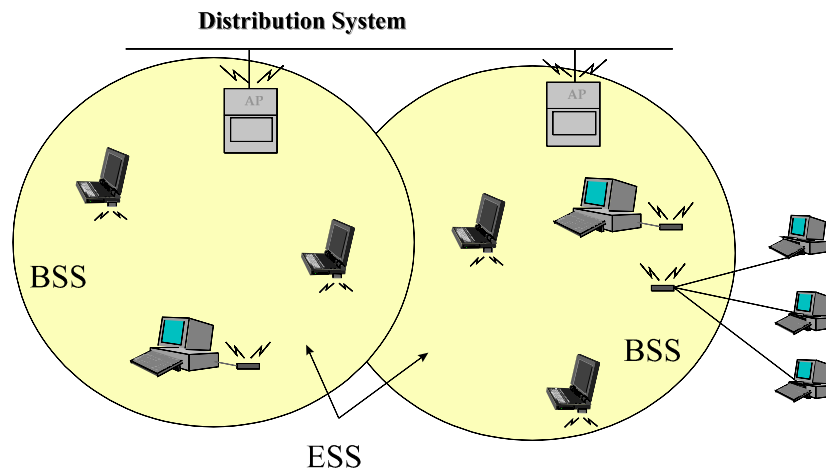


Figure 9.14: Typical 802.11 LAN

The standard also defines the concept of a **Portal**. A portal is a device that interconnects between an 802.11 and another 802 LAN. This concept is an abstract description of part of the functionality of a “translation bridge”.

Even though the standard does not necessarily require it, typical installations will have the AP and the Portal on a single physical entity. This is also the case with BreezeCOM’s AP which provides both functions.

8.5.2. IEEE 802.11 Layers Description

As in any 802.x protocol, the 802.11 protocol covers the Media Access Control Layer (MAC) and Physical Layer (PHY). The Standard currently defines a single MAC which interacts with three PHYs (all of them running at 1 or 2 Mbit/s) as follows:

- Frequency Hopping Spread Spectrum (FHSS) in the 2.4 GHz Band
- Direct Sequence Spread Spectrum (DSSS) in the 2.4 GHz Band, and
- InfraRed

802.2			Data Link
802.11 MAC			Layer
FH	DS	IR	PHY Layer

Beyond the standard functionality usually performed by MAC Layers, the 802.11 MAC performs other functions that are typically related to upper layer protocols, such as Fragmentation, Packet Retransmissions, and Acknowledges.

8.5.3. The MAC Layer

The MAC Layer defines two different access methods, the Distributed Coordination Function and the Point Coordination Function:

8.5.3.1 The Basic Access Method: CSMA/CA

The basic access mechanism, called the **Distributed Coordination Function**, is basically a Carrier Sense Multiple Access with Collision Avoidance mechanism (known as **CSMA/CA**). CSMA protocols are well-known in the industry, the most popular being Ethernet, which is a CSMA/CD protocol (CD standing for Collision Detection).

A CSMA protocol works as follows: A station desiring to transmit senses the medium. If the medium is busy (i.e. some other station is transmitting) then the station defers its transmission to a later time. If the medium seems free then the station is allowed to transmit.

These kinds of protocols are very effective when the medium is not heavily loaded since it allows stations to transmit with minimum delay. But there is always a chance of two or more stations simultaneously sensing the medium as being free and transmitting at the same time, causing a collision.

These collision situations must be identified so the MAC layer can retransmit the packet itself, not by the upper layers, to avoid significant delay. In the Ethernet case, a collision is recognized by the transmitting stations which listen while transmitting and go into a retransmission phase based on an **exponential random backoff** algorithm.

While these Collision Detection Mechanisms are a good idea on a wired LAN, they cannot be used on a wireless LAN environment for two main reasons:

1. Implementing a Collision Detection Mechanism would require the implementation of a Full-Duplex radio capable of transmitting and receiving at the same time, an approach that would increase the price significantly.
2. In a wireless environment we cannot assume that all stations can hear each other (a basic assumption of the Collision Detection scheme), and the fact that a station wants to transmit and senses the medium as free doesn't necessarily mean that the medium is free around the receiver's area.

In order to overcome these problems, 802.11 uses a Collision Avoidance (CA) mechanism together with a Positive Acknowledge scheme, as follows:

1. A station wanting to transmit senses the medium. If the medium is busy then it delays. If the medium is free for a specified time (called Distributed Inter Frame Space (DIFS) in the standard), then the station is allowed to transmit.
2. The receiving station checks the CRC of the received packet and sends an acknowledgment packet (ACK). Receipt of the acknowledgment indicates to the transmitter that no collision occurred. If the sender does not receive the acknowledgment, then it retransmits the fragment until it either receives acknowledgment or is thrown away after a given number of retransmissions.

8.5.3.2 Virtual Carrier Sense

In order to reduce the probability of two stations colliding because they cannot hear each other, the standard defines a Virtual Carrier Sense mechanism:

A station wanting to transmit a packet first transmits a short control packet called **RTS** (Request To Send), which includes the source, destination, and the duration of the following transaction (i.e. the packet and the respective **ACK**), the destination station responds (if the medium is free) with a response control Packet called **CTS** (Clear to Send), which includes the same duration information.

All stations receiving either the RTS or the CTS, set their **Virtual Carrier Sense** indicator (called **NAV**, for **Network Allocation Vector**), for the

given duration, and use this information together with the Physical Carrier Sense when sensing the medium.

This mechanism reduces the probability of a collision on the receiver area by a station that is “hidden” from the transmitter to the short duration of the RTS transmission because the station hears the CTS and “reserves” the medium as busy until the end of the transmission. The duration information on the RTS also protects the transmitter area from collisions during the ACK (from stations that are out of range of the acknowledging station).

It should also be noted that, due to the fact that the RTS and CTS are short frames, the mechanism also reduces the overhead of collisions, since these are recognized faster than if the whole packet was to be transmitted. (This is true if the packet is significantly bigger than the RTS, so the standard allows for short packets to be transmitted without the RTS/CTS transmission. This is controlled per station by a parameter called **RTS Threshold**).

The following diagrams show an exchange between stations A and B, and the NAV setting of their neighbors:

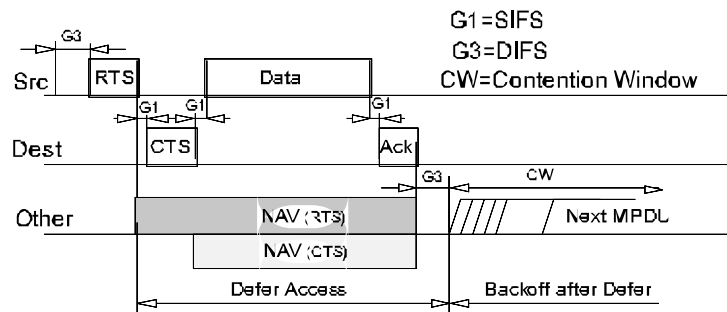


Figure 9.15: Transaction Between Stations A and B

The NAV State is combined with the physical carrier sense to indicate the busy state of the medium.

8.5.3.3 MAC Level Acknowledgments

As mentioned earlier in this document, the MAC layer performs Collision Detection by expecting the reception of an acknowledge to any transmitted fragment (Packets that have more than one destination, such as Multicasts, are not acknowledged.)

8.5.3.4 Fragmentation and Reassembly

Typical LAN protocols use packets several hundred bytes long (the longest Ethernet packet could be up to 1518 bytes long).

There are several reasons why it is preferable to use smaller packets in a wireless LAN environment:

- Due to the higher Bit Error Rate of a radio link, the probability of a packet getting corrupted increases with the packet size.
- In case of packet corruption (either due to collision or noise), the smaller the packet, the less overhead it causes to retransmit it.
- On a Frequency Hopping system, the medium is interrupted periodically for hopping (in our case every 20 milliseconds), so, the smaller the packet, the smaller the chance that the transmission will be postponed after dwell time.

However, it doesn't make sense to introduce a new LAN protocol that cannot deal with packets 1518 bytes long which are used on Ethernet, so the committee decided to solve the problem by adding a simple fragmentation/reassembly mechanism at the MAC Layer.

The mechanism is a simple Send-and-Wait algorithm, where the transmitting station is not allowed to transmit a new fragment until one of the following happens:

1. Receives an ACK for the said fragment, or
2. Decides that the fragment was retransmitted too many times and drops the whole frame.

It should be noted that the standard does allow the station to transmit to a different address between retransmissions of a given fragment. This is particularly useful when an AP has several outstanding packets to different destinations and one of them does not respond.

The following diagram shows a frame (MSDU) being divided to several fragments (MPDUs):

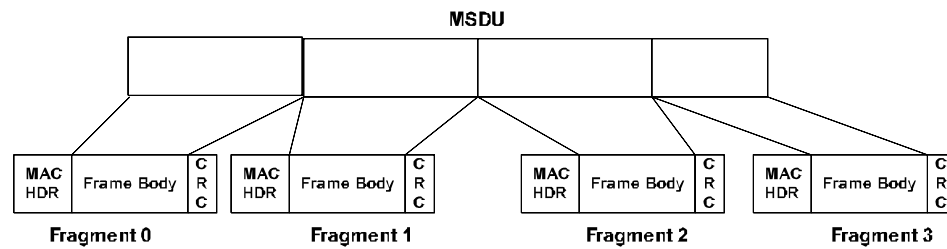


Figure 9.16: Frame Fragmentation

8.5.3.5 Inter Frame Spaces

The Standard defines 4 types of Inter Frame Spaces, which are used to provide different priorities:

- **SIFS - Short Inter Frame Space**, separates transmissions belonging to a single dialog (e.g. Fragment-Ack), and is the minimum Inter Frame Space. There is always at most one single station to transmit at any given time, therefore giving it priority over all other stations. This value is a fixed value per PHY and is calculated in such a way that the transmitting station will be able to switch back to receive mode and be capable of decoding the incoming packet. On the 802.11 FH PHY this value is set to 28 microseconds
- **PIFS - Point Coordination IFS**, is used by the Access Point (or Point Coordinator, as called in this case), to gain access to the medium before any other station. This value is SIFS plus a Slot Time (defined in the following paragraph), i.e. 78 microseconds.
- **DIFS - Distributed IFS**, is the Inter Frame Space used for a station willing to start a new transmission, which is calculated as PIFS plus one slot time, i.e. 128 microseconds.
- **EIFS - Extended IFS**, which is a longer IFS used by a station that has received a packet that it could not understand. This is needed to prevent the station (which could not understand the duration information for the Virtual Carrier Sense) from colliding with a future packet belonging to the current dialog.

8.5.3.6 Exponential Backoff Algorithm

Backoff is a well known method used to resolve contention between different stations wanting to access the medium. The method requires each station to choose a Random Number (n) between 0 and a given number, and wait for this number of Slots before accessing the medium, always checking if a different station has accessed the medium before.

The **Slot Time** is defined in such a way that a station will always be capable of determining if another station has accessed the medium at the beginning of the previous slot. This reduces collision probability by half.

Exponential Backoff means that each time the station chooses a slot and happens to collide, it will increase the maximum number for the random selection exponentially.

The 802.11 standard defines an **Exponential Backoff Algorithm**, that must be executed in the following cases:

- When the station senses the medium before the first transmission of a packet, and the medium is busy
- After each retransmission, and
- After a successful transmission

The only case when this mechanism is not used is when the station decides to transmit a new packet and the medium has been free for more than DIFS.

The following figure shows a schematic of the access mechanism:

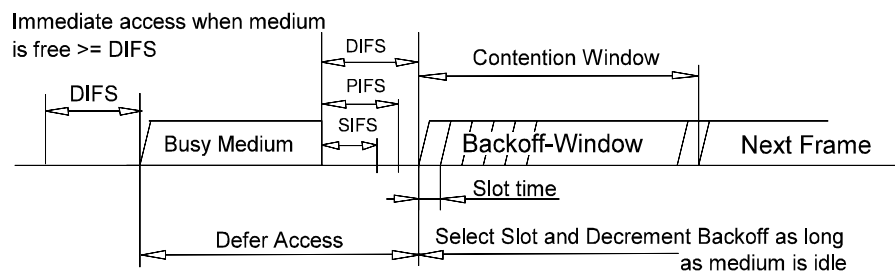


Figure 9.17: Access Mechanism

8.5.4. How Does a Station Join an Existing Cell (BSS)?

When a station wants to access an existing BSS (either after power-up, sleep mode, or just entering the BSS area), the station needs to get synchronization information from the Access Point (or from the other stations when in ad-hoc mode, which will be discussed later).

The station can get this information by one of two means:

1. **Passive Scanning:** In this case the station just waits to receive a Beacon Frame from the AP, (the beacon frame is a frame sent out periodically by the AP containing synchronization information), or
2. **Active Scanning:** In this case the station tries to locate an Access Point by transmitting Probe Request Frames, and waits for Probe Response from the AP.

Both methods are valid. A method is chosen according to the power consumption/performance trade-off.

8.5.4.1 The Authentication Process

Once the station has located an Access Point, and decides to join its BSS, it goes through the **Authentication Process**. This is the interchange of information between the AP and the station, where each side proves the knowledge of a given password.

8.5.4.2 The Association Process

Once the station is authenticated, it then starts the **Association Process**, which is the exchange of information about the station and BSS capabilities, and which allows the DSS (the set of APs) to know about the current position of the station). A station is capable of transmitting and receiving data frames only after the association process is completed.

8.5.5. Roaming

Roaming is the process of moving from one cell (or BSS) to another without losing connection. This function is similar to the cellular phones' handover, with two main differences:

1. On a packet-based LAN system, the transition from cell to cell may be performed between packet transmissions, as opposed to telephony where the transition may occur during a phone conversation, this makes the LAN roaming a little easier, but

2. On a voice system, a temporary disconnection may not affect the conversation, while in a packet-based environment it significantly reduces performance because retransmission is then performed by the upper layer protocols.

The 802.11 standard does not define how roaming should be performed, but defines the basic tools. These include active/passive scanning, and a re-association process, where a station which is roaming from one Access Point to another becomes associated with the new one¹.

8.5.6. Keeping Synchronization

Stations need to keep synchronization, which is necessary for keeping hopping synchronized, and other functions like Power Saving. On an infrastructure BSS, this is achieved by all the stations updating their clocks according to the AP's clock, using the following mechanism:

The AP periodically transmits frames called Beacon Frames. These frames contain the value of the AP's clock at the moment of transmission (note that this is the moment when transmission actually occurs, and not when it is put in the queue for transmission. Since the Beacon Frame is transmitted using CSMA rules, transmission may be delayed significantly).

The receiving stations check the value of their clocks at the moment the signal is received, and correct it to keep in synchronization with the AP's clock. This prevents clock drifting which could cause loss of synch after a few hours of operation.

8.5.7. Security

Security is one of the first concerns that people have when deploying a wireless LAN. The 802.11 committee has addressed the issue by providing what is called WEP (Wired Equivalent Privacy).

Users are primarily concerned that an intruder should not be able to:

- Access the Network resources by using similar wireless LAN equipment
- Capture wireless LAN traffic (eavesdropping)

¹The BreezeNET product line provides a patented enhanced roaming mechanism which allows stations to roam at speeds of 60 Km/h without losing or duplicating packets.

8.5.7.1 Preventing Access to Network Resources

This is done by the use of an Authentication mechanism where a station needs to prove knowledge of the current key. This is very similar to Wired LAN privacy, in the sense that an intruder needs to enter the premises (by using a physical key) in order to connect his workstation to the wired LAN.

8.5.7.2 Eavesdropping

Eavesdropping is prevented by using the WEP algorithm which is a Pseudo Random Number Generator initialized by a shared secret key. This PRNG outputs a key sequence of pseudo-random bits equal in length to the largest possible packet which is combined with the outgoing/incoming packet producing the packet transmitted in the air.

The WEP is a simple algorithm based on RSA's RC4 which has the following properties:

- **Reasonably strong:**
Brute-force attack to this algorithm is difficult because every frame is sent with an Initialization Vector which restarts the PRNG for each frame.
- **Self Synchronizing:**
The algorithm re-synchronizes for each message. This is necessary in order to work in a connection-less environment, where packets may get lost (as any LAN).

8.5.8. Power Saving

Wireless LANs are typically related to mobile applications. In this type of application, battery power is a scarce resource. This is the reason why the 802.11 standard directly addresses the issue of Power Saving and defines an entire mechanism which enables stations to go into sleep mode for long periods of time without losing information.

The main idea behind the Power Saving Mechanism is that the AP maintains a continually updated record of the stations currently working in Power Saving mode, and buffers the packets addressed to these stations until either the stations specifically request the packets by sending a polling request, or until they change their operation mode.

As part of its Beacon Frames, the AP also periodically transmits information about which Power Saving Stations have frames buffered at the AP, so these

stations wake up in order to receive the Beacon Frame. If there is an indication that there is a frame stored at the AP waiting for delivery, then the station stays awake and sends a Polling message to the AP to get these frames.

Multicasts and Broadcasts are stored by the AP, and transmitted at a pre-known time (each DTIM), when all Power Saving stations who wish to receive this kind of frames are awake.

8.5.9. Frame Types

There are three main types of frames:

- **Data Frames:** which are used for data transmission
- **Control Frames:** which are used to control access to the medium (e.g. RTS, CTS, and ACK), and
- **Management Frames:** which are frames that are transmitted in the same manner as data frames to exchange management information, but are not forwarded to upper layers (e.g. beacon frames).

Each frame type is subdivided into different Subtypes, according to its specific function.

8.5.10. Frame Formats

All 802.11 frames are composed of the following components:

Preamble	PLCP Header	MAC Data	CRC
----------	-------------	----------	-----

8.5.10.1 Preamble

This is PHY dependent, and includes:

- **Synch:** An 80-bit sequence of alternating zeros and ones, which is used by the PHY circuitry to select the appropriate antenna (if diversity is used), and to reach steady-state frequency offset correction and synchronization with the received packet timing.
- **SFD:** A Start Frame delimiter which consists of the 16-bit binary pattern 0000 1100 1011 1101, which is used to define frame timing.

8.5.10.2 PLCP Header

The PLCP Header is always transmitted at 1 Mbit/s and contains Logical information used by the PHY Layer to decode the frame. It consists of:

- **PLCP_PDU Length Word:** which represents the number of bytes contained in the packet. This is useful for the PHY to correctly detect the end of packet.
- **PLCP Signaling Field:** which currently contains only the rate information, encoded in 0.5 Mbps increments from 1 Mbit/s to 4.5 Mbit/s.
- **Header Error Check Field:** Which is a 16 Bit CRC error detection field.

8.5.10.3 MAC Data

The following figure shows the general MAC Frame Format. Part of the fields are only present in part of the frames as described later.

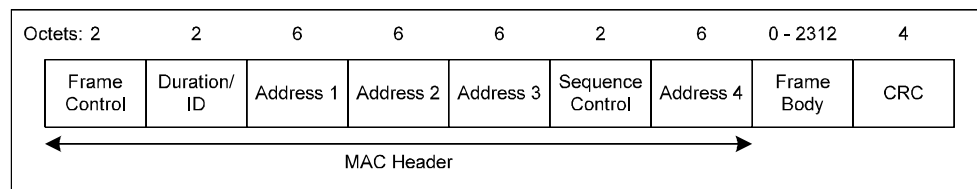


Figure 9.18: MAC Frame Format

Frame Control Field

The Frame Control field contains the following information:

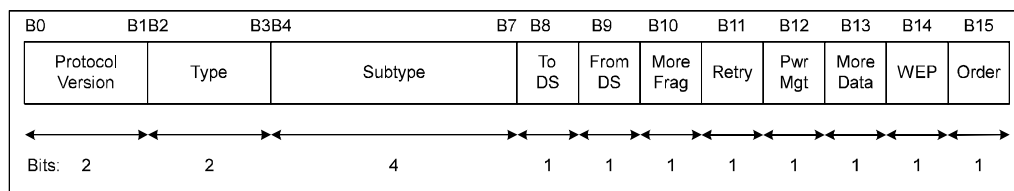


Figure 9.19: Frame Control Field

Protocol Version

This field consists of 2 bits which are invariant in size and placement across following versions of the 802.11 Standard, and will be used to recognize possible future versions. In the current version of the standard the value is fixed as 0.

Type and Subtype

These 6 bits define the Type and SubType of the frame as indicated in the following table:

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Association Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-0001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-ACK + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
10	Data	0000-1111	Reserved

ToDS

This bit is set to 1 when the frame is addressed to the AP for forwarding to the Distribution System (including the case where the destination station is in the same BSS, and the AP is to relay the frame).

The Bit is set to 0 in all other frames.

FromDS

This bit is set to 1 when the frame is received from the Distribution System.

More Fragments

This bit is set to 1 when there are more fragments belonging to the same frame following the current fragment.

Retry

This bit indicates that this fragment is a retransmission of a previously transmitted fragment. This is used by the receiver station to recognize duplicate transmissions of frames that may occur when an Acknowledgment packet is lost.

Power Management

This bit indicates the Power Management mode that the station will be in after the transmission of this frame. This is used by stations which are changing state either from Power Save to Active or vice versa.

More Data

This bit is used for Power Management as well as by the AP to indicate that there are more frames buffered for this station. The station may decide to use this information to continue polling or even changing to Active mode.

WEP

This bit indicates that the frame body is encrypted according to the WEP algorithm

Order

This bit indicates that this frame is being sent using the Strictly-Ordered service class.²

Duration/ID

This field has two meanings depending on the frame type:

- In Power-Save Poll messages this is the Station ID
- In all other frames this is the duration value used for the NAV Calculation.

Address Fields

A frame may contain up to 4 Addresses depending on the ToDS and FromDS bits defined in the Control Field, as follows:

- **Address-1** is always the Recipient Address (i.e. the BSS station that is the immediate recipient of the packet). If ToDS is set, this is the AP Address; if ToDS is not set, then this is the address of the end-station.
- **Address-2** is always the Transmitter Address (i.e. the station which is physically transmitting the packet). If FromDS is set, this is the AP address; if it is not set, then it is the Station address.
- **Address-3** is in most cases the remaining, missing address. On a frame with FromDS set to 1, Address-3 is the original Source Address; if the frame has the ToDS set, then Address 3 is the destination Address.
- **Address-4** is used in special cases where a Wireless Distribution System is used, and the frame is being transmitted from one Access Point to another. In such cases, both the ToDS and FromDS bits are set, so both the original Destination and the original Source Addresses are missing.

The following Table summarizes the usage of the different Addresses according to ToDS and FromDS bits setting:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A

² The Strictly-Ordered Service Class is defined for users that cannot accept change of ordering between Unicast Frames and Multicast Frames (ordering of Unicast frames to a specific address is always maintained). The only known protocol that would need this service class is DEC's LAT.

0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Sequence Control

The Sequence Control Field is used to represent the order of different fragments belonging to the same frame, and to recognize packet duplications. It consists of two subfields, Fragment Number and Sequence Number, which define the frame and the number of the fragment in the frame.

CRC

The CRC is a 32-bit field containing a 32-bit Cyclic Redundancy Check (CRC)

8.5.11. Most Common Frame Formats

8.5.11.1 RTS Frame Format

The RTS frame looks as follows:

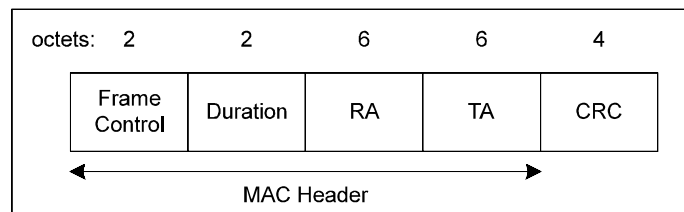


Figure 9.20: RTS Frame Format

The RA of the RTS frame is the address of the STA on the wireless medium that is the intended immediate recipient of the next Data or Management frame.

The TA is the address of the STA transmitting the RTS frame.

The Duration value is the time, in microseconds, required to transmit the next Data or Management frame, plus one CTS frame, plus one ACK frame, plus three SIFS intervals.

8.5.11.2 CTS Frame Format

The CTS frame looks as follows:

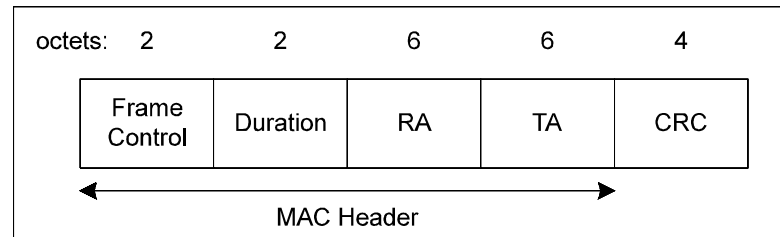


Figure 9.21: CTS Frame

The Receiver Address (RA) of the CTS frame is copied from the Transmitter Address (TA) field of the immediately previous RTS frame to which the CTS is a response.

The Duration value is the value obtained from the Duration field of the immediately previous RTS frame, minus the time, in microseconds, required to transmit the CTS frame and its SIFS interval.

8.5.11.3 ACK Frame Format

The ACK frame looks as follows:

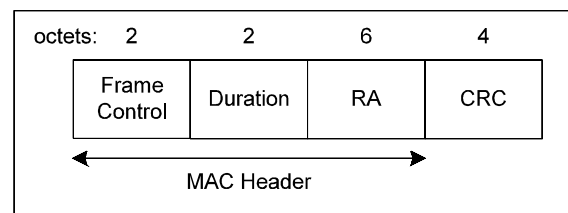


Figure 9.22: ACK Frame Format

The Receiver Address of the ACK frame is copied from the Address 2 field of the immediately previous frame.

If the More Fragment bit was set to 0 in the Frame Control field of the previous frame, the Duration value is set to 0, otherwise the Duration value is obtained from the Duration field of the previous frame, minus the time, in microseconds, required to transmit the ACK frame and its SIFS interval.

8.5.12. Point Coordination Function (PCF)

Beyond the basic Distributed Coordination Function, there is an optional Point Coordination Function, which may be used to implement time-bounded services, like voice or video transmission. This Point Coordination Function makes use of the higher priority that the Access Point may gain by the use of a smaller Inter Frame Space (PIFS).

By using this higher priority access, the Access Point issues polling requests to the stations for data transmission, hence controlling medium access. To still enable regular stations to access the medium, there is a provision that the Access Point must leave enough time for Distributed Access in between the PCF.

8.5.13. Ad-hoc Networks

In certain circumstances, the users may wish to build up wireless LAN networks without an infrastructure (more specifically without an Access Point). This may include file transfer between two notebook users, co-workers meeting outside the office, etc.

The 802.11 Standard addresses this need by the definition of an “ad-hoc” mode of operation. In this case, there is no Access Point and part of its functionality is performed by the end-user stations (such as Beacon Generation, synchronization, etc.). Other AP functions are not supported (such as frame-relaying between two stations not in range, or Power Saving).

AMP2440-250

AMP2440-500

Installation Instructions

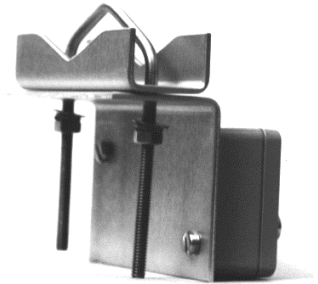
AMPLIFIER KIT

Each Amplifier Kit Includes:

- Bi-directional Amplifier, AMP2440-250 or AMP2440-500
- DC Power Injector
- 5ft. LMR-400 cable (N-male to N-female)
- 2 N-male to N-male adapters
- 110/220 VAC to 12VDC Power Supply, and power cord
- Stainless Steel U-Bolt and mounting bracket
- Vapor wrap coaxial connector sealing tape
- Installation Manual

Cable Length vs. Output Power

The AMP2440 is an amplifier designed for installation by professional radio installers. Several key factors unique to the particular installation determine the power level at the input of the amplifier. The most important consideration is the cable loss in the transmission cable between the radio and the pole mounted amp. It is important that the installer understand these and other factors when computing the input power to the amplifier. The table below shows cable length and output power for both the 250mW and 500mW models.



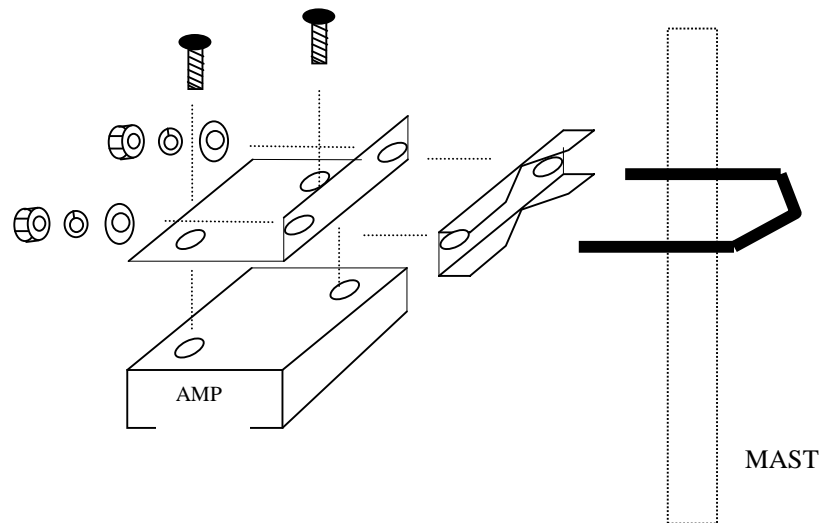
Power Output vs. Cable Length

AMP model	Cable type	Length	Power in	Power out
AMP2440-250	LMR-400	30 ft.	13.9dBm	24dBm/250mW*
AMP2440-250	LMR-400	50 ft.	12.5dBm	24dBm.250mW*
AMP2440-250	LMR-400	100 ft.	9dBm	24dBm/250mW
AMP2440-250	LMR-600	150 ft.	9dBm	24dBm/250mW
AMP2440-500	LMR-600	22 ft.	15dBm	27dBm/500mW
AMP2440-500	LMR-600	100 ft.	11.5dBm	26.5dBm/447mW

* higher output power is not possible because the output is limited.

Installation and Mounting

The amplifier can be mast mounted using the steel U-bolt included with the unit. The amplifier should be installed with the connectors facing downward. After placing the assembly on the mast, use an open-end wrench to carefully tighten the nuts. Take care not to over-tighten the nuts or you may inadvertently strip the threads. See the diagram below for proper assembly.



It is very important to waterproof the RF connectors on the amplifier. However, it is recommended that you do not seal the connectors until after all system tests have been performed. Be sure to use the high quality weather resistant vapor wrap included with your amplifier kit to seal all the outside connections.

The DC Power Injector is not in a waterproof enclosure and must be protected from the weather. It can be permanently mounted to a surface using the mounting flanges. Refer to the BreezeCom Amplifier Installation Details diagram shown later in this manual.

NOTE: When using the 24dB gain dish antenna in the United States, the external filter (P/N: SPF-1) must be installed to comply with FCC emission requirements.

Amplifier Connections and Indicators

- Transmit LED:** This LED glows RED in transmit mode.
- Receive LED:** This LED glows GREEN in the “receive” mode. (When DC power is supplied, the unit defaults to receive mode).
- DC Injector Connection:** This “N” Female connector is connected to the DC Power Injector via the transmission cable.
- Antenna Connection:** This “N” Female connector connects to the antenna with a short length of coax cable.

DC Power Injector Connections and Indicators

A DC Power Injector is an in-line device which “injects” the DC power necessary to operate the amplifier onto a transmission line. This allows the cable to carry both RF signals and DC power to the mast-mounted amplifier.

Transmit LED: This LED glows RED when the pole mounted amplifier goes into the transmit mode. The Transmit LED is driven by unique circuitry, which actually detects changes in the DC current through the transmission line to the amplifier.

Receive LED: This LED glows GREEN when DC power is applied to the amplifier and it is in the receive mode. When toggling between transmit and receive this LED will glow slightly dimmer.

To Radio Connection: This “N” Female connector is connected to the radio modem via a short jumper cable.

To Amplifier Connection: This “N” Female connector connects to the amplifier on the mast via the transmission line.

12 VDC: This is the DC power input for the injector and is a standard 2.1mm barrel jack. +12VDC applied with center positive.

Power Supply

The AMP2440 comes with power supplies that have standard 2.1 mm barrel plugs (which are configured as positive (+) tip and negative (-) outer conductor). Although normally supplied with a power supply, any regulated 12 Volt DC 1 amp supply can be used. The power supply can be used with 110 or 240 VAC power.

Operation

The unit operates automatically and there are no user adjustments.

The amplifier is only intended for use with the BreezeNET Radios. These radios “ping pong” back and forth between transmit and receive so quickly, during normal operation, that both the TX and RX LEDs will appear to be lit simultaneously. In fact, they are turning on and off so quickly that they appear to be on all the time. You can tell how quickly one of these LEDs are turning on and off by their brightness. Their glow will be slightly dimmer when they are off.