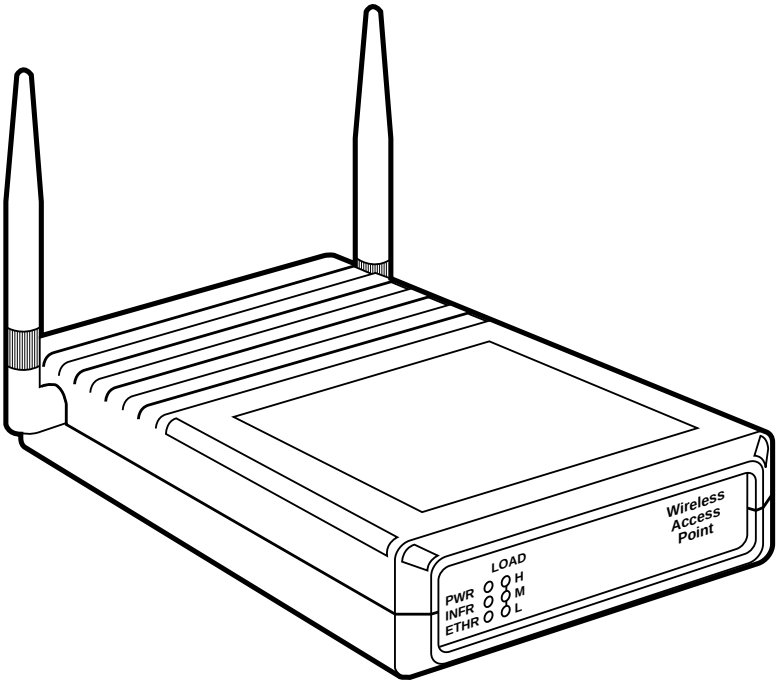
1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746

BLACK BOX®
NETWORK SERVICES

JANUARY 2000

LW0050A	LW0057A
LW0051A	LW0058A
LW0052A	LW0059A
LW0053A	LW0060A-CAN
LW0054A	LW0061A-CAN
LW0055A	LW0062A-CAN
LW0056A	LW0063A-CAN

Pro 11 Series Wireless Ethernet



CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S. 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

TRADEMARKS USED IN THIS MANUAL

Apple and AppleTalk are registered trademarks of Apple Computer, Inc.

Digital is a trademark of Digital Equipment Corporation.

HP is a registered trademark of Hewlett-Packard.

IBM is a registered trademark of International Business Machines Corporation.

Windows and Windows NT are registered trademarks of Microsoft Corporation.

Sun is a registered trademark of Sun Microsystems, Inc.

UL is a registered trademark of Underwriters Laboratories Incorporated.

Any other trademarks used in this manual are acknowledged to be the property of the trademark owners.

FEDERAL COMMUNICATIONS COMMISSION
AND
CANADIAN DEPARTMENT OF COMMUNICATIONS
RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

NORMAS OFICIALES MEXICANAS (NOM)
ELECTRICAL SAFETY STATEMENT

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

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.

Contents

Chapter **Page**

Chapter **Page**

Chapter **Page**

Chapter **Page**

Chapter **Page**

1. Introduction

1.1. How to Use This Guide

This guide contains instructions for overall planning and setting up your wireless LAN. It explains how to install each unit, plus how to install antennas and accessories.

This guide contains:

- *Chapter 1, Introduction* – Explains how to use this guide.
- *Chapter 2, Basic Installation* – Explains how to install the Pro 11 Series units.
- *Chapter 3, Using the Local Terminal for Unit Setup and Management* – Describes how to use the local terminal to set up, configure, and manage Pro 11 Series units.
- *Chapter 4, PCMCIA Adapter Installation, Setup, and Management* – Describes how to install the LW0054A and LW0059A and how to set up and manage the Adapter using the appropriate utilities.
- *Chapter 5, Planning and Installing Wireless LANs* – Guidelines and restrictions regarding antenna selection and installation.
- *Chapter 6, Upgrade Procedure* – Explains how to perform upgrades for Pro 11 Series units using a TFTP application.
- *Chapter 7, System Troubleshooting* – Solves some common problems that may occur when installing and using Pro 11 Series products.
- *Appendices* – These include: Supported MIBs and traps, specifications, wireless LAN concepts, radio signal propagation, and an IEEE 802.11 technical tutorial.

1.2. Pro 11 Series Features

- *IEEE 802.11 Compliant* – All 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* – A 3-Mbps modem, with up to 2-Mbps data throughput.
- *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.
- *Flash Updates* – All items in the Pro 11 Series line can be freely and quickly upgraded with flash updates.
- *LW0054A/LW0059A Card* – The LW0054A Pro 11 PC Card is extremely compact and does not extend beyond your PC. It comes with two retractable antennas. The LW0059A has two connectors to which antennas may be connected. Multi-rate support for 1, 2, and 3 Mbps guarantees efficient use of the medium. Throughput is up to 2 Mbps.

    Configuration Utility – This user-friendly application helps you quickly set up stations containing the LW0054A/LW0059A Card. You can save the configuration to a file and import the file to other stations for fast installation.

    Site Survey Utility – This user-friendly application records the signal strength received by the LW0054A/LW0059A Card at different locations, giving a clear image of existing coverage. The gathered data indicates whether to add, remove, or move Access Points.

1.3 Pro 11 Series Product Line

These are Pro 11 Series Wireless Ethernet Units with Integral 2-dBi Antennas.

Ethernet Access Point, Monitor Cable, Power Supply LW0050A
Single-Port Station Adapter, Power Supply LW0051A
Four-Port Station Adapter, Power Supply LW0052A
Ethernet Workgroup Bridge, Power Supply.....LW0053A
3-Mbps Type II PCMCIA Adapter with
Folding Diversity Antenna and Software LW0054A

If you're using one or two detached antennas, use one of these units.

Ethernet Access Point, Monitor Cable, Power Supply,
Mounting Bracket LW0055A
Canadian version LW0060A-CAN
Single-Port Station Adapter, Power Supply, Mounting Bracket LW0056A
Canadian version LW0061A-CAN
Four-Port Station Adapter, Power Supply, Mounting Bracket LW0057A
Canadian version LW0062A-CAN
Ethernet Workgroup Bridge, Power Supply, Mounting Bracket.....LW0058A
Canadian version LW0063A-CAN
Type II PCMCIA Adapter with MMCX Connectors LW0059A

Note: Pro 11 series products are not compatible with Pro series products, but the Pro Series can be upgraded to be compatible with the Pro 11 series. Call Technical Support for information.

1.3.1 Access Point (LW0050A, LW0055A, or LW0060A-CAN)

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

The Access Point is a wireless hub that provides access for wireless workstations into wired Ethernet LANs. It also contains the wireless relaying function that enables workstations equipped with a Station Adapter (Station Adapter, Bridge, or PCMCIA Adapter) 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.

The Access Point can support various data rates simultaneously at 3 Mbps, 2 Mbps, or 1 Mbps.

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 area. The roaming 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.

Multiple access points can be positioned in locations where heavy network traffic is expected; this creates a multicell and increases 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 Access Point contains an embedded SNMP agent, enabling effective management by any standard SNMP management station. Software upgrades can be downloaded by TFTP protocol via the wired LAN or wireless LAN.

The Access Point is available in two models:

- With two integrated omnidirectional antennas (LW0050A), and
- For use with external high-gain antennas (LW055A or LW0060A-CAN).

1.3.2 Single-Port Station Adapter (LW0051A, LW0056A, or LW0061A-CAN)

The Single-Port Station Adapter is a wireless LAN station adapter that converts any device equipped with an Ethernet interface into a wireless LAN station. The Single-Port Station Adapter is transparent to the device's hardware, software, and network operating system. This enables plug-and-play installation.

The Single-Port Station Adapter enables its workstation to communicate with any other wireless station in the same cell coverage area, and to access all network resources—such as file servers, wired stations, printers, and shared databases—via the Access Point. Any two wireless stations in two different cells can communicate through their Access Points.

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

The Single-Port Station Adapter contains an embedded SNMP agent enabling effective management. Software upgrades are downloaded by TFTP via the Ethernet port or via the Wireless LAN and Access Point.

Network connection is maintained while roaming between overlapping coverage areas. Transmission and reception can be continued while moving at high speed with no data-packet loss or duplication.

The Single-Port Station Adapter is available in two models:

- With two integrated 2-dBi omnidirectional antennas (LW0051A).
- For use with external antennas (LW0056A or LW0061A-CAN).

1.3.3 Four-Port Station Adapter (LW0052A, LW0057A, or LW0062A-CAN)

The Four-Port Station Adapter is a wireless LAN adapter that connects a workgroup of up to four Ethernet-equipped workstations to the wireless LAN. The Four-Port Station Adapter is transparent to the workgroup devices' hardware and software, allowing plug-and-play installation.

The Four-Port Station Adapter enables connected workstations to communicate with other wireless stations in the same cell coverage area, and to access all network resources—such as file servers, wired stations, printers, and shared databases—via the Access Point. The Four-Port Station Adapter also allows highly efficient and fast wired communication among the four connected workstations.

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

The Four-Port Station Adapter contains an embedded SNMP agent and software downloading capabilities which allow it to be effectively managed. Software upgrades are downloaded by TFTP protocol via the Ethernet ports or via the Wireless LAN and Access Point.

Network connection is maintained while roaming between overlapping coverage areas. Transmission and reception can be continued while moving at high speed with no data-packet loss or duplication.

The Four-Port Station Adapter is available in two models:

- With two integrated omnidirectional antennas (LW0052A).
- For use with external antennas (LW0057A or LW0062A-CAN).

1.3.4 Workgroup Bridge (LW0053A, LW0058A, or LW0063A-CAN)

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

The Workgroup Bridge communicates with the Access Points of the remote LANs, effectively creating an extended wireless network spanning sites situated up to 6 miles (9.7 km) apart (in Europe, this range is limited by ETSI regulations to 2.5 km; in deregulated regions, this range can be up to 60 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, and any other device that supports Ethernet. The unit is transparent to the workgroup devices' hardware, software, and network operating system.

The 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.

The Workgroup Bridge is available in two models:

- With two integrated 2-dBi omnidirectional antennas (LW0053A).
- With two external-antenna connector ports (LW0058A or LW0063A-CAN).

1.3.5 PCMCIA Adapter (LW0054A or LW0059A)

The PCMCIA Adapter gives the portable computer user continuous connectivity and complete mobility, allowing seamless roaming throughout the wireless LAN campus. It converts any portable computer (including notebooks, laptops, pen-based and hand-held computers) containing a PCMCIA Release 2.1 Type II slot into a wireless LAN workstation.

The PCMCIA Adapter can communicate with any other wireless station in its cell coverage area. Furthermore, any two wireless stations in two different cells can communicate through their Access Points. The PCMCIA Adapter can access all network resources, such as file servers, other wired stations, printers, and shared databases, via the Access Point.

Network connection is maintained while roaming between overlapping cell coverage areas. Transmission and reception can be continued while moving at high speed with no data-packet loss or duplication.

The PCMCIA Adapter is available in two models:

- With two integrated omnidirectional retractable antennas (LW0054A).
- With two external-antenna connector ports (LW0059A).

1.4 Pro 11 Functional Description

1.4.1 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.

1.4.2 Startup Procedure

When wireless units (other than Access Points) start up, they scan the frequencies for an Access Point. If an active Access Point is in range, the units synchronize with it. The addresses associated with the units are registered in the Access Point (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.

1.4.3 Access Point

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

The Access Point continuously "listens" for wireless messages as well. When the Access Point "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 Access Point "hears" a wireless message whose destination is not on the wireless LAN, it forwards the message to the wired LAN. Messages cannot be sent directly between wireless stations without an Access Point to relay the message.

1.4.4 Single-Port Station Adapters

The Single-Port Station Adapter is connected to a station's network card. When the station sends a message, the Single-Port Station Adapter wirelessly forwards it to the Access Point. And when the Access Point receives a message destined for the station, it wirelessly forwards the message to the Single-Port Station Adapter.

The first time the station sends a message, the station's address is registered in the Access Point. The Access Point keeps only the first address for each Single-Port Station Adapter, so the Single-Port Station Adapter will not work properly if connected to more than one station.

1.4.5 Four-Port Station Adapter

The Four-Port Station Adapter has four connectors for up to four stations, and features operation identical to that of the Single-Port Station Adapter. As each station connected to the Four-Port Station Adapter sends its first message, each address is registered in the Access Point. The Access Point only keeps up to four addresses for each Four-Port Station Adapter (1 address per port), so the Four-Port Station Adapter will not work properly if connected to more than four stations.

1.4.6 Ethernet Workgroup Bridge

The Ethernet Workgroup Bridge connects to a hub in a wired Ethernet LAN. When a station on the Ethernet Workgroup Bridge's LAN sends a message that is not destined for a local station, the Ethernet Workgroup Bridge wirelessly forwards the message to the Access Point. And when the Access Point receives a message destined for a station on the Ethernet Workgroup Bridge's LAN, the Access Point wirelessly forwards it to the Ethernet Workgroup Bridge. In this way, the Ethernet Workgroup Bridge and Access Point work together like a standard network bridge.

The first time each station on the Ethernet Workgroup Bridge's LAN sends a message, the station's address is registered in the Ethernet Workgroup Bridge and the Access Point. The Ethernet Workgroup Bridge and Access Point can hold all the addresses necessary to support an entire LAN connected to an Ethernet Workgroup Bridge.

1.4.7 3-Mbps Type II PCMCIA Adapter

The 3-Mbps Type II PCMCIA Adapter is inserted into the station's PCMCIA slot and features identical operation to that of the Single-Port Station Adapter. As opposed to the Single-Port Station Adapter that connects to the station's network card, the 3-Mbps Type II PCMCIA Adapter *is* the station's network card. The Single-Port Station Adapter can be used with stations of any operating system as long as the station sends legal Ethernet messages, but the 3-Mbps Type II PCMCIA Adapter requires a driver that is compatible with the station's operating system.

2. Basic Installation

This chapter describes the physical installation of the Pro 11 Series units described in **Chapter 1**, with the exception of the PCMCIA Adapter. Installation for the LW0054A/LW0059A PCMCIA Adapter is described in **Chapter 4**.

The Pro 11 Series features plug-and-play operation (the unit starts operating immediately after physical installation with a set of default operation parameters). A local terminal can be connected to the unit to perform system-specific parameter settings. The use of a local terminal and the configuration parameters are described in **Chapter 3**. In addition, all products in the Pro 11 Series contain an SNMP agent and can be configured from a remote location via the network.

2.1. Basic Installation Checklist

Standard installation involves these steps:

- Check the packing 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 Packing List

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

- The unit, complete with two omnidirectional antennas or RF connectors for use with external antennas (for models LW0055A through LW0059A).
- 5-VDC power-supply transformer.
- Mounting bracket for wall or ceiling installations and torque key for antenna connectors (supplied with models LW0055A through LW0058A).

The Access Points come with these additional components:

- This guide.
- A monitor connector cable for connecting the units to a monitor in order to perform Local Terminal Management functions (see **Section 3.1**).

A proprietary MIB disk for performing remote-unit configuration and monitoring via SNMP is also available.

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 should be shipped in its original package.

2.3 Position the Unit

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 point up. For models with external antennas, connect the external antennas and RF cable. For information about external antenna installation, refer to **Section 5.3**.

Heat Sources
Keep the units well away from sources of heat, such as radiators and air conditioners.

Additional Considerations When Positioning the Access Point

When positioning the Access Points, take into account the following additional considerations.

Height
Install the Access Point at least 5 feet (1.5 m) 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 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 5 VDC (1200 mA, 1500 mA 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 power transformer to a power outlet supplying 110 or 220 VAC.

2.5 Connect the Unit to the Ethernet Port

- Connect one end of an Ethernet 10BASE-T 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 a Single-Port Station Adapter or Four-Port Station Adapter to a PC, use a straight cable.

  When connecting an Access Point or Ethernet Workgroup Bridge to a LAN, use a straight cable.

  When connecting an Access Point or Ethernet Workgroup Bridge to a PC, use a crossed cable.

  When connecting an Access Point to a Ethernet Workgroup Bridge, use a crossed cable.

2.6 Check LED Indicators

Verify that the unit is functioning correctly via the front-panel LEDs. The following tables describe the front-panel LEDs for Station Adapters, Bridges, and Access Points.

2.6.1 LEDs on Station Adapters and Bridges

Name	Description	Meaning
PWR	power supply	On – After successful power-up Off – Power off
WLNK	WLAN Link	On – Unit is synchronized or associated with an Access Point Off – Unit is not synchronized or associated with an Access Point
ETHR	Ethernet activity	On – Reception on Ethernet port Off – No reception on Ethernet port

Name	Description	Meaning
QLT	Quality of reception	*H, M, and L LEDs not lit:* Very-low-quality reception (less than -81 dBm) or not synchronized with Access Point. *H and M LEDs not lit, L LED is lit:* Low-quality reception (from -81 to -77 dBm), usually enabling 1-Mbps traffic. *H LED not lit, M and L LEDs lit:* Medium-quality reception (from -77 to -65 dBm), usually enabling 2-Mbps traffic. *H, M, and L LEDs lit:* High-quality reception (greater than -65 dBm), enabling 3-Mbps traffic.

2.6.2 Access Point LEDs

Name	Description	Meaning
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)	*H, M, and L LEDs not lit:* No stations. *H and M LEDs not lit, L LED lit:* 1 to 8 stations. *H LED not lit, M and L LEDs lit:* 9 to 16 stations. *H, M, and L LEDs lit:* 17 or more stations.

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. On Access Points, the LINK indicator is located on the attached hub port; on Station Adapters, the LINK indicator is located on the NIC.

3. Using the Local Terminal for Unit Setup and Management

The Pro 11 Series units feature plug-and-play operation; the unit starts operating immediately following physical installation with a set of default parameters. System-specific configuration of the unit to meet specific requirements can be done via a local terminal (ASCII ANSI terminal or PC) connected to the unit.

This chapter explains how to use the local terminal to configure and manage the Pro 11 Series units described in **Chapter 1**. Configuration and management for the LW0054A/LW0059A PCMCIA PC Card is described in **Chapter 4**.

3.1 Getting Started with the Local Terminal

1. Use the Monitor cable supplied with the Access Point. Connect one end of the cable to the MON jack on the rear panel of the unit and the other to the COM port of the terminal.

2. Run a terminal-emulation program (such as HyperTerminal).

3. Set 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 is displayed (see Figure 3-1 on page 29).

To use Local Terminal Management:

1. Click 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 sub-submenus in the terminal program that the Installer can edit. 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 and press 1, then 2, and then 1.

Table 3-1. Configuration Menus

Menu	Sub-Menu	Sub-Submenu	Default Values
1. System Config-uration	1.1 Station Status		
	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	Enabled
		1.2.5 Display Current Values	
	1.3 Wireless LAN (WLAN) Parameters	1.3.1 Hopping Sequence (*only for Access Points*)	1
		1.3.2 Hopping Set (*only for Access Points*)	1
		1.3.3 ESS ID	ESSID1
		1.3.4 Maximum Data Rate	3 Mbps
		1.3.5 Transmit Antenna	Use 2 Antennas*
		1.3.6 Mobility	Low
		1.3.7 Load Sharing	Disabled**
		1.3.8 Preferred AP (*not available for Access Points*)	
		1.3.A Display Current Values	

* Option **1.3.5 Transmit Antenna** has the default value **Use #2** for the Four-Port Station Adapters only.

** Option **1.3.7 Load Sharing** has the default value **Enabled** for the Access Points only.

Table 3-1 (continued). Configuration Menus

Menu	Sub-Menu	Sub-Submenu	Default Values
	1.4 Bridging	1.4.1 LAN to WLAN Bridging Mode (*Access Points only)*	Reject Unknown
		1.4.2 Intelligent Bridging Period (*Access Points only*)	15 sec
		1.4.3 IP Filtering	Disabled
		1.4.4 Tunneling	Both Enabled
		1.4.5 Broadcast Relaying	Enabled
		1.4.6 Unicast Relaying	Enabled
	1.5 Station Control	1.5.1 Reset Unit	
		1.5.2 Load Defaults	
	1.6 Security	1.6.1 Authentication Algorithm	Open System
		1.6.2 Default Key ID	
		1.6.3 Pre-authentication	Disabled
		1.6.4 Privacy Option Implemented	
		1.6.A WEP Key #1	
		1.6.B WEP Key #2	
		1.6.C WEP Key #3	
		1.6.D WEP Key #4	
2.Advanced Settings	2.1 Translation Mode		Enabled
	2.3 Performance	2.3.1 Dwell Time (*Access Points only*)	128 msec
		2.3.2 RTS Threshold	120 bytes
		2.3.5 Maximum Multicast Rate	1 Mbps
		2.3.6 Power Save Support	Disabled
		2.3.7 DTIM Period	4
		2.3.8 IP Stack	Enabled
		2.3.9 Acknowledge Delay	Regular
		2.3.A P.S. Broadcast Reservation Percentage	30
	2.4 Radio	2.4.1 Hopping Standard	US FCC
		2.4.2 Display Site Proprietary Sequence	
		2.4.3 Power level	High
	2.5 Rate	2.5.1 Multi-Rate Support	Enabled
	2.6 AP Redundancy Support		Disabled

Table 3-1 (continued). Configuration Menus

Menu	Sub-Menu	Sub-Submenu	Default Values
	2.7 Maintenance	2.7.1 Auto Calibration 2.7.2 Wait for Association Address 2.7.3 Japan Call Sign	Enabled (not in Access Points)
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 3.2.3 Stop Statistics	RX only
	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 Access Points		
4. Access Control	4.1 Change Access Rights	4.1.0 User 4.1.1 Installer 4.1.2 Technician	Installer
	4.2 Change Installer Password		“User”
	4.S Show Current Access Right		

3.3 Main Menu

```
Pro 11 Series (Workstation Bridge)
Version: 4.211
Date: 25 Jun 1998 15:46:24
Monitor
 ====================
1 - System Configuration
2 - Advanced Settings
3 - Site Survey
4 - Access Control

Select option >
```

Figure 3-1. Main Menu.

3.4 System Configuration Menu

```
Pro 11 Series (Workstation Bridge)
Version: 4.4.1
Date: 26 May 1999 15:46:24
Monitor
 ========================
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's Mode –** Identifies the unit's function. For example, if the unit is an Access Point, "AP" appears in this field.
- **Unit's HW Address –** Displays the unit's unique MAC address.
- **Unit's WLAN Address (Station Adapters or Workgroup Bridges) –** The address associated with the unit. For the Single-Port Station Adapters, this is the address of the PC. For the Four-Port Station Adapters and Workgroup Bridges, this is the MAC address of the unit. This field does not appear when the unit is an Access Point.
- **Station Status (Station Adapters or Workgroup Bridges) –** Current status of the station. This field does not appear when the unit is an Access Point. There are three options:

  Scanning – The station is searching for an Access Point with which to associate.

  Sync Waiting for Address – The station is synchronized with an Access Point but has not yet learned its WLAN MAC address (this option is relevant only to the Single-Port Station Adapters). The Access Point does not forward packets to the station when it is in this mode.

  Associated – The station is associated with an Access Point and has adopted the attached PC MAC address (for Single-Port Station Adapters) or uses the unit's hardware address (Four-Port Station Adapters and Workgroup Bridges), and is receiving packets from the LAN.

- **AP Address (Station Only) –** For stations, this parameter indicates an address of the Access Point with which the unit is currently associated.
- **Total Number of Associations Since Last Reset (Station Only) –** For stations, this indicates the total number of associations and disassociations with various Access Points. This is usually an indication of roaming.
- **Current Number of Associations (Access Point Only) –** Total number of stations currently associated with this Access Point.
- **Maximum Number of Associations Since Last Reset (Access Point Only) –** Maximum number of stations that were associated with an Access Point since the last reset.

- **Current Number of Authentications (Access Point Only) –** Total number of stations currently authenticated with an Access Point. A station may be concurrently authenticated with several Access Points, but is associated with only one Access Point at a time.

- **Maximum Number of Authentications Since Last Reset (Access Point Only) –** Maximum number of stations that were authenticated with an Access Point since the last reset.

3.4.2 IP AND SNMP PARAMETERS

All Pro 11 units contain IP Host software. This software can be 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 –** Type **0** to disable SNMP trap sending. Type **1** to enable SNMP trap sending. When an event occurs, a trap is sent to the defined host address (see **Appendix A** for a list of traps). You can configure the host address to which the traps are sent through SNMP management.

- **Display Current Values –** Type **A** to display 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 (Access Points 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 Access Point is co-located in the same area (even if they are not part of the same network) it is best to assign a different hopping sequence to each Access Point.

  Hopping sequences are grouped in three hopping sets (see the next parameter). When setting up multiple Access Points 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 the LW0050A and LW0055A Pro 11 Access Point models. It is not accessible from any other Pro 11 unit. During the association process, all other stations learn the hopping sequence from the Access Point. Different co-located WLAN segments should use different hopping sequences.

- **Hopping Set (Access Points Only) –** Hopping set (between 1 and 3) of the unit. Hopping sequences are grouped in several hopping sets. Always use the same hopping set per site.

The number of hopping sequences per set is different for each hopping standard according to this table:

Hopping Standard	# of Sequences per Hopping Set
Australia	20
Canada	10
Europe ETSI	26
France	11
Israel	11
Japan	4
Korea	4
Netherlands	5
Spain	9
US FCC	26

- **ESSID –** The ESSID (up to 32 printable ASCII characters) of the unit 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 Access Point that has the same ESSID. Use different ESSIDs to segment the WLAN network and add security.

NOTE

The ESSID parameter is case-sensitive.

- **Maximum Data Rate –** Maximum data rate of the unit. 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 Pro 11 unit dynamically selects the antenna where reception is optimal. In contrast, the unit selects the antenna from which it will transmit before transmission. 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 (transmit power amplifier with a 250-mW output) or an LNA (low-noise receive amplifier) use only a single antenna for transmission. There are three possibilities for configuration: 1) use two antennas, 2) use Antenna no. 1 only, or 3)use Antenna no. 2 only.

- **Mobility –** Pro 11 stations optimize their roaming algorithms according to the Mobility 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 (Mobility). Type **2** for stations that may move at speeds of over 30 km per hour.

  Medium (Mobility). Type **1** for stations that may move at speeds of over 10 km per hour, but not over 30 km per hour.

  Low (Mobility). Type **0** for stations that will not move at speeds of over 10 km per hour. Stationary is the default value, and in almost all cases this is the best choice.

- **Load Sharing –** Type **1** to enable Load Sharing. When installing a Wireless LAN network in a high-traffic environment, you can increase the aggregate throughput by installing multiple Access Points to create co-located cells. Load Sharing allows the wireless stations to distribute themselves evenly among the Access Points to best divide the load between the Access Points.

NOTE

When working in Load Sharing mode, both the Access Points and the units should be configured to Load Sharing Enabled.

- **Preferred AP MAC (Ethernet) address of the preferred Access Point —** You can configure a station to prefer a specific Access Point unit. When the station powers up, it will associate with the preferred Access Point even if the signal from that Access Point is lower than the signal from other Access Points. The station will roam to another Access Point only if it stops receiving beacons from the preferred Access Point.

- **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 (Access Points Only) –** The options are:

  Reject Unknown – Type **0** to allow transmission of packets only to stations that the Access Point 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 Access Point recognizes as being on its wired Ethernet side.

- **Intelligent Bridging Period –** Intelligent bridging enables smooth roaming of Workgroup Bridges. When intelligent bridging is enabled, the Access Point goes into a special bridging mode for a fixed amount of time whenever a wireless bridge roams into its area. This mode causes the Access Point to forward packets destined for the stations behind the Workgroup Bridge 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 Access Point 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 Access Point will remain in special mode.

NOTE

When connecting very large networks, we recommend setting this parameter to Forward Unknown.

- **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 only IP traffic to pass through the WLAN.

- **Tunneling –** Whether the unit performs tunneling. Enable AppleTalk® tunneling if the network contains a mix of EtherTalk1 (ET1) and EtherTalk2 (ET2) stations to ensure smooth communications. Enable IPX tunneling if IPX protocol is running over your network. Be sure to set all units to the same tunneling setting.

- **Broadcast Relaying (Access Points Only) –** Whether the unit performs broadcast relaying. When Broadcast Relaying is enabled, Broadcast packets originating in WLAN devices are transmitted by the Access Point 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 for the wired LAN.

- **Unicast Relaying –** Whether the unit performs Unicast relaying. When Unicast Relaying is enabled, Unicast packets originating 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 for the local wired LAN.

3.4.5 Station Control

The Station Control Menu contains the following options:

- **Reset Unit –** Type **1** to reset the Pro 11 unit and apply any changes made to the system parameters.

- **Load Defaults –** When this option is implemented, system parameters revert to the original factory-default settings. There are two options:

  Load Full Factory Defaults – All parameters revert to defaults except for Japan Call Sign (if applicable) and Hopping Standard.

  Load Partial – All parameters revert to defaults, except for Japan Call Sign (if applicable), IP Address, Subnet Mask, Default Gateway, Hopping Sequence, Hopping Set, ESSID, Transmit Diversity, Long Range, Preferred AP, IP Filtering, Hopping Standard, Power Level, Auto Calibration, Encapsulation, WEP Attributes, Authentication Algorithm, Pre-authentication, WEP Default Keys, Ethernet Disable, and Trap Host Addresses.

3.4.6 Security (Authentication Feature)

Wired Equivalent Privacy (WEP) is an authentication algorithm which protects authorized Wireless LAN users against eavesdropping. WEP is defined in the 802.11 standard.

WEP, also referred to as the Privacy option, must be ordered specifically and is not supported by default. The security mechanism involves configuration of the following parameters:

- **Authentication Algorithm —** This module operates in two modes: **0–Open System** (default): no authentication, or **1–Shared Key authentication** (for systems that have the privacy option implemented).
- **Default Key ID —** The key to be used for the encryption of transmitted messages.
- **Pre-authentication —** Set this parameter to Enabled when there is a great deal of roaming between the Access Points. Pre-authentication must be activated on both the Access Points and the stations.
- **Privacy Option Implemented —** Yes if Shared Key authentication is supported, No if Shared Key authentication is not supported.
- **WEP Key#1–4 —** The four encryption keys must be set before you can use the Shared Key Authentication Mode. The encryption keys you enter for the Access Point must match those defined in the stations. Each key is a combination of 10 Hex digits.

NOTE

We recommend changing the encryption keys periodically to enhance system security.

3.5 Advanced Settings Menu

```
Pro 11 Series (Workstation Bridge)
Version: 4.4.1
Date: 26 May 199p 15:46:24
Advanced Settings 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.

Modification of most of the parameters in the Advanced Settings menu is limited to certified Black Box Technical Support only.

3.5.1 Translation Mode

The translation mode determines how the unit handles 802.3 packets. The translation mode is either enabled (default) or disabled.

3.5.2 Performance

The Performance menu determines the unit performance:

- **Dwell Time (Access Point Only) —** The time spent on a radio channel before hopping to the next channel in the sequence.
- **RTS Threshold –** Minimum packet size to require an RTS. For packets with a size below RTS Threshold value, an RTS is not sent and the packet is transmitted directly to the WLAN.
- **Max Multicast Rate —** Multicast and Broadcast transmissions are not acknowledged, so the chance of error increases. By default, the unit will always transmit broadcasts, multicasts, and control frames at the minimum possible rate, 1 Mbps.

- **Power Save Support —** If you enable Power Save Support on one of the WLAN stations (LW0054A or LW0059A only), you must also configure the Access Point unit. Power Save Support is influenced by two parameters:

  DTM interval on the Access Point side — Determines at which interval the Access Point will send its broadcast traffic (default 4 beacons).

  Listen interval on the LW0054A or LW0059A — Determines when the station will "wake up" to listen to unicast packets which are destined to it (default value: 4 beacons).

- **DTIM Period —** Determines at which interval the Access Point will send its broadcast traffic to all the stations in the cell, both stations that are in power-save mode and to stations that are *not* in power-save mode (normal mode). When stations that are in power-save mode "wake up" to receive broadcast frames, they can also poll the Access Point for the unicast frames if there are any stored in the Access Point's buffer. Default value is 4 beacons (approximately every 1 second).

- **IP Stack —** By default this parameter is disabled, to check connectivity. Any changes to this parameter will be returned to the default value whenever the unit resets.

- **Acknowledge Delay —** Enlarges the range of system but can only be enabled for links above 20 km. It must be enlarged on both sides. The values are Long or Regular (default) and can be configured by an Installer or Technician.

- **P.S. Broadcast Reservation Percentage —** Determines the buffer space reserved for broadcast frames in percentages. Default value is 30% (auto storing—no reservation). Allowed range is 0 to 30%.

NOTE

We recommend leaving it at the default setting.

3.5.3 RADIO

The Radio menu contains the following parameters:

- **Hopping Standard –** 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. Use this parameter to set the unit's hopping standard to that of the relevant country.

- **Power Level –** Output power level at which the unit is transmitting. There are two possibilities, Low (4 dBm) or High (17 dBm), at the antenna connector.

3.5.4 Rate

- **Multi-Rate Support –** When this parameter is enabled, the unit will automatically switch to the best transmission rate at any given time. When the parameter is disabled, the unit will always stay at the maximum rate configured in the WLAN Parameters menu.

3.5.5 Access Point Redundancy Support

When the Access Point identifies that the Ethernet link has been discontinued over a defined period of time, it then stops transmitting and forces the stations associated with it to associate with another Access Point.

The default mode for the Access Point Redundancy Support parameter is disabled (the Access Point continues transmitting even when the ETH link is discontinued). This can only be configured by a Technician (see **Section 3.7**, **Access Control Menu**). We recommend using this parameter only when more than one Access Point is connected to the same distribution system and this Access Point is configured to the same ESSID.

3.5.6 Maintenance

The Installer has access to modify the following parameters of the Maintenance menu:

- **Auto Calibration –** When the unit is started, it performs an internal self-test. A part of this test is automatic calibration of the DC Offset and deviation pattern.

- **Japan Call Sign –** The Japan Call Sign is part of the Japanese standard, defined according to local regulations. The Japanese Ministry of Communications supplies an activation code for the units; this code is set in the factory for each unit.

3.6 Site Survey Menu

```
Pro 11 Series (Workstation Bridge)
Version: 4.4.1
Date: 26 May 1999 15:46:24
Site Survey menu
 ==================
1 - System Counters
2 - Survey Software
3 - Event Log
4 - Display Neighboring APs

Select option >
```

Figure 3-4. Site Survey Menu.

The Site Survey Menu allows performing a site survey that helps you position your units and align their antennas of the units, as well as perform troubleshooting.

3.6.1 System Counters

The System counters are a simple yet efficient tool for monitoring, interpreting, and analyzing 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. Read further in **Section 3.6.1** for a detailed description of the counters.
- **Display Rate Counters —** Displays contents of packets at each rate. The Access Point displays counters per station.
- **Display Rx Packets per Frequency —** Histogram of the number of frames received on each channel.
- **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 counters per station, the number of transmitted frames, and the number of discarded frames. This applies only to Access Points.

3.6.1.1 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 –** Indicated the total number of frames that have been received from the Ethernet port. This counter includes both bad and good frames.
- **Received Bad Frames –** The number of frames with errors received from the UTP port. A large number of received bad frames indicates a problem in the UTP connection such as a bad UTP cable or hub port.
- **Received good frames –** The number of good frames (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 (frames that have been received from the Wireless side, and frames generated by the unit itself).

3.6.1.2 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, 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 also the number of control and management frames.

  Notice that an Access Point 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 Access Point is not connected to an active LAN.

- **Total Transmitted Frames (Bridge) –** The total number of data frames transmitted to the wireless media (that is, frames that were received from the UTP port and forwarded to the internal bridge, which decided to transmit them to the wireless media).

- **Frames Dropped (too many retries) –** The number of frames which have been dropped because 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 also 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 be about the same as 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 Access Point discarded because of 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 –** Total number of buffered frames that were aged out. This counter counts the number of frames dropped by the Access Point because a station did not poll those frames for a long period of time.
- **Power Saving Free Entries –** The current number of free buffers (one frame each) available for power-save management. These buffers hold messages for stations that are currently in Power Save mode.
- **Total Received Frames –** The number of frames received from the wireless media. The count includes data and control frames (including beacons received from Access Points).
- **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 the Duplicates and Dwell Timeouts parameter below).
- **Bad Fragments Received –** The number of frames received from the WLAN with errors.
- **Duplicates and Dwell Timeouts –** When a unit receives a frame, it sends an acknowledge for it. If the acknowledge is lost, it receives a copy of the same frame. Although duplicate frames are counted, only the first copy of the frame is forwarded to the UTP port.

3.6.1.3 Display Rate Counters

The rate counters display the number of frames transmitted in each data rate since the last reset. The rate counters show the number of frames transmitted at 1 Mbps, 2 Mbps, 3 Mbps, and the number of retransmitted frames (Ret). The counters display the rate of packets transmitted for the first time only (without retransmission).

NOTE

Counters for Access Points are displayed for all associated stations, indicated by their MAC address. Rate counters for stations are displayed with no indication of MAC address.

Checking the rate counters is the best way to determine which data rate is the optimal data rate for the unit. We recommend restricting the Maximum Data Rate for each unit according to the Rate counters (see also **Section 3.4.3**). The Ret counter displays the number of frames that had to be retransmitted; however, it does not count the number of retransmissions that actually accrued.

3.6.1.4 Using the Rx Packets per Frequency Histogram

Use the Display Rx Packets per Frequency option to see a histogram of the number of frames received on each channel.

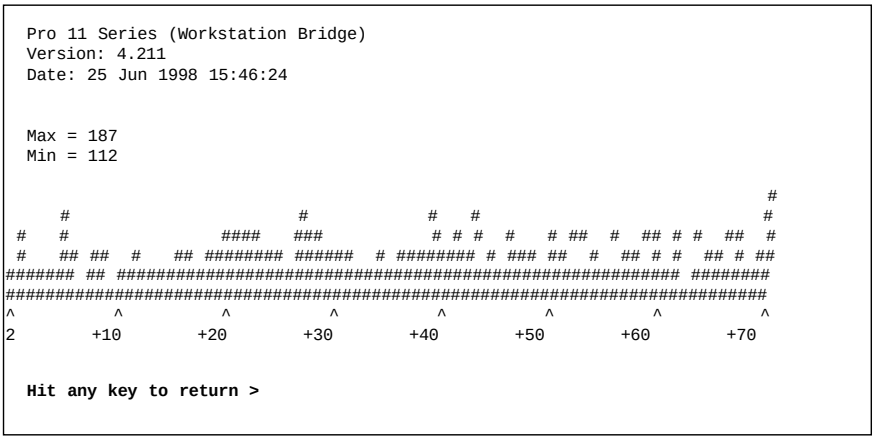


Figure 3-5. Display Rx Packets per Frequency.

Each point of the histogram line corresponds to a frequency. The base frequency appears at the far left, and gradations are marked in steps of ten along the line. A hash (#) represents each packet received on a given frequency. The Max and Min values indicate the highest and lowest number of frames received across all frequencies. This graph is very useful for tracking interference. Frequencies with small numbers of packets received probably have more interference than other frequencies.

3.6.1.5 Reset All Counters

This option allows you to reset the system counters, Ethernet counters, WLAN counters, and Rate counters.

- Click **1** to reset all counters.
- Click **0** to cancel request.

3.6.1.6 Power-Saving Counters

These counters apply only to Access Points.

- **PS stations —** Number of associated stations currently working in Power Save mode.
- **Internally Discarded —** Number of frames that were discarded because of aging.
- **Table —** Valid only when Power Save mode is enabled.

  Station ID — Current number of buffered frames per station.

  Aged — Number of buffered frames that were aged out from buffer per station.

  Send — Number of buffered frames that were sent to a specific station.

  Queue — Number of frames that could not be stored in the buffer.

3.6.2 Survey Software

The Survey Software 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).
- **Start Statistics –** Type **2** and then press any digit to start Site Survey.
- **Stop Statistics –** Type **3** and then press any key to stop update of Site Survey statistics.

3.6.3 Using 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. Type **1** to access 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 Access Point (transmitting from the station to the Access Point), 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 3-6). This list is updated continuously. Select option (3) to stop sending packets.

```
Pro 11 Series (Workstation Bridge)
Version: 4.211
Date: 25 Jun 1998 15:46:24
# 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

Hit any key to return >
```

Figure 3-6. Transmit Statistics.

6. On the receive side of the link, the screen displays a table showing the packet number received, the frequency at which each packet was transmitted, the Received Signal Strength Indicator (RSSI) for each antenna, and the antenna that was selected for reception (refer to Figure 3-7). Use only the RSSI reading from the selected antenna.

# Pack	Ant	RSSI1	RSSI2	Bit_Err	Freqs	Rate	Quality
105	1	92	84	0	76	2	#########..
106	1	92	82	0	75	2	#########..
107	1	89	89	0	58	2	########...
108	1	95	92	0	51	2	##########.
109	1	95	89	0	46	2	##########.
110	1	95	81	0	10	2	##########.
111	1	95	90	0	31	2	##########.
112	1	95	51	0	4	2	##########.
113	1	92	85	0	5	2	#########..
114	1	99	90	0	77	2	##########.
115	1	102	89	0	43	2	##########
116	1	95	89	0	22	2	##########.
117	1	105	86	0	58	2	##########
118	1	103	89	0	51	2	##########
119	1	102	89	0	46	2	##########
120	1	104	69	0	64	2	##########
121	1	97	87	0	78	2	##########.
122	1	100	87	0	33	2	##########
123	2	87	85	0	71	2	########...
124	2	82	85	0	70	2	########...

Figure 3-7. Receive Statistics.

7. The RSSI is given in arbitrary units. Use the following graph to correlate RSSI to dBm.

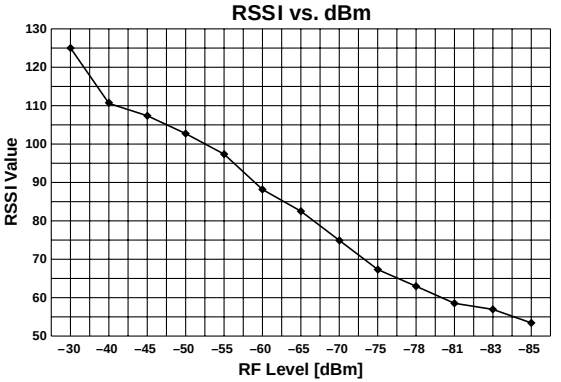


Figure 3-8. RSSI to dBm Graph.

8. Re-align the antennas until the maximum received signal strength is attained. As you align the antennas, the RSSI (received signal strength indicator) continually increases until it reaches a certain level, after which it begins to decrease. That highest point is the maximum attainable RSSI level, indicating optimum receive antenna alignment.

9. Switch the functions of either side of the link (set the transmit unit to receive and the receive unit to transmit) and repeat the procedure to check the link from the opposite direction.

3.6.4 Event Log

- **Display Event Log —** The error messages that the unit displayed since the last Load Full Factory Defaults reset or since the log was erased by Erase Event Log. The Event log stores events in four levels of error notifications: MSG (Message), WRN (Warning), ERR (Error), and FTL (Fatal).
- **Erase Event Log —** Erases the event log.
- **Event Storage Policy —** Defines severity policy for storage level of the event log. There are four levels of storage policy:

  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.

3.6.5 Display Neighboring Access Points

Displays neighboring Access Points on the same ESS for both the Access Point and the station units.

3.7 Access Control Menu

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

```
Pro 11 Series (Workstation Bridge)
Version: 4.211
Date: 25 Jun 1998 15:46:24
Access Control menu
 ==================
1 - Change Access Rights
2 - Change Installer Password
3 - Show Current Access Right

Select option > 1
```

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 Pro 11 unit's setup and configuration menus. When the unit is first installed, the default access right is 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 an authorized technician 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.

4. PCMCIA Adapter Installation, Setup, and Management

This chapter describes how to install the PCMCIA Adapter and its associated firmware, drivers, and utilities. The PCMCIA Adapter Configuration and Site Survey utilities, which are used to set up and manage the card, are also described in this chapter.

4.1 Packing List

The PCMCIA Adapter package should contain:

- PCMCIA Adapter (LW0054A or LW0059A).
- Drivers diskette.
- Utilities diskette.
- Installation and Users' Guide.

4.2 Before You Begin

- Verify that the Access Point you are going to use is compliant with the 802.11 standard.

  Turn on the Access Point before installing the PCMCIA Adapter, so you can use the PCMCIA Adapter's LEDs to check the status of the PCMCIA Adapter when installation is complete. See **Section 4.3.2** for more information about the LEDs.

- When installing in Windows® 95/98, verify that you have the Windows CD with you, or that the Windows CAB files are installed on your local hard disk in a directory whose name does not exceed eight letters. When the CAB files are on the disk, they are usually found in **C:\Windows\Options\Cabs**.

- When installing in Windows NT®, verify that you have the Windows NT CD with you, or that the Windows NT distribution files are installed on your local hard disk. During installation, enter the path of the distribution files whenever a message appears asking for them.

- We highly recommend that you remove all PCMCIA cards from the notebook prior to installing the PCMCIA Adapter. This will help to avoid conflicts during installation. If you have another network card installed (for example, an Ethernet card), you *must* remove it prior to installing the PCMCIA PC Card.

4.3 Installing the PCMCIA Adapter

Installing the PCMCIA Adapter consists of the following installation steps:

- Installing the card in a PCMCIA slot
- Installing the PCMCIA Adapter drivers and utilities

Section 4.3.3 provides instructions on performing initial configuration of the Card. **Section 4.8** provides installation troubleshooting information.

NOTE

If you are installing the card under Windows 95 or Windows 98, there are two installation options. You can install the drivers and utilities separately, or you can use the Upgrade Kit program to install all components in one session. The Upgrade Kit program is described in Section 4.7.

4.3.1 Installing the PCMCIA Adapter Drivers

The PCMCIA Adapter can be installed to operate under a wide range of PC operating systems. The following table lists the supported operating systems, together with the section number in this guide which describes the relevant installation procedure.

If you are installing the PCMCIA Adapter under:	Refer to:
Windows 98	**Section 4.3.1.1**
Windows 95A	**Section 4.3.1.2**
Windows 95B	**Section 4.3.1.3**
Windows NT	**Section 4.3.1.4**
ODI (DOS)	**Section 4.9**

4.3.1.1 Installing the PCMCIA Adapter Drivers in Windows 98

1. Insert the PCMCIA Adapter in a free PCMCIA slot. Windows detects the unit and displays the **New Hardware Found** window.

2. When the **Add New Hardware Wizard** window appears, press **Next**.

3. Select the **Search for best driver** option and press **Next**.

4. Insert the Black Box drivers diskette, select the **Floppy disk drives** option, and press **Next**.

5. The installation wizard notifies you that the driver for the Brz 802.11 Wireless LAN PC Card has been located. Press **Next**.

6. A window appears notifying you that the driver for the Brz 802.11 Wireless LAN PC Card has been installed. Press **Finish**.

7. Restart the computer.

Uninstalling the PCMCIA Adapter Drivers in Windows 98

1. Press the **Windows Start** menu, select **Settings**, and then select **Control Panel**. Double-click on the **Network** icon, click the **Configuration** tab, select **Brz 802.11 Wireless LAN PC Card**, and click **Remove**.

   A message appears asking whether you want to restart the computer; click **No**.

2. Insert the Black Box Drivers diskette. Press the **Windows Start** menu, select **Run**, and type `a:\DrvClean`.

3. When notified that the PCMCIA PC Card driver has been deleted, click **Setup**.

4. Restart the computer.

Installing the PCMCIA Adapter Drivers in Windows 95

Check which version of Windows 95 operating system your PC is running:

1. From the Windows 95 desktop, right-click the **My Computer** icon and select **Properties**. The **System Properties** window opens.

2. Click the **General** tab. The letter indicating the type of operating system (**a** or **b**) is displayed under the **System** heading.

3. If you are running the Windows 95A operating system, refer to **Section 4.3.1.2**. If you are running the Windows 95B operating system, refer to **Section 4.3.1.3**.

4.3.1.2 For Windows 95A

1. Insert the PCMCIA Adapter in the PCMCIA slot on your computer. Windows 95 detects the unit and displays the **New Hardware Found** window.

2. Select the **Driver from disk provided by hardware manufacturer** option and press **OK**.

3. When prompted for the location of the driver, insert the Black Box drivers diskette and type A:\ and press **OK**. The necessary files are copied from the diskette.

4. When **Please insert disk labeled Windows 95 CD-ROM** appears, insert the Windows 95 CD and press **OK**. If the Windows 95 CAB files are located on your local hard disk, you can point to that directory (usually found in **\Windows\Options\Cabs**).

5. If this is the first time a network card has been installed on this PC, a network setup window may appear. It is not necessary to fill out this window for the purposes of this installation.

6. Restart the computer.

4.3.1.3 Installation for Windows 95B

1. Insert the PCMCIA Adapter in the PCMCIA slot on your computer. Windows 95 detects the unit, briefly displays the **New Hardware Found** window, and then displays the **Update Device Driver Wizard** window.

2. Insert the Black Box drivers diskette and press **Next**. When Windows 95 notifies you that it has found the driver, press **Finish**.

3. If the Windows 95 CAB files are not found automatically, the message **Please insert disk labeled Windows 95 CD-ROM** appears. Press **OK**.

4. If the file **BRZCOM.VXD** is not found, direct the window to **A:** and press **OK**.

5. If no other windows appear, the installation is complete. If **Please insert disk labeled Windows 95 CD-ROM** appears, press **OK**, enter the path of the Windows 95 CAB files, and press **OK**. Installation is now complete.

6. Restart the computer.

UNINSTALLING PCMCIA ADAPTER DRIVERS IN WINDOWS 95

1. Press the Windows **Start** button, select **Settings**, and then select **Control Panel**. Double-click on the **PC Card** icon, select **Wireless LAN PC Card**, and click **Stop**. Close all active applications.

   When asked to restart the computer, press **No**.

2. From the Windows **Start** menu, select **Settings**, and then select **Control Panel**. Double-click on the **Network** icon, click on the **Configuration** tab, select **Brz 802.11 Wireless LAN PC Card**, and click **Remove**.

3. Insert the Black Box Drivers diskette. From the **Windows Start** menu, select **Run**, and type `a:\DrvClean`.

4. When notified that the PCMCIA PC Card driver has been deleted, click **Setup**.

5. Restart the computer.

4.3.1.4 INSTALLING THE PCMCIA ADAPTER DRIVERS IN WINDOWS NT

1. Press the Windows **Start** button, select **Settings**, and then select **Control Panel**. Double-click on the **Network** icon.

2. If the message **The Windows NT Networking is not installed. Do you want to install it now?** appears, continue with step 2a. If this message does not appear, continue with step 2b.

   a. Press **Yes** and choose **Wired to the network**. When a list of supported network adapters appears, press **Have Disk**.

   b. Click on the **Adapters** tab, press **Add**, and then click **Have Disk**.

3. Insert the Black Box drivers diskette, enter the location of the diskette (such as `a:\`) and press **OK**.

4. From the list choose **Brz 802.11 Wireless LAN PC Card** and press **OK**. The **PCMCIA PC Card LAN Adapter Properties** window appears.

5. The default settings are memory range D0000h to D3FFFh, IRQ 11. In the following steps we will verify that these default settings are acceptable for your machine.

NOTE

If the PCMCIA PC Card Configuration utility is already installed, you can access it directly by pressing Advanced**.**

6. Press the Windows **Start** button and select **Run**. Type `WINMSD` and press **OK**. The **Windows NT Diagnostics** window appears.

Figure 4-1. Windows NT Diagnostics Window.

7. Press **IRQ** and verify that IRQ 11 is not taken. If it is, find a free IRQ. For example, in the illustration, IRQ 2 is free.

8. Press **Memory** and verify that memory from D0000h to D3FFFh is not taken. If it is, find another free memory location, such as E0000h.

9. Return to the **PCMCIA PC Card LAN Adapter Properties** window. If the default values for Memory Address and Interrupt are acceptable, press **OK**. Otherwise, enter new values and press **OK**.

10. Press **Close** to close each installation window.

11. If configuration windows for other network components (such as Protocol) appear, enter the requirements according to the instructions of your network administrator.

12. Restart Windows NT.

UNINSTALLING PCMCIA ADAPTER DRIVERS IN WINDOWS NT

1. From the Windows **Start** menu, select **Settings**, and then select **Control Panel**. Double-click on the **Network** icon, click on the **Configuration** tab, select **Brz 802.11 Wireless LAN PC Card**, and click **Remove**.

2. Insert the Black Box Drivers diskette. From the Windows **Start** menu, select **Run**, and type `a:\DrvClean`.

3. When notified that the PCMCIA Adapter driver has been deleted, click **Setup**.

4. Restart the computer.

4.3.2 CHECKING THE LED INDICATORS

Verify correct operation of the PCMCIA Adapter using the LED indicators:

Color	Description	Meaning
Yellow	Link Status	Blink – Scanning Solid – Associated
Green	Data Traffic	Blink – According to traffic

The LED indicators are useful only if there is an active Access Point in the area.

The LED indicators can be used to verify correct firmware download procedure; the LEDs turn on and off quickly, one LED being ON while the other is OFF.

4.3.3 INITIAL CONFIGURATION

If your wireless network uses a non-default ESSID, enter the proper ESSID as follows:

1. Start the **WLAN PC Card Configuration** utility as described in **Section 4.5**. From the **Windows Start** menu, select **Programs - Brz 802.11 Utilities**, and then **Configure**.

2. Edit the ESSID parameter. Click the **WLAN Parameters** tab and enter the ESSID that matches the Access Point.

3. Restart the computer.

4.4 Installing the PCMCIA Adapter Utilities

If a previous version of the PCMCIA Adapter utilities is installed, uninstall it before reinstalling the new version (as described in **Section 4.4.1**).

To install the PCMCIA PC Card utilities:

1. Insert the Black Box utilities diskette.
2. From the Windows **Start** menu, select **Run**. Type `A:\setup` and click **OK**.
3. When the notification dialog box appears, click **Setup**.
4. In the **Utilities** window, choose a location for the installation, then click **OK**.
5. When the **Setup Complete** window appears, click **OK**. Icons for the utilities are added to the **Windows Programs** menu, and a **WLAN PC-Card Configure** icon is added in the **Control Panel**.

4.4.1 Uninstalling PCMCIA Adapter Utilities

1. From the Windows **Start** menu, select **Programs–WLAN Utilities** and then select **Uninstall**.
2. You can also uninstall the PCMCIA Adapter utilities by using **Windows Add/Remove Programs** feature.

4.5 Using the Wireless LAN Configuration Utility

This section describes how to use the Wireless LAN Configuration utility to configure and manage your PCMCIA Adapter.

Access the PCMCIA PC Card Configuration utility as follows:

- Click the **Start** button, select **Programs**, select the **WLAN Utilities** program group, and choose **Configure**.

The **Wireless LAN Configuration** main window opens, with the **Station Status** tab selected.

The **Wireless LAN Configuration** main window contains several tabs, as described in the following sections. In addition, the Configuration windows contain the following buttons:

- *OK* – Implements any changes you made and closes the window.

- *Undo* – Causes the window to display currently active values. This is useful if you started changing values and you want to start again from the current values.
- *Cancel* – Closes the window without implementing any changes you made.
- *Apply* – Implements any changes you made but leaves the window open.

4.5.1 Station Status Tab

The **Station Status** tab of the **Wireless LAN Configuration** utility displays information regarding the Adapter and its status.

The **Station Status** tab contains the following parameters:

- *Network Type* – In the current version, the value of this parameter should be always set to **Infrastructure**.
- *Firmware Version* – Displays the version of unit's current firmware (internally installed software). The first two numbers of the firmware and driver versions should be identical. The remaining numbers (if any) indicate the minor version. The final letter indicates the hardware version.
- *Driver Version* – Displays the version of unit's current driver.
- *MAC Address* – Displays the unit's unique IEEE MAC address.
- *BSS Address* – The MAC address of the Access Point with which the unit is currently associated.
- *Station Status* – Current status of the unit.

  Scanning – The unit is searching for an Access Point with which to associate.

  Associated – The unit is associated with an Access Point and has adopted the attached PC MAC address.
- *WEP Enabled* – Wired Equivalent Privacy (WEP) is an authentication algorithm which protects authorized Wireless LAN users against eavesdropping. WEP is defined in the 802.11 standard.

NOTE

Parameter changes take effect only after reset.

4.5.2 WLAN Parameters Tab

The **WLAN Parameters** tab of the **Wireless LAN Configuration** utility lets you view and edit basic Wireless LAN parameters of the Adapter.

The **WLAN Parameters** tab contains the following parameters:

- *ESSID* – An ASCII string of up to 32 characters used to identify a WLAN. The ESSID prevents the unintentional merging of two co-located WLANs. The ESSID must be set to the same value in all stations and Access Points in the extended WLAN. Note that the ESSID is case-sensitive.
- *Maximum Data Rate* – By default, the unit adaptively selects the highest possible rate for transmission. Under certain conditions (for range/speed trade-off) you may decide not to use the higher rates. Possible values are 1, 2, or 3 Mbps.
- *Transmit Antenna* – By default, the unit dynamically selects the antenna where reception and transmission is optimal. If your model has an external antenna and uses only a single antenna, set Transmit Antenna to transmit only from that single antenna. Antenna number one is the antenna nearest the yellow LED.
- *Load Sharing* – When installing a Wireless LAN network in a high-traffic environment, you can increase the aggregate throughput by installing multiple Access Points to create co-located cells. Enable Load Sharing to cause your stations to divide their traffic equally between the available Access Points.

NOTE

Parameter changes take effect only after reset.

4.5.3 Station Control Tab

The **Station Control** tab of the **Wireless LAN Configuration** utility allows you to return the Adapter to default configuration values, and export/import configuration files.

The **Station Control** tab contains the **Default** button, which returns all parameters to factory-default values.

As a time-saving feature, you can configure one unit and then save the configuration as a file (with a .BRZ extension). You can later import the configuration file to other units.

- *Import* – Imports a configuration file to this unit, and overwrites all previous settings.
- *Export* – Exports the current configuration of this unit to a file.

NOTE

Parameter changes take effect only after reset.

4.5.4 Configuration Access Tab

The **Configuration Access** tab of the **Wireless LAN Configuration** utility lets you log into the Adapter as User, Installer, or Technician, and lets you change the password.

The **Configuration Access** tab displays the current mode (User, Installer, or Technician) in the **Present Mode** box. This mode determines the security access to system parameters. Users can view some of the window tabs, but cannot modify parameters. Installers can view all of the tabs and can modify some of the values. Technician access rights are reserved for authorized technicians.

When the Configuration utility opens, it will begin at the same mode that was active when it closed. If security is an issue, change the access mode to **User** before you close the utility. The first time the utility is opened, it is set to **Installer** access mode.

The default password for **Installer** mode is **User**. If security is an issue, change the Installer password.

To change the **Configuration Access** mode:

1. Select the radio button next to the desired mode.
2. Type in the password. (No password is necessary to *lower* the Access Right level.)
3. Click **Set Mode**. The name of the new mode appears in the **Present Mode** box.

To change the password for **Installer Configuration Access** mode:

1. Look at the **Present Mode** box to verify that you are in **Installer** mode.
2. Click **Change Password**.
3. In the **Change Password** dialog box, type in the new password twice and click **OK**. The password has changed.

IMPORTANT

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

4.5.5 Power Management Tab

The **Power Management** tab allows you to enable/disable **Power Save** mode and to configure **Power Save** mode parameters.

Power Save mode is intended for laptops and hand-held computers, in order to conserve battery energy. When **Power Save** mode is enabled, the unit "sleeps" most of the time and "wakes up" occasionally to transmit to and receive from the Access Point. This will extend the battery life span of a laptop with the PCMCIA Adapter installed.

NOTE

Expect a degradation in performance of the entire cell, even if only the Access Point and one station are set to Power Save mode.

The **Power Management** tab includes the following parameters:

- **Power Management Mode —** Enable **Power Save** mode by clicking the **Powersave** option; disable by clicking the **Normal** option (default).
- **Listen Interval Settings —** Specifies how often the station is to "wake up" in order to transmit or receive data (unicast packets). This parameter enables performance optimization on a per-station basis. In contrast, the DTIM period (that is, set in the Access Point only) defines the time period for all stations in the cell to "wake up" in order to receive broadcasts.

NOTE

If the Power Save mode is enabled on one of the WLAN's PCMCIA Adapter stations, you must also enable the Power Save mode on the Access Point through HyperTerminal.

4.5.6 Security Tab

The **Security** tab of the **Wireless LAN Configuration** utility allows you to set the security parameters of the station.

The station in which the PCMCIA Adapter is installed can use one of the following authentication algorithms (as defined in the 802.11 standard):

- **Open System —** Any station in the WLAN can associate with an Access Point and receive and transmit data (null authentication).
- **Shared Key —** Only stations using a shared key encryption identified by the Access Point are allowed to associate with it. You can only select this option if the card was ordered with the **Privacy** option or if you enabled the WEP feature during the upgrade procedure. The option which was ordered is displayed in a read-only field at the top of the dialog box. To see whether the WEP option was enabled during installation, select the Station Status tab described in **Section 4.5.1**.

Values:	**Unknown**	Adapter is not inserted.
	Implemented	Shared Key authentication is enabled.
	Not Implemented	Shared Key authentication is disabled. Only open system authentication is available in this mode.

If you selected the Shared Key algorithm, proceed to set the following parameters:

- **Default Key ID —** Sets the default key for encryption in the Authentication process. This is the encryption key that will be used for transmissions between the station and the Access Point.
- **WEP Key —** Define the encryption keys used for transmissions between the station and the Access Point. Specify each key by clicking the appropriate WEP Key row (First, Second, Third, or Fourth) and entering 10 Hex digits (5 pairs of characters) for each of the four keys.

To configure security parameters in ODI/DOS environment, use the brzsetup application.

NOTE

The default Key ID you enter for the PCMCIA Adapter must match the Key ID defined in the Access Point. Section 3.4.6 describes the procedure for setting the encryption keys for Access Points.

It is recommended that you change the encryption keys periodically to enhance system security.

4.5.7 Maintenance Tab

The **Maintenance** tab of the **Wireless LAN Configuration** utility allows you to cause the unit to verify firmware/driver compatibility, and set how the unit handles 802.3 packets.

This tab is not visible when in **User login** mode. When in **Installer login** mode, you can see the parameters. When in **Technician login** mode, you can edit the parameters.

The **Maintenance** tab contains the following parameters:

- *Version Information* – Windows drivers are divided into three files: Brzcom.vxd, Brzwlan.sys, and Brzwlan.inf. The version number of all these files must be identical. Control information of these files is displayed. The **Configuration utility file** is called **BrzConfig.exe**. The first two numbers of the Configuration utility version must match the first two numbers of the drivers.

- *Disable AppleTalk tunneling* — Allows you to disable (default) or enable AppleTalk tunneling if the network contains a mix of EtherTalk 1 (ET 1) and EtherTalk 2 (ET 2) stations to ensure smooth communications. Make sure all units are set to the same tunneling settings.

- *Show control on taskbar* — Check the box with an icon of the PCMCIA Adapter on the Windows taskbar. When this option is enabled, you can double-click the **PCMCIA Adapter** icon to display the **Wireless LAN Configuration** utility at any time.

4.5.8 Radio Tab

The **Radio** tab of the **Wireless LAN Configuration** utility allows you to set the power level of the unit and choose a hopping standard.

This tab is not visible when in **User login** mode. When in **Installer login** mode, you can see the parameters. When in **Technician login** mode, you can edit the parameters.

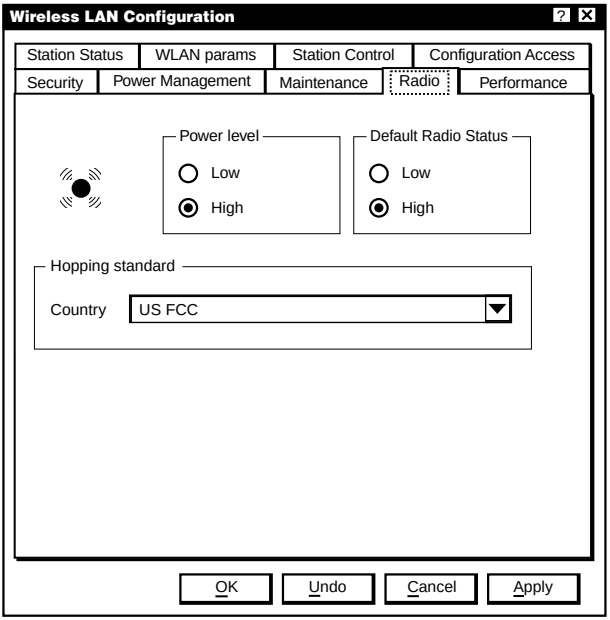


Figure 4-2. Radio Tab.

The **Radio** tab contains the following parameters:

- *Power Level* – Level of power at which the unit is operating. There are two possibilities, Low or High.
- *Default Radio Status* — For **on**, the radio receives in regular mode; when **off**, the radio does not work at startup. You would choose **off**, for example, when traveling in planes.
- *Hopping Standard* – 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. Use this parameter to set the unit's hopping standard to that of the relevant country. Proprietary hopping standards can also be implemented. Refer to **Section 3.5.3**.

4.5.9 Performance Tab

The **Performance** tab of the **Wireless LAN Configuration** utility allows you to fine-tune performance and roaming parameters.

This tab is not visible when in **User login** mode. When in **Installer login** mode, you can see the parameters. When in **Technician login** mode, you can edit the parameters.

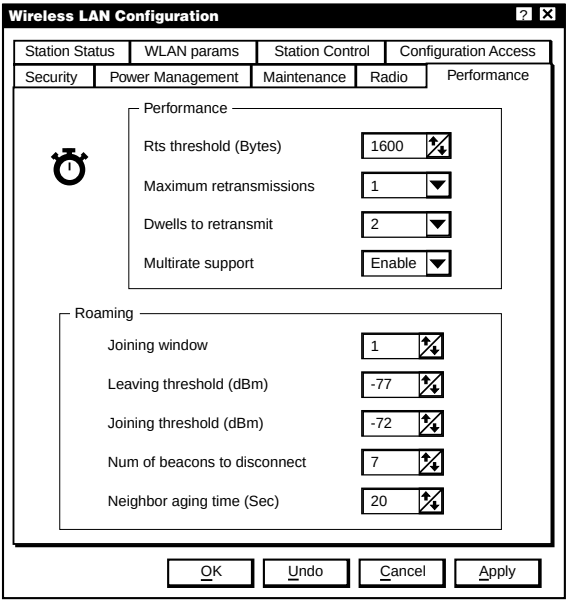


Figure 4-3. Performance Tab.

The **Performance** tab contains the following important parameter:

- *Rts threshold (bytes)* – Minimum packet size to require an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the WLAN.

4.5.10 Resetting the PCMCIA Adapter

It is necessary to reset the PCMCIA Adapter after making configuration changes via the **Wireless LAN Configuration** utility. Perform this procedure as follows:

1. Close the **Configuration and Site Survey** utilities and then do one of the following:

2. Restart the computer, or

   stop the Adapter: From the **Control Panel**, double-click the **PCMCIA Adapter** icon, select the **PCMCIA PC Card**, and click **Stop**. Then eject and reinsert the card, or

   stop and refresh the driver as follows:

3. Right-click the **My Computer** icon on the desktop, choose **Properties**, and go to the **Device Manager** tab.

Select **Network Adapters - WLAN PC Card**, and click **Refresh**.

4.6 Using the Site Survey Utility

NOTE

This utility cannot be used in systems installed under ODI.

This section describes how to use the **Site Survey** utility to manage your PCMCIA Adapter. The **Site Survey** utility keeps you informed of the signal strength your unit is receiving.

You can run a Site Survey to compare reception at various locations. This is extremely useful when first setting up the wireless LAN, since you can easily determine where reception is good or bad, and where many Access Points overlap.

The following sections describe how to access the **Site Survey** utility, how to read the main **Site Survey** window, and how to perform a site survey.

4.6.1 Accessing the Site Survey Utility

Open the **Site Survey** utility as follows:

- Click the **Start** button, select **Programs**, select the **WLAN Utilities** program group, and choose **Site Survey**.

The **Site Survey for Wireless LAN Card** main window opens.

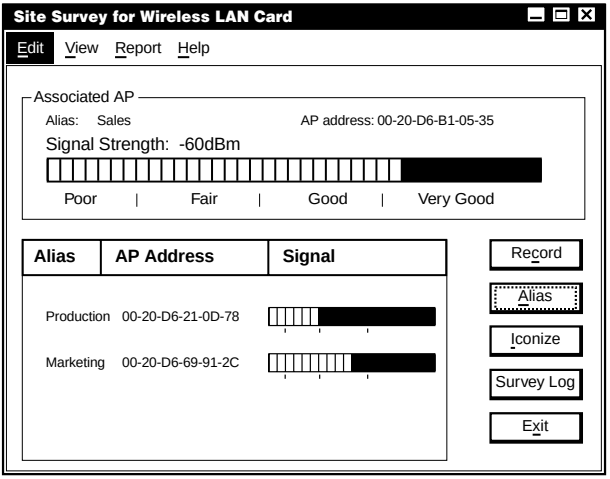


Figure 4-4. Site Survey utility.

4.6.2 Site Survey Main Window

The **Site Survey** main window contains the following sections:

- **Associated AP –** This section, located at the top of the window, displays various parameters regarding the Access Point with which the unit is currently associated.

  Alias – The alias you have assigned to the Access Point that the PCMCIA Adapter is currently associated with. To assign aliases to Access Point units, click the **Alias** button. If no alias has been assigned to the Access Point, this field displays "no alias."

  AP Address – The IEEE MAC address of the Access Point.

  Signal Strength – The strength of the signal from the Access Point in dBm. The table below maps the signal strength indicators to dBm ranges:

Signal	Poor	Fair	Good	Very Good
dBm	less than -74	-74 to -69	-68 to -61	greater than -61

  Signal Bar – The signal bar is a graphical representation of the signal strength. The longer the bar, the stronger the signal. As signal strength drops, the bar changes from green, to yellow, to red.

- **Neighbor APs –** This section, located at the bottom of the window, displays nearby Access Points (up to 4) from which the station is receiving a signal. For each Access Point, the following parameters are displayed:

  Alias – The alias you have assigned to the Access Point. To assign aliases to Access Point units, press the **Alias** button. If no alias has been assigned to the Access Point, this field displays "no alias."

  AP Address – The IEEE MAC address of the Access Point.

  Signal – A miniature signal bar indicating the current signal strength from the Access Point. When you hold the cursor over the line, the exact value appears.

The following buttons appear on the right side of the **Site Survey** window. Several of the buttons are used in the course of performing a Site Survey.

Record – Records the signal strength of the current location in the Survey Log, as well as all neighboring Access Points. In the **Record** window, you can add the name of the location and a remark. You can view the Survey Log by pressing **Survey Log**.

Alias – Lets you assign alias names to Access Points. In the **Alias** window, enter the Access Point address and the desired alias. For convenience, you can drag and drop the address of the associated Access Point from the main window into the **Alias** window. For neighbor Access Points, you should use **Ctrl-C** to copy the AP Address from the main window.

Iconize – Closes the **Site Survey** window and opens the Connection Quality Graph, which indicates current signal strength of the associated Access Point at a glance. The Graph can be moved anywhere on the screen, and will always appear on top of other applications. Hold the cursor over the X to see the signal strength in units. Press the **X** to close the Graph and open the **Site Survey** window.

Figure 4-5. Connection Quality Graph.

Survey Log – Opens the Survey Log at the bottom of the main window. The Survey Log displays the information recorded using the **Record** button. Press **Clear Log** to clear the Survey Log. Press **Delete Last** to delete the last recorded reading.

- Menu Bar — The menu bar at the top of the window contains four menus: Edit, View, Report, and Help. These menus contain sub-menus which correspond in most cases to the buttons at the side of the window.

  Edit Menu – Three sub-menus: Record, Alias, and Exit.

  View Menu – Has two sub-menus: Survey Log and Iconize.

  Report Menu – Two sub-menus: Preview and Print (do not have corresponding buttons on side of window).

  Preview – Enables you to preview a Site Survey report before proceeding further.

  Print – Opens a Site Survey report showing the information in the Survey Log, including neighboring Access Points.

  You can print the file by clicking the **Printer** button, or save the file by clicking on the **Diskette** button. You can save the file as text, or as a QRP file viewable using this application.

  Help Menu – Contains two sub-menus: About and Getting Started (do not have corresponding buttons on side of window). **About** contains standard Windows format information about the application. **Getting Started** provides basic information to enable you to begin working.

4.6.3 Performing a Site Survey with the PCMCIA Adapter

You can run a Site Survey to compare reception at various locations. This is extremely useful when first setting up the wireless LAN, since you can easily determine where reception is good or bad, and where many Access Points overlap.

To run a Site Survey:

1. Open the **Site Survey** utility.

2. Press **Survey Log** to expand the bottom of the **Site Survey** window.

3. Bring the station to a new location.

4. Press **Record**. Type in the name of the location and a remark, and press **OK**. The signal details of the current location appear in the Survey Log at the bottom of the window.

5. Repeat steps 2 and 3 with other locations. The recorded readings should give you a good idea of where reception is good or bad, and where many Access Points overlap unnecessarily.

6. When you are done recording, press **Print**. A site survey report appears containing information about each recorded location, including signal strength of associated Access Point and of neighbor Access Points. You can print the file by pressing the **Print** button, or save the file by pressing the **Diskette** button. You can save the file as text, or as a QRP file viewable using this application only.

4.7 Using the Upgrade Kit Program

The Upgrade Kit program is an application that allows you to upgrade previous versions of the firmware, drivers, and utilities of the PCMCIA Adapter, if installing on a machine that had a previous version installed. The Upgrade kit can be obtained at www.blackbox.com. At this point, please call Technical Support for assistance.

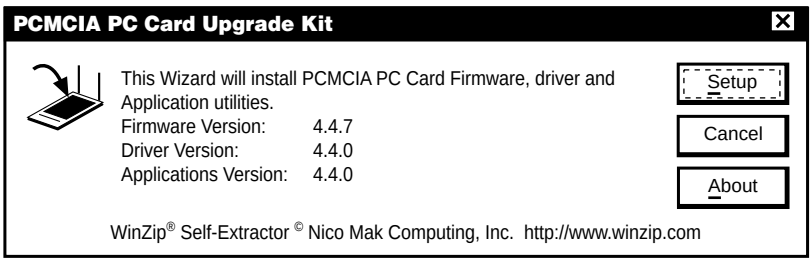
In addition, under Windows 95/98 you can use this program as another way to install the firmware, driver, and utilities.

NOTE

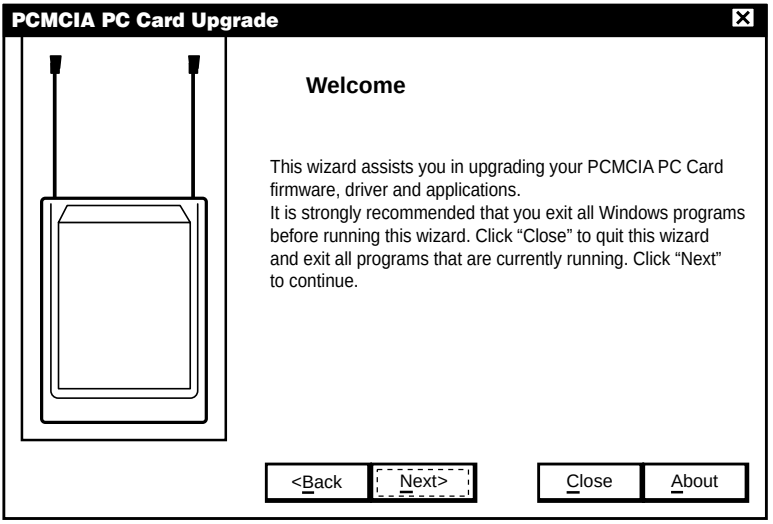
Upgrading causes your system to lose all configuration parameters that were set previously.

UPGRADE PROCEDURE FOR WINDOWS 95/98

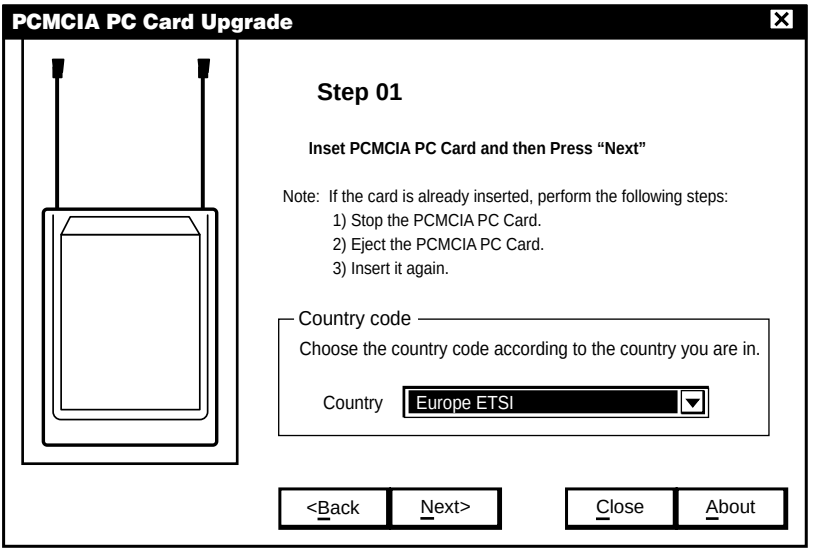
1. Run the **UPGR4402.EXE** program from the diskette. The following dialog box is displayed.



2. Click **Setup**. The following dialog box is displayed.

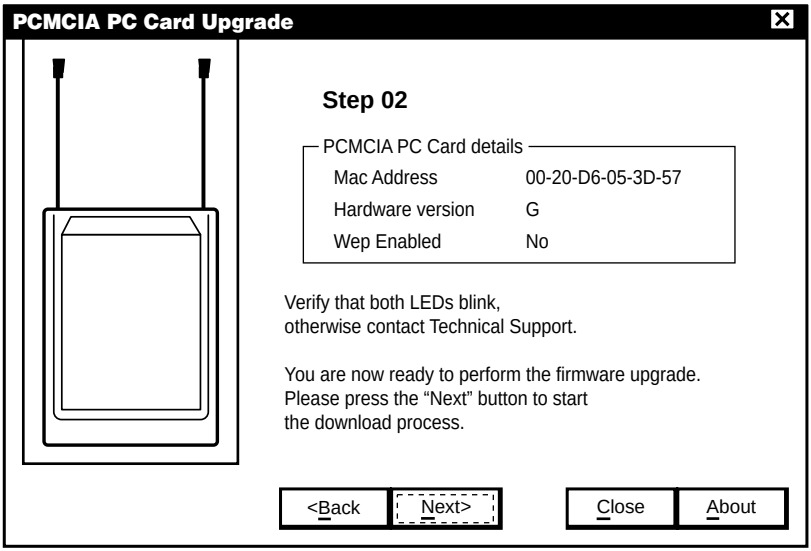


3. Click **Next**. The following dialog box is displayed.



4. From the **Country** drop-down list, select the standard applicable to your country and click **Next**. You do not need to select the country if you are installing the application in the following countries: USA/FCC, Europe/ETSI, Japan.

5. If the Adapter is already installed, stop the Adapter as follows: from the **Control Panel**, double-click the **PCMCIA Adapter** icon, select the **PCMCIA PC Card**, and click **Stop**. Remove the PCMCIA Adapter from the slot. Wait for about 15 seconds and then reinsert. Click **Next**.



6. The MAC address of the PC and the hardware version of the PCMCIA Adapter are displayed in a read-only field.

   If you purchased the PCMCIA PC Card without the Wired Equivalent Privacy (WEP) feature and want to enable this feature, contact Technical Support, or

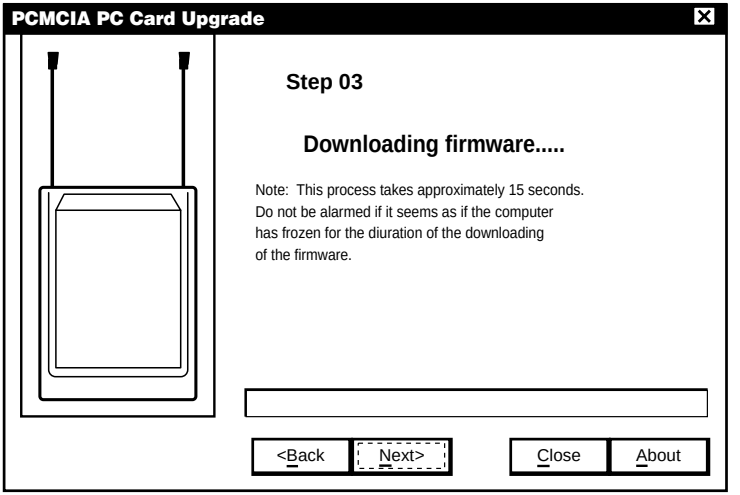
   Double-click the WEP field value (set to **NO** by default). A **Password** dialog box appears.

   Enter the supplied password and click **OK** to return to the dialog box from step 2.

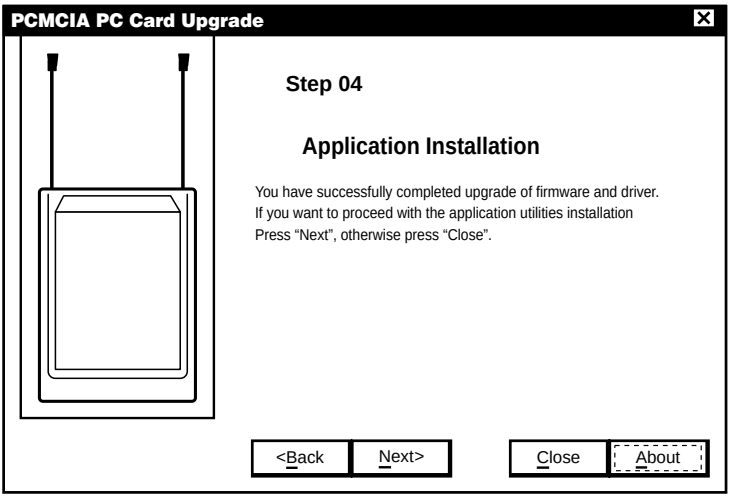
NOTE

The password for enabling the WEP feature can only be obtained from Black Box.

7. Follow the on-screen instructions and check the Adapter's LEDs as described in **Section 4.3.2**. Click **Next**. The following dialog box is displayed.

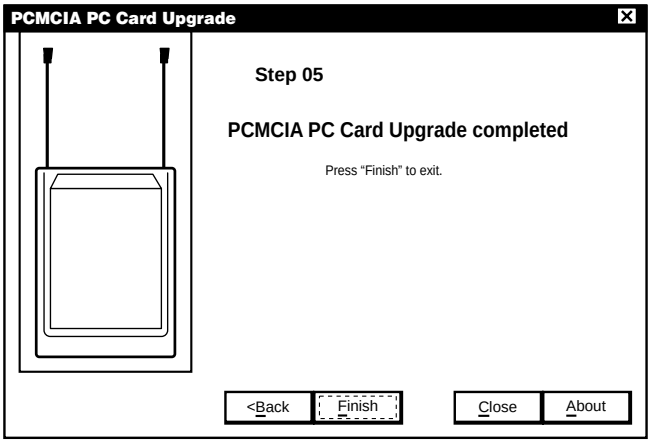


8. When the firmware has completely downloaded, the following dialog box is displayed.



9. At this point, the upgrade program installs the **PCMCIA PC Card** utilities. Specify the directory in which the program installs the utilities.

10. Continue to follow the on-screen prompts until the following dialog box is displayed.



11. Restart the computer when prompted. When the computer is restarted, the New Hardware wizard is entered automatically and the new drivers are installed and shortcuts are updated.

UPGRADE PROCEDURE FOR WINDOWS NT, DOS/ODI

Follow these instructions in order to upgrade PCMCIA PC Cards installed in machines running Windows NT or DOS/ODI.

1. Upgrade the firmware in a Windows 95/98 machine, using the Upgrade Kit program.

2. Remove the old drivers and utilities from your Windows NT or DOS/ODI machine.

3. Download new drivers and utilities from the Black Box web site (www.blackbox.com) according to your country.

4. Use the drivers and utilities that you have downloaded to install the new versions of the drivers and utilities.

4.8 Installation Troubleshooting

The following are some problems that may occur while installing the PCMCIA PC Card, and some recommended solutions to these problems. Should you encounter problems during installation which are not listed in this section, contact Black Box Technical Support.

Problem 1: Adapter does not function properly.

1. Check **Device Manager** for conflicts with any other devices and drivers.

2. Right click **My Computer**, **Properties**, and then the **Device Manager** tab.

3. Click **Network Adapters** to verify status of the Adapter—an exclamation mark next to the card indicates a conflict.

Problem 2. There is a resolution conflict.

1. Double-click the **PCMCIA PCI Card**.

2. Select the **Resources** tab.

3. In the event that the conflicting resources are listed in the conflicting device list, edit the **Memory** range and **Interrupt** to values that do not cause conflicts.

Problem 3. There is no resource conflict, but the card still fails to work. There may be a conflict with DOS drivers not recognized by Windows.

1. Look for device drivers or lines containing device or call commands in either the autoexec.bat or the config.sys file.

2. Disable the conflicting drivers and devices, and uninstall and reinstall the card.

4.9 Installing the PCMCIA Adapter Drivers in ODI Systems

The ODI driver supports Novell VLM and NETX clients, Novell TCPIP, Lantastic v.6 (with ODINSUP), Microsoft Windows 3.11 (with ODINSUP).

The following files are supplied for the DOS ODI environment:

brzwlan.com	ODI driver file, generic version
brzwlanf.com	ODI driver file for Falcon 310 (supplied only on request)
brzwlan.ini	Default configuration file
brzsetup.exe	Site survey utility
net.cfg	Sample ODI16 configuration file
brzwlan.ins	Installation information for Novell client (DOS and Windows)

1. The ODI driver gets its resources from the Card & Socket Services. Verify that the PC you are using has Card & Socket Services software installed.

2. Copy all files from the DOSODI directory on the driver to the NetWare client directory. (If you already have a NET.CFG file that you want to keep, copy and paste the BRZWLAN section from the sample NET.CFG file supplied by Black Box, into your existing file.)

3. In order to log into a NetWare server, run the following files (make sure that the NET.CFG and the BRZWLAN.INI files are located in the directory from which you run the following files):

   - LSL.COM (supplied by Novell)
   - BRZWLAN.COM
   - IPXODI.COM (supplied by Novell)
   - VLM.EXE (supplied by Novell)

4. After running the BRZWLAN file, the yellow LED on the Adapter should blink several times and then remain lit.

Configuration Notes

1. To configure the PCMCIA PC Card, use the brzsetup.exe configuration utility.

2. A sample net.cfg file is provided; you may edit this to configure the parameters for IRQ and MEM.

3. For DOS versions 3.30 to 6.20, **LASTDRIVE=E** by default. If the user only has drive C, letters D and E will be available for Novell network drives. To make all letters available for the network, add **LASTDRIVE=Z** to the config.sys file.

4. The units can only work with Access Points which have 802.11 software version 4.3 or later.

5. To see the version of the PCMCIA Adapter, make sure the card is inserted and run the **Site Survey** utility.

6. For configuration of the NDIS2 stack using ODINSUP, refer to ODINSUP documentation.

Running the Configuration Utility

1. Change to the NetWare client directory.

2. Type `brzsetup` and press **Enter**.

3. Enter the ESSID as defined in the Access Point (if using default ESSID, do not change).

4. Reset/restart the computer.

NOTE

Default ESSID is ESSID1 in capital letters.

TROUBLESHOOTING ODI INSTALLATION

The following paragraphs provide information that can help in the event of problems encountered in the ODI drivers installation.

- It is important to note which net.cfg and brzwlan.ini is used. After installation of new Novell client, two copies of brzwlan.ini, brzwlan.com, and net.cfg files may exist, one in the Windows directory and another in the directory where the Novell client is installed.

- If Card Services fails to provide correct memory and IRQ automatically, edit net.cfg and use IRQ and MEM parameters.

- If the driver did not display a message **Testing Device**, this indicates that Card Services failed to recognize the card or to provide the required information to the driver. Check the Card Services information configuration.

- The driver reports an error in allocating IRQ or memory. The Card Services failed to provide the required resources to the driver, or there are no resources available. Reboot without EMM386 or other programs that may take up the adapter memory region. Change the IRQ or MEM parameters in net.cfg to force the driver to request specific resources.

- The driver reports errors in net.cfg or brzwlan.ini. The files are corrupt or you are not in the correct directory.

- The yellow LED blinks and turns off after several seconds. The Access Point is configured with incorrect parameters. Check the Access Point configuration. The built-in antennas are not pulled out or the external antenna is not attached to the PC card.

- The yellow LED does not blink and is not lit. The driver is not receiving interrupts. Try to change IRQ—wrong firmware version or card initialization error.

5. Planning and Installing Wireless LANs

Models LW0050A through LW0054A are equipped with two integrated 2-dBi omnidirectional antennas and are suitable for indoor, short- to medium-range installations. Models LW0055A through LW0059A are equipped with two customized female connectors for use with a range of external antennas.

This chapter describes various possible system configurations, lists points to consider when performing indoor and outdoor installations, and presents guidelines and restrictions regarding external antenna installation.

5.1 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 Access Point-Workgroup Bridge pairs that extend the range of the wireless LAN.

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

5.1.1 Single-Cell Configuration

A basic cell consists of an Access Point and the wireless workstations associated with it. You can convert most workstations (for example, PCs and X-Terminals) that are equipped with an Ethernet network interface card (NIC) to wireless workstations simply by connecting a Station Adapter. You can convert most laptop computers with a PCMCIA slot into wireless mobile stations by using the PCMCIA Adapter (LW0054A or LW0059A).

There are three types of Single-Cell Configuration:

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

Each type is explained in the following sections.

5.1.1.1 Point-to-Point

Point-to-Point installations 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.

5.1.1.2 Point-to-Multipoint

Point-to-Multipoint applications consist of one or more Access Points at the central site and several remote stations and bridges. In this case, use a 6-dBi Omnidirectional Antenna (LW011A) with the Access Point because of its 360° radiation pattern. In the United States, the 7.2-dBi Omnidirectional Antenna, LW0029-R2 (which also has a 360° radiation pattern but has a wider range), can also be used. The 7.2-dBi Omnidirectional antenna comes with a 20-ft. low-loss cable and a mast mount bracket for rooftop installations.

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

5.1.1.3 Mobile Applications

In mobile applications, station orientation changes continuously. In order to maintain connectivity throughout the entire coverage area, most mobile applications require omnidirectional antennas for both Access Points and wireless stations. In a motor vehicle, for example, you can install a Single-Port Station Adapter in the cabin, and mount the antenna (in most cases a LW016A Omnidirectional Antenna) on the roof.

5.1.1.4 Extending the LAN with WLAN Bridging

The figures in this section demonstrate how the Workgroup Bridge (LW0053A) can be used with an Access Point to extend a regular network with a wireless link.

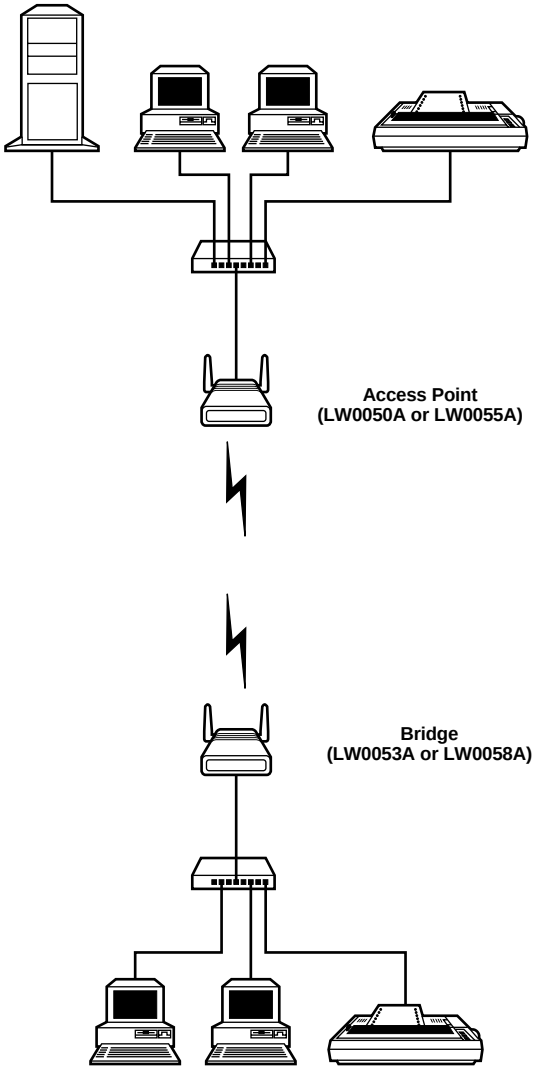


Figure 5-1. Connecting Remote Offices to Main Office Network.

The Workgroup Bridge (LW0053A) also enables connectivity between a wireless LAN and individual workstations or workgroups located outside the LAN. The Workgroup Bridge 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.

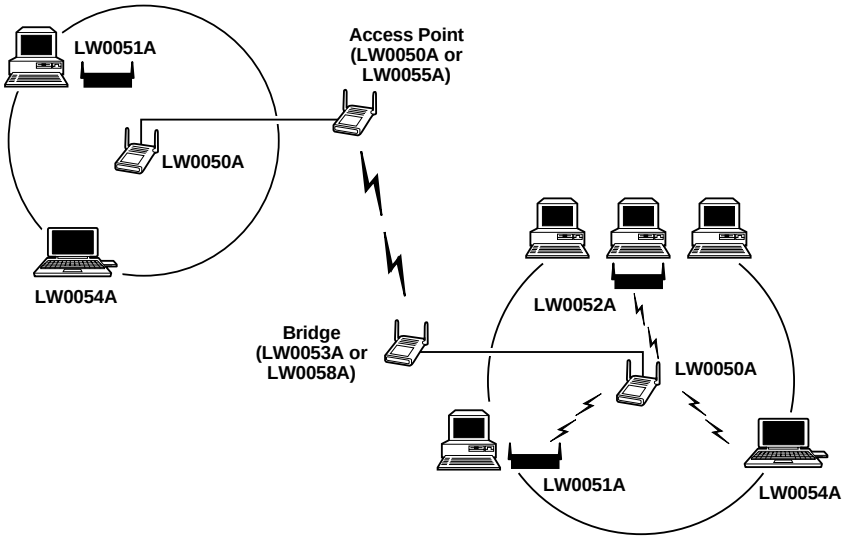


Figure 5-2. Wireless Bridging Between Two or More Wireless LAN Segments.

5.1.1.5 Setting Up a Single Cell

1. Install the Access Point (refer to **Chapter 2**). 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 **Chapter 2**) or PCMCIA PC Card (refer to **Chapter 4** for installation instructions).

3. Look at the Station Adapter's front-panel LED indicators, or the PCMCIA PC Card's Site Survey application, to check signal strength.

4. Make any necessary adjustments. For example, adjust the antennas, the location of the Station Adapter, or the location of the Access Point.

5. Set up the other workstations.

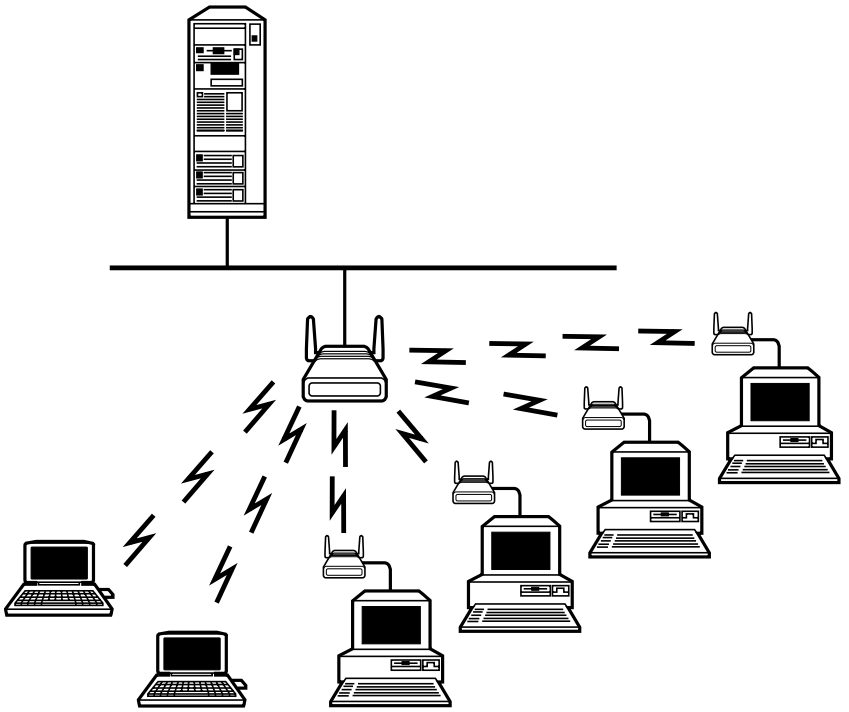


Figure 5-3. Single-Cell Configuration.

5.1.2 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.

To set up overlapping cells:

1. Install an Access Point (refer to **Chapter 2**). 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 5.2.4**).
3. To allow roaming, configure all Access Points and station 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 PCMCIA Adapter on a workstation.
6. Position the wireless workstation approximately equal distances 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. Look at the Station Adapter's front-panel LED indicators, or the PCMCIA Adapter's Site Survey application, to check signal strength of the first Access Point.
8. Disconnect the second Access Point from the power supply and reconnect the first Access Point. Look at the Station Adapter's front-panel LED indicators, or the PCMCIA Adapter's Site Survey application, to check signal strength of the second Access Point.

NOTE

It isn't 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.

9. If necessary, adjust the distance between the Access Points so the coverage areas overlap. Continue setting up overlapping cells until the required area is covered.

5.1.3 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 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 1.5 Mbps (which is the net throughput supported by collocated Access Points). Consider the example of 5 active stations, each requiring 0.5-Mbps throughput. The calculation is $5 \times 0.5/1.5 = 1.7$. 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 collocated 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 at the highest points possible.

3. To allow roaming and redundancy, configure all Access Points and station 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 PCMCIA Adapters in workstations.

6. Make sure 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 isn't 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.

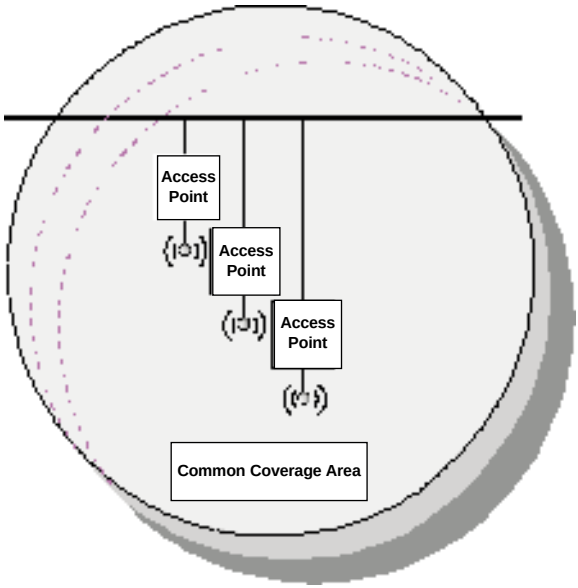


Figure 5-4. Multicell Configuration.

5.1.4 Multi-hop Configuration (Relay)

When you need to connect two sites and no line of sight exists between them, an Access-Point/Workstation-Bridge pair can be positioned at a third location where line-of-sight exists with each of the original locations. The third location then acts as a relay point.

In areas where a wired LAN backbone is not available, another Access Point can be added to the Access-Point/Workgroup-Bridge relay to distribute a wireless backbone. In this manner, the range of a wireless system can be extended.

To set up a multi-hop cell:

1. Install an Access Point at the main office (refer to **Chapter 2**).

2. Install a Workgroup Bridge at the remote site.

3. Install an Access-Point/Workgroup-Bridge pair in a high location that has a clear line of sight to both the main office and the remote site. Many Access-Point/Workstation-Bridge pairs can form a chain.

4. When an Access Point and Workstation Bridge communicate over the wireless LAN, set them both to the same ESSID. For example, set the Access Point of the main office and the Workstation Bridge of the first Access-Point/Workstation-Bridge relay pair to the same ESSID. Also, set the Access Point of the last Access-Point/Workstation-Bridge relay and the Workstation Bridge 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 Workstation Bridge to its paired Access Point (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.

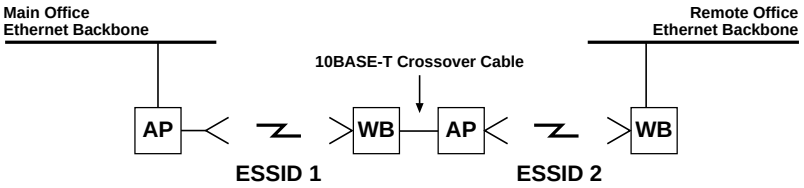


Figure 5-5. Multihop Configuration.

6. If desired, an additional Access Point may be added at the main office and remote site, and between each Access-Point/Workstation-Bridge pair to provide wireless LANs at those points.

7. Install Station Adapters or PCMCIA Adapters in workstations (refer to **Chapter 2**).

5.2 Indoor Installation Considerations

This chapter describes various considerations to take into account when planning an indoor installation. This includes site selection, antenna diversity, antenna polarization, construction materials, and cell size.

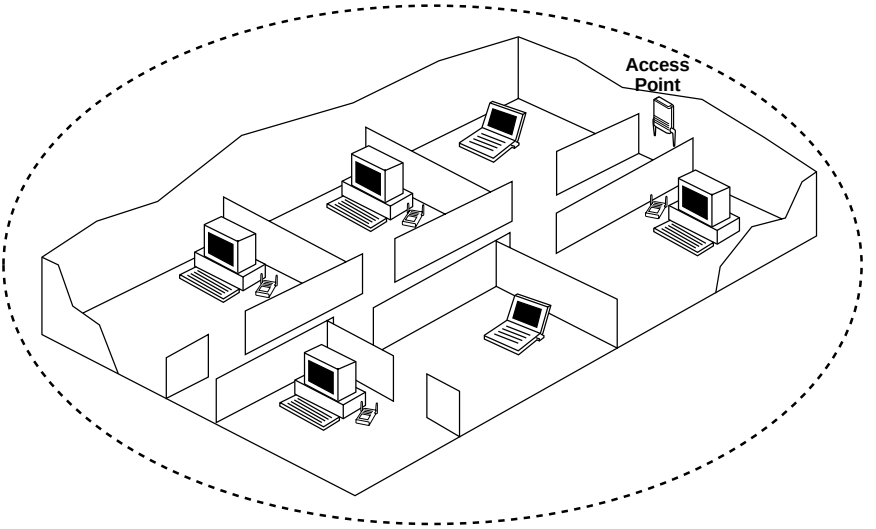


Figure 5-6. Access Point LAN in a Typical Office Environment.

5.2.1 Site-Selection Factors

The Pro 11 Series Wireless Ethernet products are 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
Make sure the antennas point up. For models with external antennas, connect the external antennas and RF cable.

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

Site Selection for Access Points
When positioning Access Points, take into account the following additional considerations.

Height

Install the Access Point at least 5 feet (1.5 m) 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 Pro 11 LAN are reflected along the metal partitions and enter the offices through the doors or glass sections.

5.2.2 Antennas for Indoor applications

For most indoor applications, the best choice is the standard unit equipped with its integrated 2-dBi antennas. The units are small, easy to install, and cover a large area.

In some installations, you need to install the unit and antenna separately. In such instances, use the LW0055A Access Point with a 6-dBi Omnidirectional Antenna with ≈3-ft. (0.9-m) RG58 cable.

The 8.5-dBi Unidirectional Antenna is also useful in indoor applications. It is very small and easily wall-mounted, but its radiation pattern is limited (75°).

We recommend that, for indoor applications, you use two antennas per unit to take advantage of the diversity gain of the system.

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, we recommend 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 few 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 diversity option to either antenna 1 or antenna 2, according to the antenna being used (refer to **Section 3.4.3**).

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.

5.2.3 Construction Materials

A cell's coverage area is affected by the construction materials of the walls, partitions, ceilings, floors, and furnishings of the cell. These materials may cause radio signal loss:

- Metal objects reflect radio signals. They do not let the signals pass through.
- Wood, glass, plastic, and brick reflect part of the radio signals and allow part of the radio signals to pass through.
- Water and objects with a high moisture content absorb a large part of the radio signals.

Use the following table as a guideline to predict the effects of different materials.

Table 5-1. Signal Loss Chart

Obstruction	Additional Loss (dB)	Effective Range	Approximate Range
Open Space	0 dB	100%	1000 ft. (300 m)
Window (non-metallic tint)	3 dB	70%	700 ft. (215 m)
Window (metallic tint)	5 to 8 dB	50%	500 ft. (150 m)
Light Wall (dry wall)	5 to 8 dB	50%	500 ft. (150 m)
Medium Wall (wood)	10 dB	30%	300 ft. (100 m)
Heavy Wall (solid core 6")	15 to 20 dB	15%	150 ft. (50 m)
Very Heavy Wall (solid core 12")	20 to 25 dB	10%	100 ft. (30 m)
Floor/Ceiling (solid core)	15 to 20 dB	15%	150 ft. (50 m)
Floor/Ceiling (heavy solid core)	20 to 25 dB	10%	100 ft. (30 m)

Note: Take stairwells and elevator shafts into consideration when positioning Access Points. There is no way to quantify the loss associated with these obstructions, but they do have an effect on the signal.

5.2.4 Cell Size

Cell size is determined by the maximum possible distance between the Access Point and the Station Adapter. This distance varies according to the building floor plan and the nature of that environment. There are several general categories:

Open Indoor Areas
Open office areas with no partitioning and no obstacles between the Access Point and the workstation.

The suggested maximum distance between a standard Access Point (LW0050A) and a workstation is 600 ft. (200 m).

Semi-Open Indoor Areas
Open-plan offices partitioned into individual workspaces, factory floors, warehouses, etc.

The suggested maximum distance between a standard Access Point and a workstation is 300 ft. (100 m).

Closed Indoor Areas
A floor divided into individual offices by concrete, masonry, or sheet-rock walls. A house is also a closed indoor area.

The suggested maximum distance between a standard Access Point and a workstation is 150 ft. (50 m).

5.3 Outdoor Installation Considerations

This section 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.

5.3.1 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 structures such as trees, mountains, or other natural geographic features higher than the antenna and situated in the path between the two sites can be 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.

5.3.2 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.
- Fewer obstacles in path.
- Improved performance due to greater height.
- Reduced multipath problems.

5.3.3 Antennas for Outdoor Applications

The Pro 11 Series can be used in point-to-point or point-to-multipoint configurations.

Point-to-Point
A point-to-point link is based on the use of one Access Point with external antennas (LW0055A) and one adapter (LW0056A–LW0059A). The Access Point and the Workstation Bridge must be equipped with one or two directional antennas. The necessary antenna gain depends on the required range and performance.

Point-to-Multipoint
Setting up a point-to-multipoint link requires the use of an LW0055A Access Point equipped with omnidirectional antennas and a remote LW0058A Workgroup Bridge (or LW0056A, LW0057A, or LW0059A) equipped with high-gain directional antennas.

Antenna Alignment
Low-gain antennas do not require alignment, since they have a very wide radiation pattern. High-gain antennas have a narrow beamwidth, so you need to align them 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 (LW0056A, LW0057A, or LW0058A), or use the site survey program with the LW0059A. The LED indicators, if you decide to use them, show you the 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 Access Point at the main site.

4. Connect the coaxial cable to the Workstation Bridge (or Station Adapter) at the remote site.

5. Power on the Access Point and the Workstation Bridge (or Station Adapter).

6. Synchronize the units by aligning the antennas manually until the WLNK indicator LED on the front panel of the wireless Bridge or Station Adapter lights.

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 cable connections.

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, we recommend 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 few 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-diversity option to either antenna 1 or antenna 2, according to the antenna being used (refer to **Section 3.4.3**).

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.

5.3.4 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.

5.3.5 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 Pro 11 workstation, the suggested maximum distance between a standard Access Point (LW0050A) and a workstation is 2000 ft. (700 m).

5.3.6 Link Distance

Link distance is the maximum distance between the Access Point 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:

- up to 7 miles (10 km) in the USA (with an LW0055A Access Point with external antennas)
- up to 2.5 km in Europe (with an LW0055A Access Point with external antennas)

NOTE

The maximum distance of 10 km/7 miles is achieved using 24-dBi antennas. The maximum distance of 2.5 km is achieved using 18-dBi antennas.

5.3.7 Outdoor Installations

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.

5.4 Precautions

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.

5.4.1 Transmit Antenna

Regulations regarding maximum antenna gains vary from country to country. It is your responsibility 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 transit power to 36 dBm (USA) and 20 dBm (Europe). The maximum total assembly gain of antennas and cables equals 19 dBi (USA) and 3 dBi (Europe).

5.4.2 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 Pro 11 unit's connector.

5.4.3 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 arrestor 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 arrestor) 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 arrestor (LW014) should be installed and grounded at the point where the cable enters the building. The arrestor 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.

5.4.4 Rain Proofing

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

6. Upgrade Procedure

IMPORTANT!

Please read the information below before proceeding with any upgrades.

There are two options for upgrading to the Pro 11 Series:

1. Send in your Pro Series equipment, and we will upgrade the units to the Pro 11 802.11 standard for a service fee.

2. Download the software at no charge from the Black Box FTP site and perform the upgrade yourself. If you choose to do the upgrade yourself, you assume all responsibility for the condition of the product after the upgrade. Black Box provides this upgrade software without warranty of any kind, either implied or expressed and may change the upgrade software at any time without notification. Performing the firmware upload to the Pro 11 Series flash-ROM is recommended only for experienced system administrators. Improper uploads can result in the permanent erasing of the flash-ROM, and necessitate the return of the unit for repair and the user incurs an upgrade/service fee.

You can download firmware upgrades to the unit's flash memory with a TFTP application. Before beginning an upgrade, *be sure you have the correct files and latest instructions.* Upgrade packages can be obtained at the Black Box web site: www.blackbox.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 during the download procedure in any case.*

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 6-1. Upgrade Files

Current Version of Unit	Flash Erase File Name	Software Download File Name	
		LW0050A	LW0051A, LW0052A, LW0053A
3.2, 3.38, 3.42, 3.50	download	eanaf	eansf
3.52, 4.204, 4.41	erase	eanafb	eansfb
3.62, 4.210, 4.211, 4.310, 4.41	erase_fw	ap_fw	sawb_fw

The *current* version and type of the unit determine the files used for upgrade. For example, when upgrading LW0050A from version 3.52 to version 4.4.1, use the *erase* and *eanafb* files. When upgrading LW0051A from version 3.62 to version 4.4.1, use the *erase_fw* and *sawb_fw* files.

7. System Troubleshooting

This troubleshooting guide provides answers to some of the more common problems which may occur when installing and using the Pro 11 Series products. If problems not mentioned in this guide should arise, checking the Ethernet and WLAN counters may help. If the problem persists, call Technical Support.

7.1 Troubleshooting Guide

Problem and Indication	Possible Cause	Corrective Action
No power to unit. PWR LED is off.	1. Power cord is not properly connected. 2. Power supply is defective.	1. Is the power cord properly connected to the unit and the power outlet? 2. If the cord is properly connected, replace the power supply.
Failure to establish wireless link. WLNK LED is off and unit resets every few minutes.	1. Power supply to units may be faulty. 2. The units may not have the same ESSID as the Access Point.	1. Verify power to units (Access Point and Station Adapter/Workstation Bridge). 2. Verify that all units in the network have the same ESSID as the Access Point (ESSID must be identical in all units in the network). 3. Verify wireless link: • Set the Access Point and the unit (Station Adapter or Workgroup Bridge) side by side. • Power on each unit and see if a wireless link is established (even models LW0055A through LW0058A without their external antennas should establish a link if placed side by side with the Access Point). • If the units fail to associate, reset units to factory-default values (see **Section 3.4.5**). The units should now establish a wireless link.

Problem and Indication	Possible Cause	Corrective Action
Failure to establish wireless link (LW0055A–LW0058A)	1. Power supply to units may be faulty. 2. Cables may be improperly connected. 3. There may be some problem with antenna installation.	1. Verify power to units. 2. Verify that all cables are connected securely. 3. Refer to the previous section and verify wireless link between the units. 4. Verify that the antenna(s) are properly installed: • 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 (Access Points and Workstation Bridges).	1. Ethernet hub port or UTP cable is faulty. 2. Ethernet port in unit is faulty.	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 the unit is working. Ping the unit to verify Ethernet connection. 3. Verify that you are using a cross-over UTP cable (pins 1 & 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 (see **Section 3.6.1**).

Problem and Indication	Possible Cause	Corrective Action
Wireless link established, but there is no Ethernet activity (Station Adapters).	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 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. • Re-establish network connection. • Verify that the workstation is properly configured for the network. 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 (see **Section 3.6.1**).

Problem and Indication	Possible Cause	Corrective Action
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. • Check counters to see if more than 10% of total transmitted frames are retransmitted fragments (see **Section 3.6.1**). • Check if more than 10% of total received data frames are bad fragments (see **Section 3.6.1**). 2. Verify Ethernet port activity by checking Ethernet counters (see **Section 3.6.1**).
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. • Check for heavy metal structures (for example, 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 Access Points) because of 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.	Refer to **Section 5.3**: • Is there a clear line of sight? • 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).

Problem and Indication	Possible Cause	Corrective Action
Unit associates with the wrong Access Point.	In a multicell structure with overlapping cells, the units may not associate with the closest Access Point.	For a unit to associate with a specific Access Point, assign 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-Access Point configuration.	The Access Points in the same coverage area have not been assigned unique hopping sequences.	Assign a unique hopping sequence to each Access Point in the coverage area. Each Access Point must have a unique hopping sequence regardless of ESSID.

7.2 Checking Counters

Checking counters is also a good way to pinpoint any problems that may occur in the wireless LAN. Counters can be checked from the monitor. See **Section 3.6.1**.

7.2.1 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 7.1**) above for possible corrective action.

7.2.2 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.

Appendix A. Supported MIBs and Traps

A.1 Supported MIBs

All products in the Pro 11 Series contain an embedded SNMP (Simple Network Management Protocol) agent. All functions can be accessed from the Management Information Base (MIB) using an SNMP application.

Pro 11 Series agents support the following MIBs:

- MIB-II (RFC1213)
- BRIDGE-MIB (RFC1286)
- Pro 11 Private MIB

The Pro 11 Private MIB can be viewed by opening the MIB file **brz11prv.mib**. The MIB is not included; call Technical Support if you need the Pro 11 Private MIB.

A.2 Supported Traps

The following traps are implemented by the Pro 11 units. All Pro 11 units that have the SNMP Traps parameter enabled 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 table on the next page lists the traps implemented by the Pro 11 units.

Trap	Variables	Description
brzAProamingIn	brzTrapSTAMacAddr	A station has roamed into this Access Point coverage area. The trap contains the MAC address of the associated station.
brzAPassociated	brzTrapSTAMacAddr	A new station is associated with this Access Point. The trap contains the MAC address of the associated station.
brzAPdisassociated	brzTrapSTAMacAddr	A station has disassociated itself from this Access Point. The trap contains the MAC address of the associated station.
brzAPaging	brzTrapSTAMacAddr	A station association was aged out and removed from this Access Point. The trap contains the MAC address of the aged-out station.
brzAProamedout	brzTrapSTAMacAddr	A station has roamed out of this Access Point'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 Access Point. The trap contains the MAC address and average RSSI level of the new Access Point (TrapAPMac and TrapRssiQuality variables). If the station has been roaming, the MAC address of the old Access Point and the RSSI level prior to roaming are also provided (LastAPMacAddr and LastRssiQuality variables). For an association, the second address appears as all zeros.

Trap	Variables	Description
brzWlanStatus	brzTrapToggle brzTrapMacAddress	The wireless media condition has changed. An ON value is sent when the wireless LAN quality for a station or Access Point drops below the WLAN trap threshold. An OFF value is sent if the quality improves beyond the threshold. The current value of wireless LAN is also sent.
brzWlanStatus-OfStation	brzTrapToggle brzTrapMacAddress	The quality of the wireless connection to the Access Point 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 brzTrapMacAddress variable contains the MAC address of the applicable station.
brzGeneral	brzTrapIndex brzTrapText	For future use.

Appendix B. Specifications

B.1 Specifications for LW0050A–LW0053A and LW0055A–LW0058A

WIRED LAN INTERFACE

Compliance — Ethernet/IEEE 802.3 CSMA/CD standard

Physical Interface — 10BASE-T

Network Operating Systems Supported — All

Network Protocols Supported — All

WIRELESS LAN INTERFACE

Compliance — IEEE 802.11 CSMA/CA Wireless LAN standard

Physical Interface — Two integrated or external antennas

RADIO SPECIFICATIONS

Type — Frequency-Hopping Spread Spectrum (FHSS)

Frequency Range — 2.4 GHz to 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 (20 dBm) EIRP; External antennas: High power (at the connector) of 17 dBm (50 mW), low power (at the connector) of 4 dBm (25 mW)

Sensitivity — 1 Mbps: -81 dBm; 2 Mbps: -75 dBm; 3 Mbps: -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

Configuration and Management

Configuration and Setup — Via Local Monitor port (serial RS-232)

SNMP Management — SNMP agents: MIB II, Bridge MIB, WLAN MIB, and private MIB; Access via: Wired LAN, Wireless LAN

Site Survey — Via Local Monitor port (serial RS-232), via SNMP

Indicators — Power on, Wired LAN activity, Wireless LAN synchronization, Wireless LAN signal quality/Load

Software Upgradable — 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)

Range (unobstructed with integrated antennas) — 2000 ft. (600 m)

Range (unobstructed with external antennas) — USA FCC: up to 6 miles (about 9 km); Europe ETSI: up to 2.5 km; Non-Regulated: 30 km and above

Range (office environment) — Up to 500 ft. (150 m)

Maximum Number of Access Points per Wired LAN — Unlimited

Maximum Number of Overlapping Access Points — 15

Data Rate — Over the air: 1, 2, or 3 Mbps; Nominal net: Up to 2 Mbps; Aggregate: Over 5 Mbps with overlapped cells

High-Speed Roaming — Up to 60 mph (90 kph)

Load-Sharing Support — Yes (with WIX)

Rate Selection — Dynamic, based on quality of radio medium

Environmental

Operating Temperature — 32 to 105°F (0 to 40°C)

Operating Humidity — 5 to 95% noncondensing

ELECTRICAL

External Power Supply — 100 to 250 VAC, 50 to 60 Hz, 0.5 A

Input Voltage — 5 VDC

Power Consumption — 1.5 A peak, 1.2 A average

PHYSICAL

Size — 5.1"H x 3.4"W x 1.35"D (13 x 8.6 x 3 cm) without antennas and power supply

Weight — 0.9 lb. (0.4 kg) without antennas and power supply

B.2 Specifications for LW0054A and LW0059A

WIRED LAN INTERFACE

Physical Interface — PC Card type II/PCMCIA 2.1

Network Operating Systems Supported — Windows 95, 98, NT4

Network Protocols Supported — NDIS

WIRELESS LAN INTERFACE

Compliance — 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 to 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 (20 dBm) EIRP; External antennas: High power (at the connector) of 17 dBm (50mW), low power (at the connector) of 4 dBm (25 mW)

Sensitivity — 1 Mbps: -81 dBm; 2 Mbps: -75 dBm; 3 Mbps: -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

Configuration and Management

Configuration and Setup — Via application

Site Survey — Via application

Indicators— Link Status, Data Traffic

Software Upgradable — Via PC

System Considerations

Range (Access Point to Station) — Depends on rate and antenna cable length/quality (accurate values must be calculated for specific installations)

Range (unobstructed with integrated antennas) — 1500 ft. (450 m)

Range (office environment) — Up to 500 ft. (150 m)

Maximum Number of Access Points per Wired LAN — Unlimited

Maximum Number of Overlapping Access Points — 15

Data Rate — Over the air: 1, 2, or 3 Mbps; Nominal net: Up to 2 Mbps; Aggregate: Over 5 Mbps with overlapped cells

High-Speed Roaming — Up to 60 mph (90 kph)

Load-Sharing Support — Yes (with WIX)

Rate Selection — Dynamic, based on quality of radio medium

Environmental

Operating Temperature — 32 to 105°F (0 to 40°C)

Operating Humidity — 5 to 95% noncondensing

Electrical

Power — Via network PC

Input Voltage — 5 VDC

Power Consumption — XMT: 365 mA peak; RCV: 280 mA peak

Physical

Size — Standard PCMCIA Type II

Weight — 1.1 oz. (32 g)

Appendix C. Wireless LAN Concepts

Wireless LAN technology is becoming increasingly popular in large-scale and complex wireless networks, as more and more users are discovering its reliability and high performance.

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

C.1 Topology

C.1.1 Wired LAN Topology

Traditional LANs link PCs and other computers to one another and to file servers, printers and other network equipment using cables or optical fibers as the transmission medium.

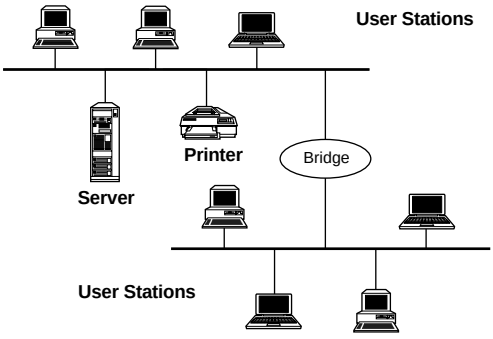


Figure C-1. Wired LAN Topology.

C.1.2 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 and notebook or pen-based computers can move freely in the cell.

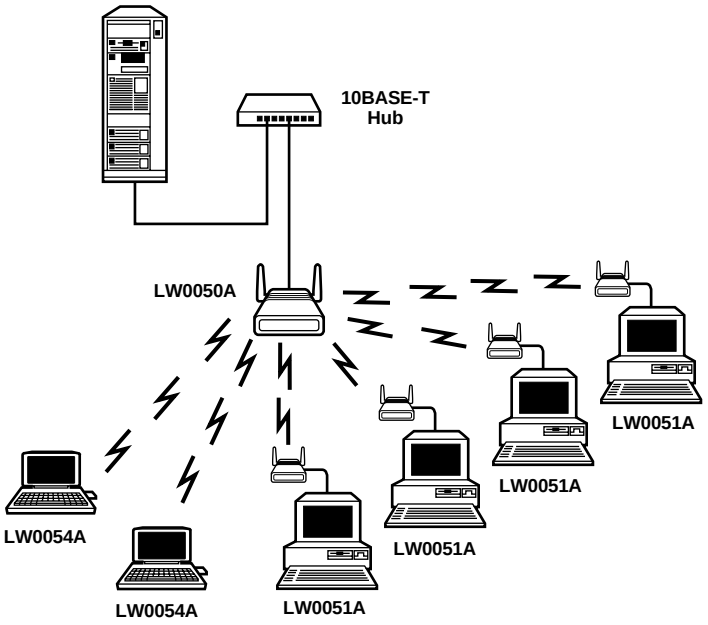


Figure C-2. The Basic Wireless LAN Cell.

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

The Access Point also functions as a bridge between the wireless stations and the wired network and the other wireless cells. Connecting the Access Point 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.

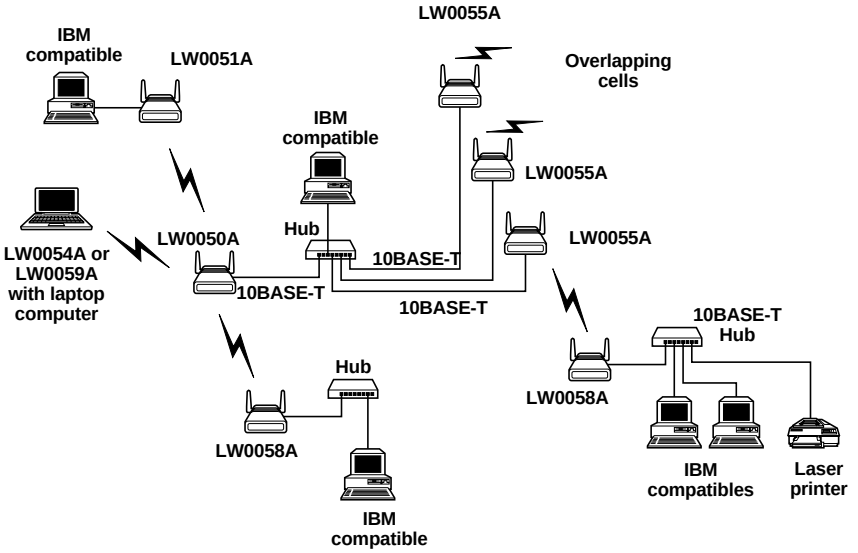


Figure C-3. Wireless LAN Connectivity.

C.2 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.

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

C.3 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 Access Points "illuminate" the same area, creating a common coverage area, which increases aggregate throughput. Stations inside the common coverage area automatically associate with the Access Points that is less loaded and provides the best signal quality. The stations are equally divided between the Access Points in order to equally share the load between all Access Points. Efficiency is maximized because all Access Points are working at the same low-level load. Load balancing is also known as load sharing.

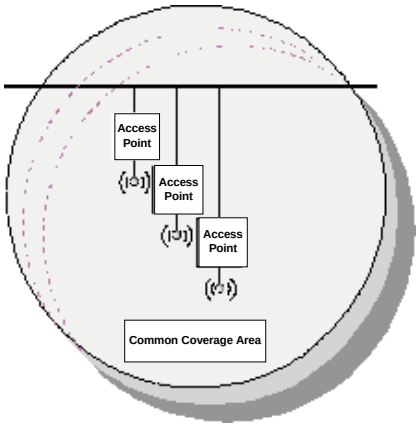


Figure C-4. The Common Coverage Area of a Multi-cell Structure.

C.4 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.

C.5 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.

C.6 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. When errors and retransmissions are occurring, no fragmentation or longer fragment length adds overhead and reduces efficiency.

C.7 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 information on how long 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 x milliseconds, so they cannot transmit even if the medium seems to be free.

C.8 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, the system must hop quickly. If the link is quiet and clean, it is better to hop slowly, reducing overhead and increasing efficiency.

Appendix D. Radio Signal Propagation

D.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.

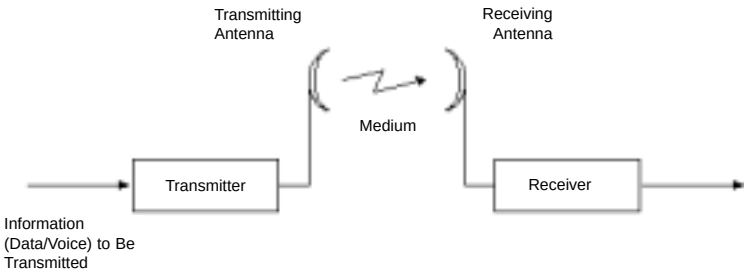


Figure D-1. A Typical Radio System.

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.

D.2 RF Terms and Definitions

dB

An abbreviation for decibel, a comparative measure of signal strength.

dBm

An *absolute* measure of signal strength. 0 dBm = 1 milliwatt. (See "RF Power Level" below.)

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:

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

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

For 100 mW, the calculation would be:

$$P_{dBm} = 10 \times \text{Log } 100 = 20 \text{ dBm}$$

For link-budget calculations, it's more convenient to express the measurements in dBm than in watts.

Attenuation

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

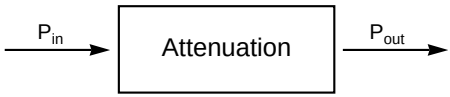


Figure D-2. Attenuation of an RF signal.

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, because of attenuation, half the power is lost (P_{out}/P_{in} = 1/2), then attenuation in dB is $-10 \times \text{Log}\ (1/2) = 3$ dB

PATH LOSS

Loss of power of an RF signal traveling (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:

Free-space loss = $32.4 + 20 \times \text{Log}(F_{MHz}) + 20 \times \text{Log}(R_{km})$

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: $100+20 \times \text{Log}(R_{km})$

ANTENNA CHARACTERISTICS

Isotropic Antenna
A hypothetical 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 (isotopically). 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.

Omnidirectional Antenna
An antenna that 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.

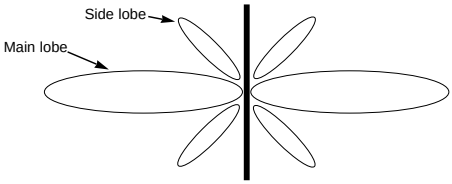


Figure D-3. Side View.

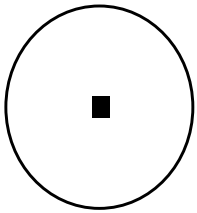


Figure D-4. Top View.

Directional Antenna
An antenna that 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:

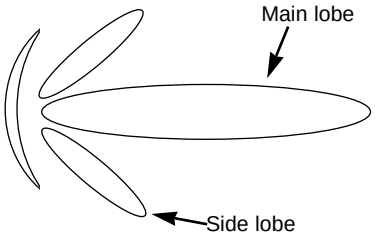


Figure D-5. Radiation Pattern of Directional Antenna.

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.

EIRP (Effective Isotropic Radiated Power)
The power transmitted by an antenna. 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
Pl	Path loss in dB
Cr	Receiver cable attenuation in dB
Si	Received power level at receiver input in dBm
Ps	Receiver sensitivity in dBm

$Si = P_{out} - Ct + Gt - Pl + Gr - Cr$
$EIRP = P_{out} - Ct + Gt$

Example:

Link Parameters:

Frequency: 2.4 GHz
P_{out} = 4 dBm (2.5 mW)
Tx and Rx cable length (Ct and Cr) = 10 m cable type RG214 (0.6 dB/meter)
Tx and Rx antenna gain (Gt and Gr) = 18 dBi
Distance between sites = 3 km
Receiver sensitivity (Ps) = -84 dBm

Link Budget Calculation:

$EIRP = P_{out} - Ct + Gt = 16$ dBm
$Pl = 32.4 + 20 \times Log(F_{MHz}) + 20 \times Log(R_{km})$ @ 110 dB
$Si = EIRP - Pl + Gr - Cr = -82$ 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 because of 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.

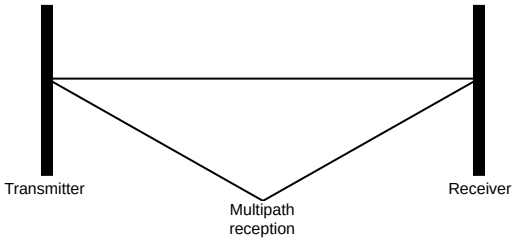


Figure D-6. Multipath Reception.

- *Bad Line of Sight*

  An optical line of sight exists if you can see one antenna from the other—there are no obstructions between them.

  Radio-wave clear line of sight exists if a certain area around the optical line of sight (Fresnel zone—see the next page) 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.

Line of Sight

An optical line of sight exists if you can see one antenna from the other.

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:

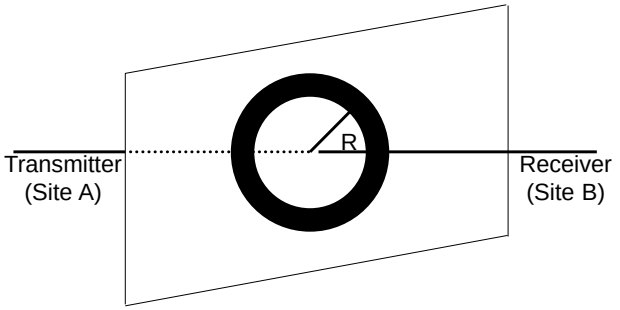


Figure D-7. Fresnel Zone.

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

R: radius of the first Fresnel zone

λ: wavelength

D: distance between sites

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

Appendix E. IEEE 802.11 Technical Tutorial

The purpose of this chapter is to give you a basic overview of the IEEE 802.11 Standard. You'll be able to understand the basic concepts, principles of operation, and reasons behind some of the features of the Standard.

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

E.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).

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:

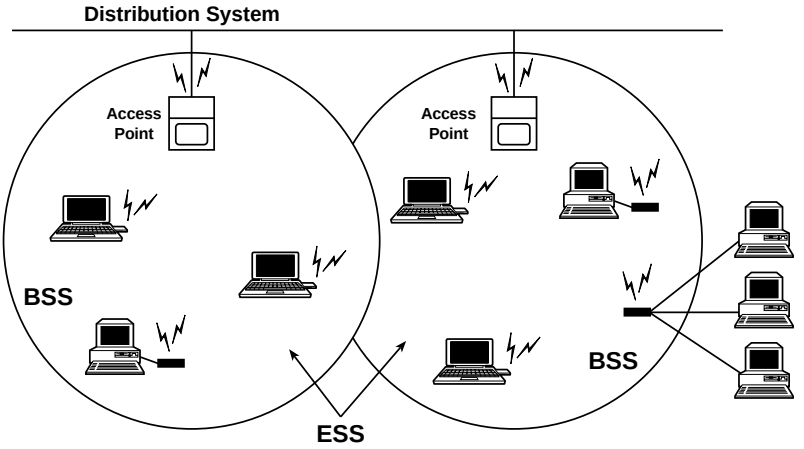


Figure E-1. Typical 802.11 LAN.

The standard also defines the concept of a "portal." A portal is a device that interconnects an 802.11 LAN 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 Access Point and the Portal on a single physical entity. For example, the Pro 11 Series Access Point provides both functions.

E.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 Mbps) 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.

E.3 The MAC Layer

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

E.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 (meaning that 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 they allow 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 packet can be retransmitted by the MAC layer 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 either it receives acknowledgment or the fragment is thrown away after a given number of retransmissions.

E.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, because 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:

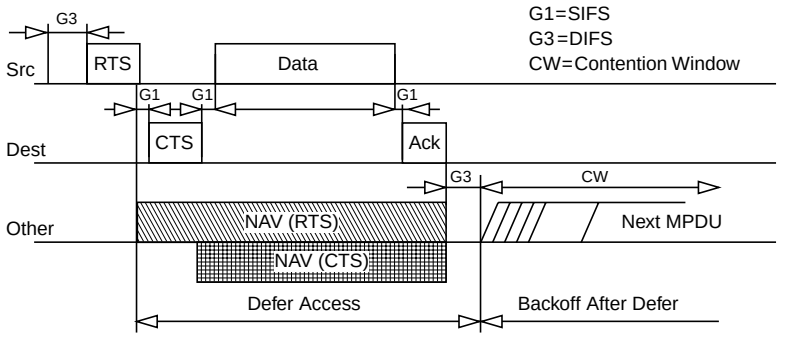


Figure E-2. Transaction Between Stations A and B.

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

E.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.)

E.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:

- Because of the higher Bit Error Rate of a radio link, the probability of a packet's getting corrupted increases with the packet size.
- In case of packet corruption (due to either 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. It receives an ACK for the said fragment, or

2. It 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 Access Point 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):

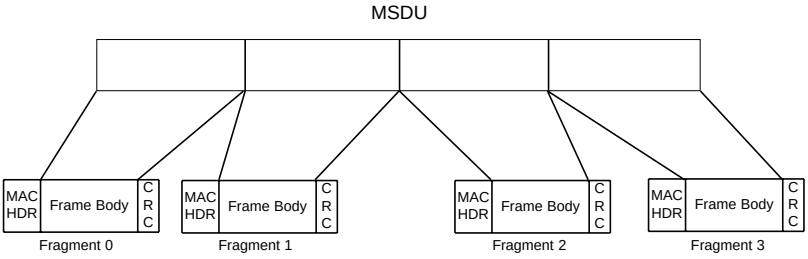


Figure E-3. Frame Fragmentation.

E.3.5 Inter Frame Spaces

The Standard defines four 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, so it has 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 it's called in this case), to gain access to the medium before any other station. This value is SIFS plus a Slot Time (defined in **Section E.3.6**), 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.

E.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:

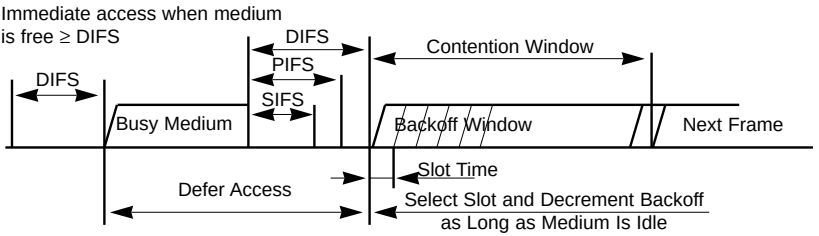


Figure E-4. Access Mechanism.

E.4 How Does a Station Join an Existing Cell (BSS)?

When a station wants to access an existing BSS (either after power-up, after 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 Access Point (the beacon frame is a frame sent out periodically by the Access Point 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 Access Point.

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

E.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 Access Point and the station, where each side proves the knowledge of a given password.

E.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 Access Points) 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.

E.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 one. (The Pro 11 Series product line provides a patented enhanced roaming mechanism which allows stations to roam at speeds of 60 km/h without losing or duplicating packets.)

E.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 Access Point's clock, using the following mechanism:

The Access Point periodically transmits frames called Beacon Frames. These frames contain the value of the Access Point'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 Access Point's clock. This prevents clock drifting, which could cause loss of sync after a few hours of operation.

E.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)

E.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.

E.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 connectionless environment, where packets may get lost (as any LAN).

E.8 Power Saving

Wireless LANs are typically related to mobile applications. In this type of application, battery power is a scare 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 Access Point 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 Access Point also periodically transmits information about which Power Saving Stations have frames buffered at the Access Point, 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 Access Point waiting for delivery, then the station stays awake and sends a Polling message to the Access Point to get these frames.

Multicasts and Broadcasts are stored by the Access Point, and transmitted at pre-defined intervals (called DTIM), all stations—both stations working in Power Saving mode and stations working in Normal mode, will be awake at that period and will receive this kind of frames.

Unicasts are stored by the Access Point, and transmitted at station-defined intervals (called Listen Intervals), when all stations who wish to receive this kind of frames are awake. Unicast frames are transmitted upon request only, whereas, Multicast frames are transmitted automatically at every DTIM interval.

NOTE

Unicast frames can also be poled by the stations at the DTIM intervals.

E.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 (for example, 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 (for example, beacon frames).

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

E.10 Frame Formats

All 802.11 frames are composed of the following components: Preamble, PLCP Header, MAC Data, and CRC.

E.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.

E.10.2 PLCP Header

The PLCP Header is always transmitted at 1 Mbps 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 Mbps to 4.5 Mbps.
- **Header Error Check Field**, which is a 16-bit CRC error-detection field.

E.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.

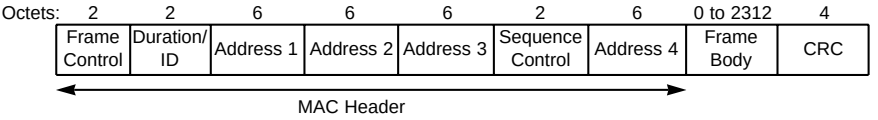


Figure E-5. MAC Frame Format.

Frame Control Field

The Frame Control field contains the following information:

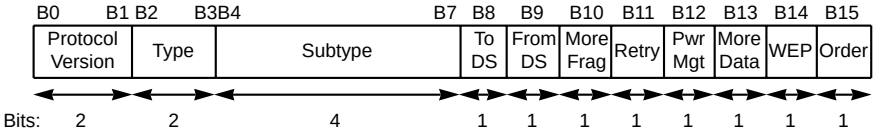


Figure E-6. Frame Control Field.

Protocol Version

This field consists of 2 bits which are unvarying 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 Access Point for forwarding to the Distribution System (including the case where the destination station is in the same BSS, and the Access Point 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 Access Point 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. (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 LAT.)

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 Access Point 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 Access Point 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
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)

E.11 Most Common Frame Formats

E.11.1 RTS Frame Format

The RTS frame looks like this:

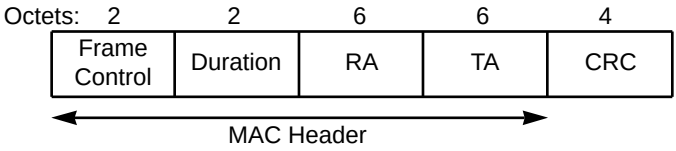


Figure E-7. RTS Frame Format.

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

The TA is the address of the Station Adapter 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.

E.11.2 CTS Frame Format

The CTS frame looks like this:

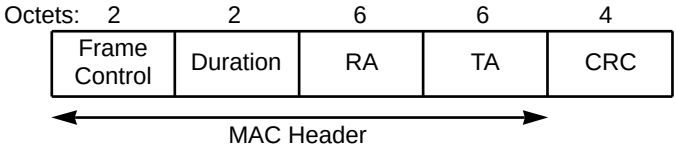


Figure E-8. CTS Frame.

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.

E.11.3 ACK Frame Format

The ACK frame looks like this:

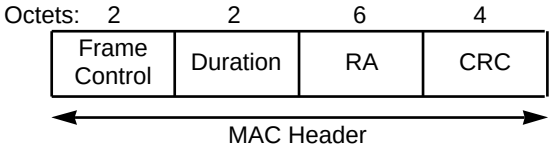


Figure E-9. ACK Frame Format.

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.

E.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, thus 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.

E.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, coworkers 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 Access Point functions are not supported (such as frame-relaying between two stations not in range, or Power Saving).