
Wireless Local Area Network Campus BridgeLINK-II™ User Guide

Notices

FCC

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC ID:	MCIPUNIIT
FCC Rule Part(s):	15
Frequency:	5.8 GHz
Equipment Class:	Low Power Communication Device Transmitter
Max. Output Power:	50 mW

Notes:

This device has shown compliance with new rules adopted under Docket 87-389 and is not affected by Section 15.37, transition rule.

Each radio is marked with its operating frequency.

FCC regulations require that a person knowledgeable in electronics and trained in the correct installation of this device professionally install this device.

All interface cables must be shielded.

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: 1) this device may not cause harmful interference, and 2) this device must accept any interference received, including interference that may cause undesired operation.

Disclaimer

The instructions in this document have been carefully checked for accuracy and are presumed to be reliable. RadioLAN Marketing Group and its writers assume no responsibility for inaccuracies and reserve the right to modify and revise this document without notice.

It is always our goal at RadioLAN Marketing Group (also known as RMG for short) to supply accurate and reliable documentation. If you discover a discrepancy in this document, please e-mail your comments or suggested corrections to docs@radiolan.com.

No part of this publication may be placed in a retrieval system, transmitted, or reproduced in any way, including, but not limited to, photograph, photocopy, computer disk or other record, without prior agreement and written permission from:

RadioLAN Marketing Group (RMG)
185 Lewis Road, Suite 30
San Jose, CA 95111
Phone: (408) 365-6200
FAX: (408) 365-7675

Trademark Disclosures

RMG has made every effort to provide disclosures when using trademarks owned by other companies. Trademarked designations appear throughout this publication. The publisher states that it is using the designations only for editorial purposes, and to the benefit of the trademark owner with no intent to infringe upon that trademark. The following trademarks are found in this manual:

10BaseRadio™, RadioNET™, RadioLAN10™, and Campus BridgeLINK-II-II™ are trademarks of RadioLAN Marketing Group.
Microsoft™, Microsoft Internet Explorer™ and LAN Manager™ are trademarks of the Microsoft Corporation.
Netscape™ is a registered trademark of The Netscape Corporation
Java™ is a trademark of Sun Microsystems, Inc.
RSA™ is a trademark of RSA Security, Inc.

Manual Conventions

The following text formats are used throughout this manual:

References to other locations in the manual or to other manuals provided by RMG are *italicized*.

Narrow Bold Letters describe **buttons** and **fields** on the screen.

SMALL CAPITAL LETTERS describe **Screen Names** or **Screen Tab Names**.

Bold and Italicized Letters indicate important information

Table of Contents

Notices	ii
FCC	ii
Disclaimer	iv
Trademark Disclosures.....	v
Manual Conventions.....	v
Table of Contents	6
Introduction	10
Before you get started.....	12
The Campus BridgeLINK-II™ System.....	13
The Directional Antenna	17
A Typical Campus BridgeLINK-II™ Application.....	18
Determining the Distance Between Buildings.....	19
Initial IP Address Setup	20
IPAssign method.....	20
Installing the CPU	24
Tools You Will Need.....	24
Locating the CPU	25

Mounting the CPU.....	26
Grounding Considerations.....	27
Installing the Antenna.....	28
A Brief Word About Safety.....	28
Choosing the Best Mounting Height.....	29
Siting Each Campus BridgeLINK-II Antenna	29
Apply Power to the CPU.....	31
Adding Security to the Wireless Network	32
Local Management.....	32
Dual Remote Management: HTML and SNMP.....	32
Using the RadioNET Campus BridgeLINK™ Manager.....	34
The CBL Web Server	34
Aiming the Directional Antennas.....	39
Discovering the Distant CBL.....	41
Setting Up Security Features.....	44
Setting Up SNMP Capabilities.....	45
Setting the CPU's Mode of Operation.....	54
System Features.....	55
Bridging the Link and 10BaseT Networks	56
Managing Packet Flow Through the CPU	64

Spanning Tree Parameters.....	69
Interrogating the CBL for Performance Information.....	72
Upgrading System Software.....	79
Saving or Rejecting Configuration Setting Changes.....	81
Resetting the CPU	82
Recording Important System Information.....	83
Viewing the System Log.....	86
Managing the CPU Locally.....	87
CPU Local Management	88
Hot Keys.....	88
Logging onto the CPU Configuration Screen	89
Using the Main Menu	91
Working with the System Configuration Menu.....	93
Configuration Manager Menu Items	97
Troubleshooting.....	112
Glossary.....	114
Appendix A: Indicators, Switches, and Connectors.....	117
Indicators	117

MDI/MDI-X	118
I/O Connectors	119
Serial Port Connector	120
Appendix B: Technical Specifications	121
Network Protocol.....	121
Standards Support	121
Electrical Specifications.....	121
Physical Specifications	122
Environmental Specifications.....	122
Electromagnetic Emissions.....	123
Safety Agency Approvals	123
Getting Technical Support	124

Introduction

Historically, connecting two buildings to allow networking between two local area networks required the expense and effort related to running a cable from one building to another. This may have involved installing an aerial cable or digging a trench and installing conduit and wiring between the two buildings, which is time-consuming, labor-intensive, and costly.

After installation, cable degradation, due to moisture, corrosion, or alterations in landscaping, can compromise the network connection between the two buildings. Repairing and replacing cable runs is also costly, time-consuming, and labor-intensive.

RMG overcomes these difficult installation issues with its Campus BridgeLINK-II™ product line. This exciting new technology easily connects two buildings, using radio frequency technology. Because this technology uses radio frequency to make the connection between the buildings, cable runs, conduit, trenching, and labor involved with these activities are no longer required.



Figure 1: The Campus BridgeLINK-II™

RMG allows you to connect two buildings, which are up to one mile (1.6 km) apart, using a Campus BridgeLINK-II Processor Unit (CPU), a Companion Radio Module (CRM), and an 8.86 inch square directional antenna for each building link. When using the CBL application, you need only install the components at each building, aim the antennas toward one another, and power the system on. The only requirements for each building location are Campus BridgeLINK-II™ system components and access to network cabling and power.

The directional antenna and its cabling is weatherproof, small-profile, and sturdy. Because the directional antenna allows for a 19° angle of operation, aiming the antennas so they point toward one another is nearly effortless.

Connecting two networks in two locations using the old-fashioned, hard-wired method could take days, considering the labor-intensive effort needed. When using Campus BridgeLINK-II, the task is simplified. The task of connecting two networks is reduced to a few hours, without the labor related to trenching, laying conduit and then cleaning up afterward.

In this section, we will introduce you to the concepts of Campus BridgeLINK communication, using a RMG Wireless Campus BridgeLINK-II system. Here, you will become familiar with the CPU, the CRM, the directional antenna, and the signal analysis tools.

Before you get started

Tools you'll need

- Drill and drill bit
- Screwdriver and screws
- Ladder
- Pencil
- Measuring tape
- Carpenter's square

Check line-of-site

To maintain a very high quality link, it is important to have a line-of-sight between the transceiving stations. Check to make sure that there will not be any objects, such as buildings or trees, blocking the line-of-site between the two antennas.

The Campus BridgeLINK-II™ System

The Campus BridgeLINK-II system includes the Processor Unit (CPU) with a mounting bracket, a Companion Radio Module (CRM), an RF Cable, and a directional antenna. Also included are the power transformer and connector cable.

Campus BridgeLINK-II™ Processor Unit (CPU)

The CPU has a number of LED indicators and jacks that allow you to connect the module to external devices and help you see its status.

LED Indicators

The front of the CPU features three LED indicators:

- The green Power LED illuminates when power is applied to the CPU. As long as the CPU is powered, this LED is normally illuminated.
- The green Diagnostic LED illuminates for several seconds during the power-on diagnostic sequence. When the CPU is operating, this LED is normally extinguished.
- The green Radio LED illuminates when the CPU detects the presence of the distant CBL. When the CPU is operating, this LED normally illuminates when the near and far CPUs are active.

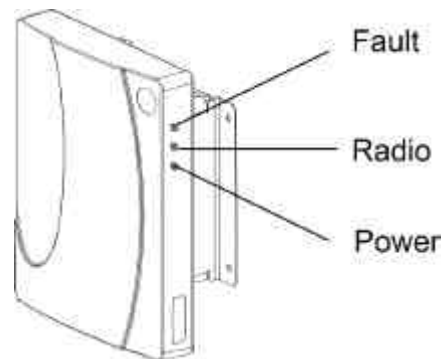


**Figure 2: Campus BridgeLINK-II™
Basic Assembly**

I/O Ports

The back of the CPU features four ports from left to right:

- Power port
- 10BaseT (Ethernet) port
- Console port
- CRM Radio port

Power Port

Insert the Power adapter into this port.

AC Power Transformer

The power transformer provides an easy connection to electrical outlets. One end of the transformer has a power cable with a connector that is compatible with the CPU's power jack. The other end plugs into an electrical outlet. RMG recommends using a non-switched electrical outlet for connection to the CPU.

The output from the Campus BridgeLINK-II power transformer is AC. Be careful not to use older DC power transformers from the original Campus BridgeLINK to power the Campus BridgeLINK-II. Use only the AC Power transformer that came with the Campus BridgeLINK-II unit, or contact RMG for a suitable replacement power transformer.

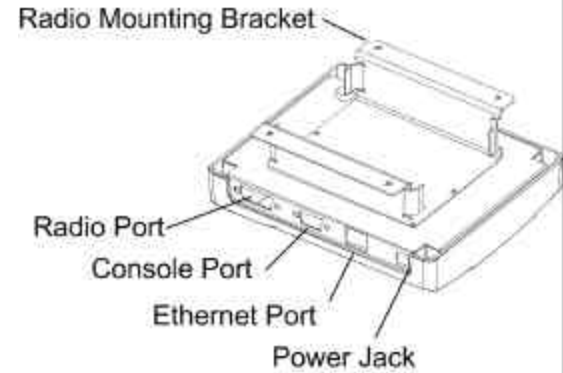


Figure 3: CBL-II Ports

10BaseT Ethernet Port Jack

The 10BaseT port interfaces the CPU to its local area network. The 10BaseT port is RJ45-compatible, which allows an eight-wire connection to a network hub or other hard-wired external device. The 10BaseT interface is set to automatically detect MDI/MDI-X, and you may hear a clicking sound during this detection process. You may use a straight through or cross over cable.

10BaseT LED Indicators

- On the upper left and right corners of the 10BaseT port are green LEDs, which indicate transmit and receive status from the network.
- When the CAR LED illuminates, this indicates that the Ethernet carrier is active. This LED should be illuminated when the Campus BridgeLINK-II is operating normally.
- When the ACT LED illuminates, this indicates Ethernet activity on the network. This LED flickers when there is communication taking place on the Ethernet network.

Console Port Jack

The console port is a female DB9 connector and allows you to connect a local terminal or terminal emulator to the Campus BridgeLINK-II using a standard straight-through, male-to-female serial cable. You need a local terminal connection to configure the CPU. Typically, this is only needed at installation or when particular upgrades are to be applied. Although the Campus BridgeLINK-II is browser manageable, troubleshooting is best done using the *Console Port*.

CRM Port

At the opposite end of the CPU, there is a female 15-pin D connector. The connector allows you to connect the CRM to the CPU, using the cable that is attached to the Radio Unit.

CRM Mounting Bracket

The mounting bracket is specially shaped so that it allows the CRM to slide into the mounting bracket before securing the CPU to a flat surface.

The Companion Radio Module (CRM)

The CRM interfaces the CPU with the directional antenna. The CRM is small, durable, and designed to insert easily into the mounting bracket that is attached to the CPU.

On one end of the CRM, there is a Type N connector and an LED indicator. The Type N connector attaches the CRM to the directional antenna.

The LED illuminates amber when the CRM is transmitting data. It illuminates green when the CRM is receiving data.

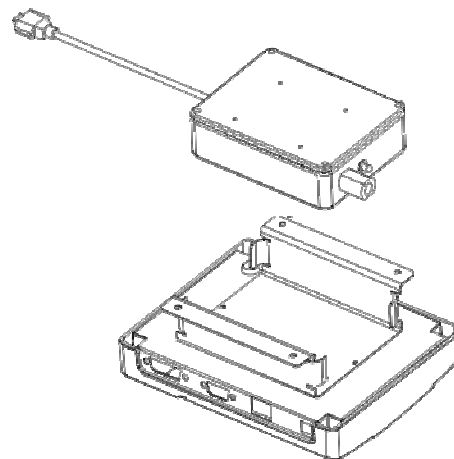


**Figure 4: CRM Radio
(Companion Radio Module)**

The Directional Antenna

The directional antenna assembly includes the directional antenna and a mounting clamp. The directional antenna is an 18dbi-gain, small-profile directional antenna. It is 8.86 inches square, and mounted on a pivoting base.

Antenna Cable

The antenna cable provided is either a 15-foot or 45 foot, low-loss cable. Cold-shrink tubing is supplied to cover the antenna end connector after connection to the cable. See the installation instructions packaged with the shrink tubing for installation directions.

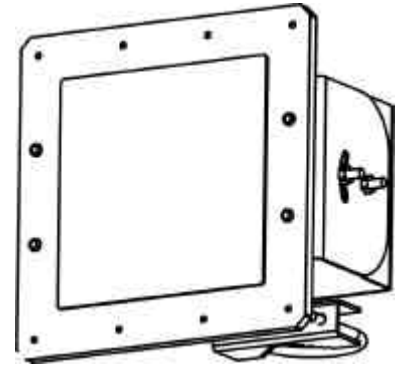


**Figure 5:
Directional
Antenna**

A Typical Campus BridgeLINK-II™ Application

Figure 6 shows a typical Campus BridgeLINK-II application in which two buildings, with local area networks in each, are located up to 1 mile away from one another. Notice that there are no solid obstructions between the two buildings and that each building antenna points toward the other.

Because the system uses radio frequency to establish the connection between the two buildings, it is important to avoid blocking the radio link with any objects, such as trees, buildings, walls, or items that are attached to the building walls, such as stairwells, fire escapes, or other antenna equipment.

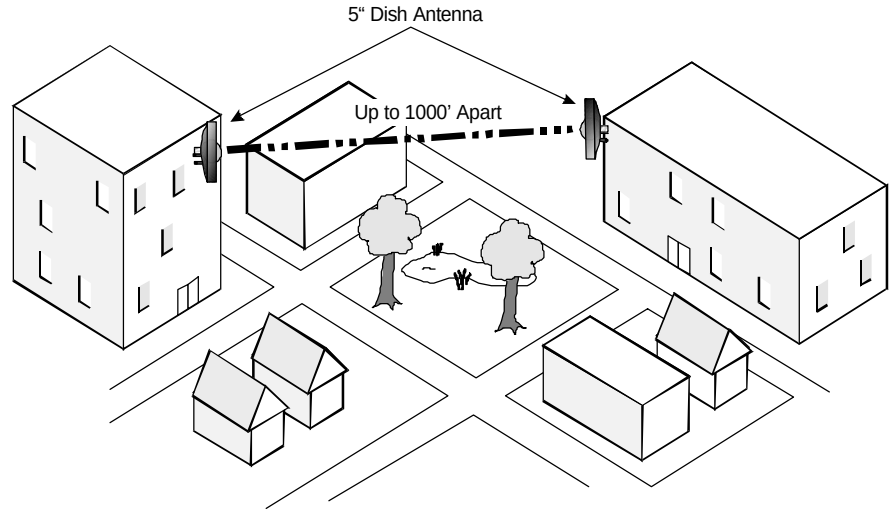
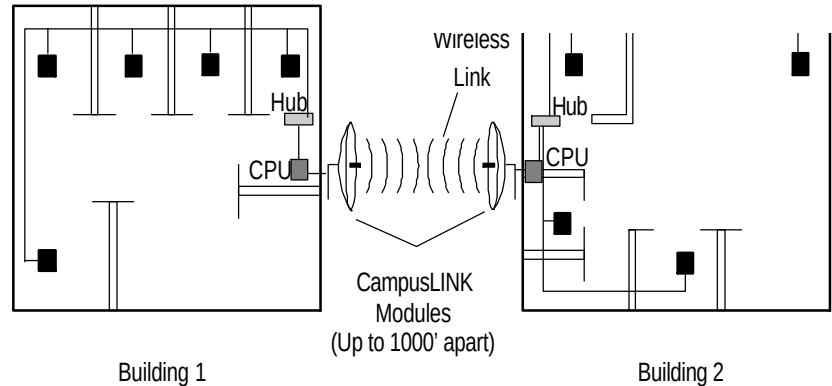


Figure 6: A Typical Campus BridgeLINK-II™ Application

Figure 7 illustrates the networks inside each building. Notice that the CPU is attached directly to a hub, which connects network nodes together.



Determining the Distance Between Buildings

Figure 7: Linking Networks in Two Locations

It is important to verify that you do not exceed the distance capabilities of Campus BridgeLINK-II. If you are unsure of the distance between the two points, you can use a measuring device, such as optical devices found in some binoculars. You can also see the architect's site plan or contact a local surveying service for assistance.

Initial IP Address Setup

Before you can use the TCP/IP management services of a CPU, it must contain a valid network IP Address. There are two ways to assign an IP Address to the CPU:

- The IPASSIGN utility provided by RMG.
- A VT-100 terminal connection to the CPU Local Port.

This section describes in detail each method for assigning the CPU an IP Address.

IPAssign method

To use the IPASSIGN Utility, you must connect the Campus BridgeLINK-II CPU to a PC with a 10BaseT Card, as in Figure 8. Neither the PC nor the network can be running a DHCP server while performing this procedure. (A DHCP server assigns IP Addresses to devices on the network.) You should also keep isolated from your main network.

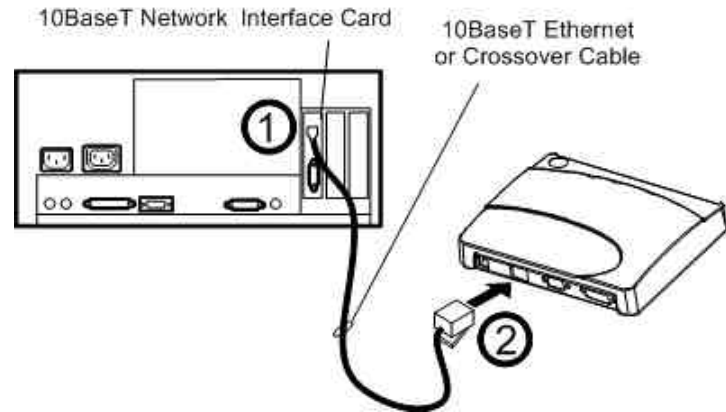


Figure 8: Quick Configuration

To run the IPASSIGN Utility in a PC with a 10BaseT Network Interface Card, connect a 10BaseT cable between the CPU and the jack on the PC's Network Interface Card. You may also connect the PC to the CPU through a 10BaseT network or across a CBL link as long as there is not a DHCP server running on the network.

1. Connect one end of the RJ45-compatible cable to the PC's network interface card or network hub, and connect the other end of the cable to the 10BaseT port on the CPU.
2. Connect the CRM to the CPU, if you will run IPASSIGN across the CBL link.
3. Connect the CPU's power adapter to the power jack on the CPU, and plug the power adapter into an electrical outlet.

Make sure the 10BaseT Link light is on.

Using the IPASSIGN Utility to assign the CPU's IP Address

RMG provides the IPASSIGN program with your package. The utility allows you to assign an IP Address to the CPU quickly. The PC's Network Interface Card must have an IP Address assigned, and the address you wish to assign the CPU must be on the same IP Subnet.

1. Insert the diskette or CD into the appropriate drive. These instructions assume that you are using Drive A.
2. In Windows, click on Start, then click on **Run**.
3. In the field that appears, type `a:\ipassign`, and then choose **OK**. The utility will start.

After the utility starts, it automatically searches the network for any new CPUs. It finds the CPU that is connected, then lists the CPU's MAC Address in the **New BLINK unit** field.

4. Type in the appropriate IP address and Subnet Mask address into the fields on the screen, and then click the **Assign** button.
5. The utility assigns a temporary IP address, and displays a message asking if you want to further configure the CPU. Note the temporary IP address and make the following choices:

Yes This launches your web browser and connects you to the CBL Home Page, allowing you to assign a permanent IP address and to further configure the CPU. You must also disable DHCP to set a permanent IP address, and save all your settings. See IP parameters on page ?.

No This quits the utility. You will need to assign a permanent IP address, disable DHCP and save your settings from a PC running a web browser before powering off the CPU.

Assigning an IP Address using the Serial Port

You can connect the CPU to a VT-100 terminal or a PC running terminal emulation software.

1. Set up a terminal or run terminal emulation software with the following settings: 9600 bits per second, 8 data bits, no parity, 1 stop bit, and no flow control.
2. Connect a standard DB-9 serial cable (not included) between a COM port on the terminal or on the PC and the CPU's DB-9 serial port.
3. Power on the CPU. You will see a series of tests then a logon screen. Initially there is no password, so press **<ENTER>**.
4. Arrow down to System Configuration, and press **<ENTER>**.
5. Arrow down to IP Parameters, and press **<ENTER>**.
6. Enter the IP Address, Subnet Mask, and Default Gateway IP Address.
7. Next, highlight DHCP Operation Mode. Press **<ENTER>** until the Disabled is displayed.
8. Press **<BACKSPACE>** to go to the previous screen. Arrow down to Configuration Changes, and press **<ENTER>**.
9. Choose Save All Configuration Changes, and press **<ENTER>** twice. The CPU will reset using the new IP address.

You may also use this same serial connection to configure and manage the CPU. See Managing the CPU Locally on page **87** for more information.

Installing the CPU

When installing a CPU you may mount it onto a wall or a ceiling. You must locate the CPU at a distance from the antenna that is no farther than the cable will allow. The cable length is either 15 or 46 feet; this means you must consider all bends in the cable when determining your distance.

You must also locate the CPU in an area from which it has access to local network cabling and electricity. Before selecting an electrical outlet for use in powering the CPU, verify that the electrical outlet is non-switched (for example, it is not attached to a wall switch). You should also consider placing the CPU in a location where it is out of reach of the general public.

FCC regulations require that this device be professionally installed by a person knowledgeable in electronics and trained in the correct installation of this device.

All interface cables must be shielded.

Tools You Will Need

To install the CPU, you will need the following tools: drill, drill bit, screwdriver, screws, pencil, and measuring tape.

Locating the CPU

After verifying that the CPU is located near a power source and network cabling, and is within the antenna's cable distance constraint you may install the CPU securely to the mounting surface (for example, a shelf, wall or ceiling).

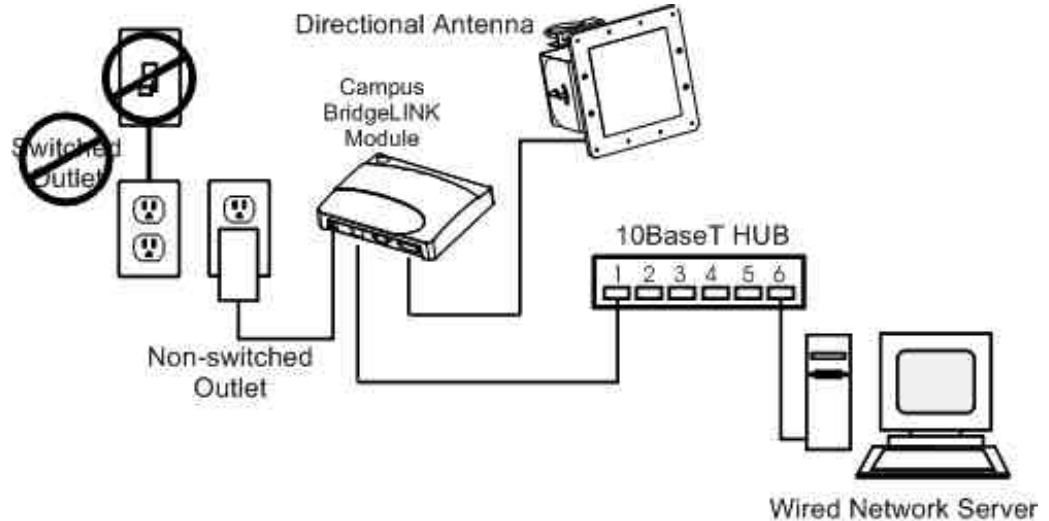


Figure 9: Locating the CPU Closely to Network, Power, and the Antenna

Mounting the CPU

Before mounting the CPU to the mounting surface, connect the connector at the end of the CRM's cable to the D-connector on the CPU using the supplied 15-pin cable.

Route the antenna cable from the directional antenna to the CRM, and slip the cold-shrink tubing over the end of the cable before connecting the cable to the antenna.

Connect the cable to the CRM, using a clockwise rotation. Tighten the antenna connector so that it is snug but does not strip the threads of the connector on the CRM. Complete the shrink tubing installation by following the instructions provided with the tubing.

Orient the CRM so that its cable does not cross over the mounting brackets and then insert the CRM into the mounting bracket so that it is flush with the rim of the bracket.

Orient the CPU on the mounting surface in the location where you would like it to be attached. Use a pencil to mark the brackets screw hole locations onto the surface upon which you will mount the CPU.

At the location's screw holes, install any necessary anchoring devices. This is especially recommended when installing the CPU onto a sheet-rock or gypsum surface.

Hold the CPU up to the mounting surface, orienting the screw holes with the mounting anchors, then drive screws securely into the surface. Tighten down the screws.

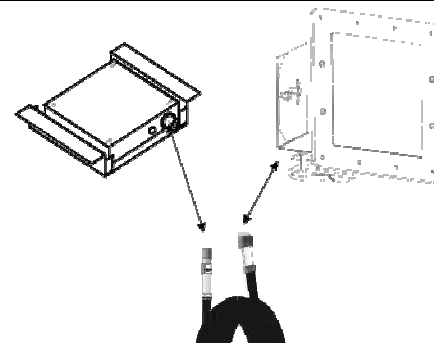


Figure 10: Connecting the Antenna

Attaching to the Network

When connecting the CPU to the network hub or to a PC, you must use a RJ45-compatible, dual modular cable. The cable is an eight-wire, twisted-pair cable and must not exceed the distance limitations provided by the IEEE 802.3 standard. After routing the cable to the network, insert the modular connector into the port on the CPU.

Grounding Considerations

RMG recommends that you properly ground the directional antenna as described in mounting hardware installation instructions and required by your local ordinances.

It is recommended that you connect the antenna assembly to a ground rod driven a minimum of 10 feet into the soil. For proper grounding of the antenna and cable, follow Section 810 of the National Electrical Code. Use UL-listed ground clamps and lugs.

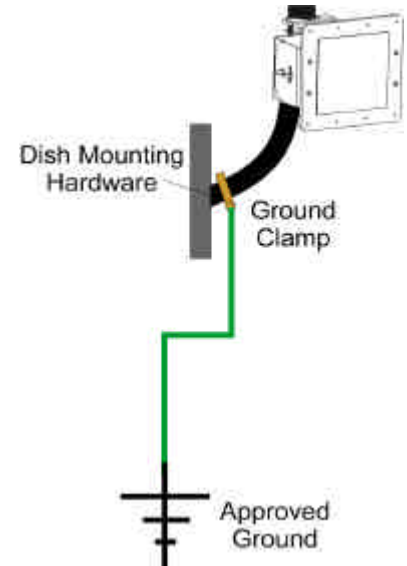


Figure 11: Acceptable Ground Source

Installing the Antenna

There are many methods for mounting the antenna onto a wall. The assembly includes a U-bolt that allows you to connect the directional antenna to a standard size mounting assembly that is used for other directional antenna applications. Directional antenna wall-mounting assemblies are available at your local computer store or retailer who sells directional antennas or satellite services. The directional antenna uses a U-bolt with a nut on each end. Slide the mounting clamp through the two eyeholes on the backside of the directional antenna, then secure the clamp to the mounting equipment that you chose.

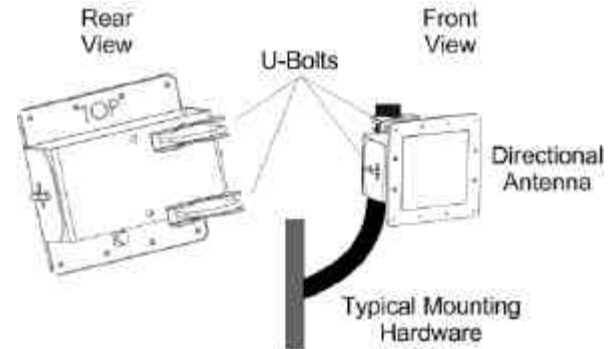


Figure 12: Attaching the

A Brief Word About Safety

If you chose to mount the antenna high up on a wall, make sure that you use the appropriate type of ladder. Follow ladder safety tips provided by its manufacturer. RMG recommends that you have a partner available to secure the ladder and to offer assistance while you are on the ladder. RMG recommends that you not mount the unit during stormy weather, on windy days, or anywhere near electrical cables.

Choosing the Best Mounting Height

Make sure that you choose the appropriate mounting height for the directional antenna. You must consider the cable distance between the directional antenna and the CPU, and the level of accessibility for routing cable and mounting the CPU.

If the structure has an eave, RMG recommends that you not place the antenna up so high into the eave that the roof of the antenna blocks a line-of-sight view to the antenna on the distant Campus BridgeLINK-II™ building. Before securing the antenna to the wall, verify that you can see the distant directional antenna and that the line of site is clear of all obstructions.

Siting Each Campus BridgeLINK-II Antenna

Once you have installed and grounded the mounting bracket assembly (provided by others), you can point the directional antenna toward the location of the distant antenna.

Tools You Will Need

To site the antenna properly, you will need to have a crescent wrench, a carpenter's square, a ladder, and a helper.

Adjusting the Antenna's Direction

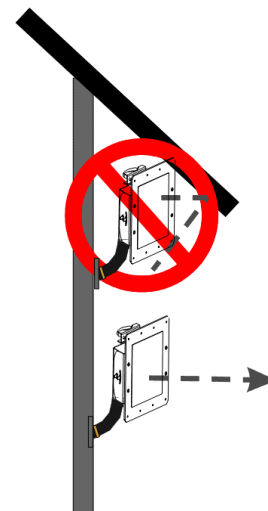


**Figure 13:
Mounting**

To adjust the antenna's direction you will:

1. Loosen the U-bolts to turn the antenna into the correct side-to-side direction (azimuth).
2. Loosen the nut on the tilt mount to adjust the antenna to the proper elevation.
3. Tighten all the nuts and bolts to safeguard the antenna against directions changes during high winds.

Siting Procedure

The Campus BridgeLINK-II has a 17° angle of reception for each of its antennas. This means that, from the center of the directional antenna, you can angle away from your target for as much as 8.5° in any direction. This makes it very easy to site the two antennas and align them properly.

If your application requires that the buildings are nearly one mile apart, it may be difficult to visually resolve the distant CBL antenna. In these cases you may need a compass, GPS, local maps, or other direction calibration equipment. Greater distances increase probability for line-of-site blockages: As the distance between buildings increases, there is a greater likelihood for objects appearing that block the line-of-site between CBL sites. When planning applications with greater distances, avoid problems caused by new construction, or a large grove of trees between the two sites by placing the antenna higher. This decreases the likelihood for line-of-site blockages over time.

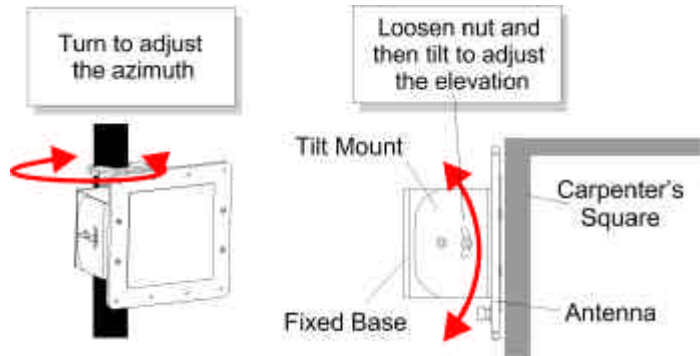


Figure 14: Aligning Antennas

Eyeball the Direction

Using a carpenter's square, align the square across the directional antenna's surface and adjust the antenna so that the carpenter's square points toward the distant Campus BridgeLINK-II™ antenna location.

After aligning the antenna, tighten the nuts on the mounting assembly so that it stays affixed in this direction and cannot be easily blown out of alignment by wind or heavy rain.

Next, connect the antenna cable to the back of the antenna. You can further align the two antennas, using the Campus BridgeLINK-II Manager. See *Aiming the Directional Antennas* on page 39 for more information.

Apply Power to the CPU

After verifying that the antenna cable is properly attached to the antenna and the CRM, and after making sure that the CRM is properly attached to the CPU, you can apply power to the CPU following these steps:

1. Connect the CPU to the power transformer.
2. Connect the power transformer to the electrical outlet.

If the CPU is properly powered, you should notice that the green Power LED illuminates.

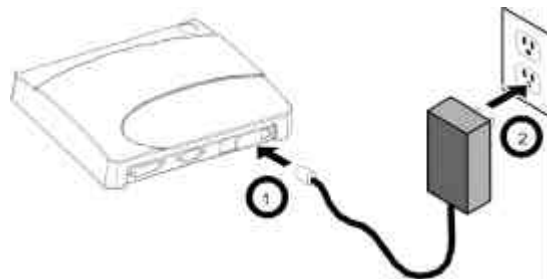


Figure 15: Power Connection Sequence

Adding Security to the Wireless Network

As an option, you can contact RMG to enable the RSA™ Data Encryption feature. This feature secures the wireless link by setting an encryption key that protects your sensitive data on the wireless link. When you enable Data Encryption, only CPUs that share the same encryption key can share data.

Local Management

The CPU includes a built-in serial port for connecting a VT-100 terminal or a modem. Using a terminal allows you serial access to configuration and system performance pages. Connecting a modem to the serial port allows you to dial into the CPU from a remote location to log in and configure or view system performance.

Dual Remote Management: HTML and SNMP

The CPU contains an SNMP (Simple Network Management Protocol) agent. When a remote SNMP Manager interrogates the agent, the agent presents system configuration and statistical information by way of the MIB (Management Information Base). While connected to the agent through the network, the manager receives the MIB and can see wireless network performance information.

When you use your SNMP Manager, you can make changes, see current status, and review new network history. The CPU now supports SNMP management, using the standard MIB for selected functions. Contact RMG for a copy of the CPU's MIB object functions.

The CPU's interface includes system security authentication passwords, so only remote users with the correct password can access and configure the CPU. The CPU offers up to three security access passwords, each configurable for read and/or write rights.

System Requirements

To successfully place a CPU into operation, you must meet the following requirements:

- The CPU must connect directly to a 10BaseT Network.
- The Campus BridgeLINK-II™ must be located within one mile of another Campus BridgeLINK.
- The network must use TCP/IP to communicate, using remote management.

Browser Requirements

To access the CPU by way of a 10BaseT Network, you must use a browser that is compatible with HTML, frames, and Java™ script language, such as Netscape™ 4.x or Microsoft Internet Explorer™ 4.x provides.

Using the RadioNET Campus BridgeLINK™ Manager

The Campus BridgeLINK Manager allows you to interrogate and interact with the CPU from a remote location on the IP network, using a Web browser to communicate with the CPU. Your browser must support Javascript™ and frames. After launching your browser, enter the IP Address for the CPU. If you just set up the CPU for the first time, you should have already assigned the CPU's IP Address using the IP ASSIGN Utility or with the VT-100 terminal.

This section discusses how to find the CPU on your network, how to log on to it, and how to use the CBL Web Server.

The CBL Web Server

The CBL Web Server allows you to view pages that contain configuration information about the CPU. Using the Web Server, you can assign passwords, set up IP Addresses for the CPU and SNMP management stations, set address filters, and view system performance statistics.

Most configuration pages have the following three buttons at the bottom of the page:

Reload.....Reloads entries in all fields on the page with previously saved values

OK Accepts entries. Choose this button when you have finished entering the desired information.

Use Default Enters default information into each field.

When using the Campus BridgeLINK-II™ Manager to make changes, edit your choices on the site pages and press OK on that page, then accept all session changes by accessing the SYSTEM CONFIGURATION - CONFIGURATION CHANGES page. Choose Save All Changes and Rest. This causes the CPU to store configuration changes and reset using the new configuration.

Browsing the Network for the CPU

To find the CPU on your network, follow these steps:

1. Open your Web browser
2. In the browser's address field, type the IP Address for the CPU, then press **<ENTER>**.

The browser searches the network for the CPU. When it finds the CPU, the CBL's Home Page or LOGON window appears, depending on the security.

Logging onto Campus BridgeLINK™ Manager

The LOGON window provides security to CPU configuration items. There are two fields on the page:

- User Name
- Password

Enter one of the user name/password combinations set in Access Security. (see Setting up Security Features on page 44) If this is the first time that you logged on, set up Access Security features immediately:

User Name

The **User Name** field is an entry field where you enter your user name to gain access to the configuration and diagnostic pages. Only entries matching those programmed into the SYSTEM CONFIGURATION: ACCESS SECURITY page are allowed access to the program.

Password

The **Password** field allows you to enter your user password for access to configuration and diagnostic pages. Enter your password here and then press **OK** to go to the home page.

If the user name and password match those stored in the ACCESS SECURITY page, you will be allowed to view and edit items on the page. If you make entries that do not match those stored in the program, you will fail to reach the home page and must try again.

Campus BridgeLINK™ Manager Organization

The Campus BridgeLINK™ Manager Website uses frames that allow you to size and view the pages according to your needs. The main menu is made up of the following items:

- Node Discovery—Checks the receive quality of the link.
- System Features—Enables enhanced CBL features.
- System Configuration—Configures the CPU for use with your network.
- System Statistics—Displays system performance statistics.
- System Status—Displays the system's current status.
- Antenna Aiming—Fine tune your directional antenna, and check connectivity.
- Reset—Resets the CPU.

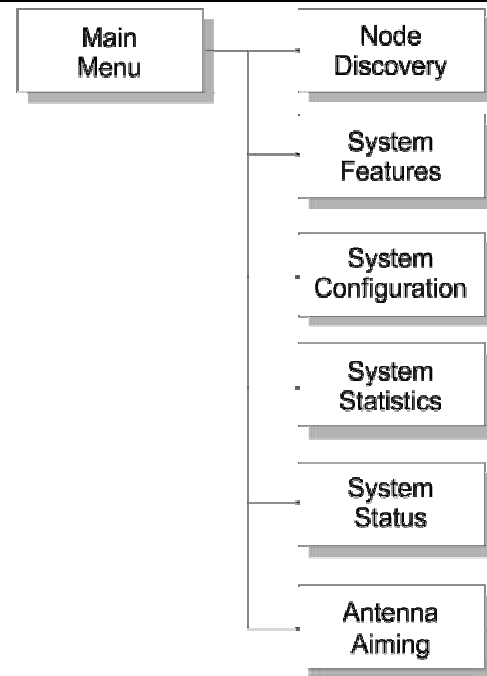


Figure 16: CBL Manager Main

Figure 17 shows the main screen. The left side of the page contains a menu that allows you to select the screen that you want to view or change.

Menu items that have a [+] next to them have submenu items that lead to more pages. After selecting a submenu item, the right frame of the page changes to display program items and other information. You can size the frames by clicking on the divider line and dragging the line to the size that meets your needs.



Figure 17: Campus BridgeLINK-II™ Manager Main Page

Aiming the Directional Antennas

If you are installing the Campus BridgeLINK-II™ system, or if you want to improve the alignment of the two directional antennas, use the System configuration - ANTENNA AIMING page. You may also want to check the connection to find the distant antenna's signal, and to improve signal quality. The page includes the following items:

- **Explicit Address** check box
- **CPU Name** drop-down list box
- **Frame Size** field
- **Estimated Distance** list
- **Successful %** field
- **Best** field
- **Worst** field
- **Sound** check box
- **Start** button
- **Stop** button
- **Save Distance Parameter** button

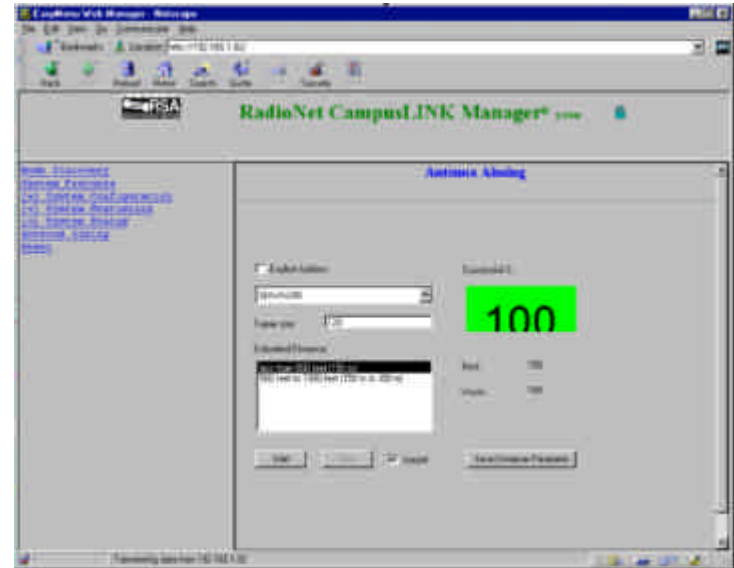


Figure 18: Antenna Aiming Page

Selecting the Distant Campus BridgeLINK-II's Address

The ANTENNA AIMING page allows you to select the remote CPU's Radio port name or explicit MAC address. If you place a check in the **Explicit Address** check box, the **CPU Name** drop-down list box changes to a field to enter a MAC address for the target CPU's radio port. Clearing the **Explicit Address** check box should display the Radio port name of the distant CBL in the **CPU Name** drop-down list box.

Setting the Frame Size

Select the desired frame size that you want to use for testing purposes. Similar to a PING, adjusting the frame size can vary test results. Enter your selection in the **Frame Size** field.

Setting the Estimated Distance Between Antennas

The **Estimated Distance** list allows you to choose the estimated distance between links. You must set this value on **both** sides of the link. Click a value in the list to make your selection. After testing, you can save the entries on the page by clicking the **Save Distance Parameter** button. This change is stored immediately, you do not have to save changes and reset.

Starting and Stopping the Test

You can begin and end the testing at any time. Click on the **Start** button to begin, and **Stop** to end.

Viewing or Hearing Status of the Link

Once you have started the test by clicking the **Start** button, you can view test results by viewing the **Successful %** field. You can also view the best and worst-case scenarios by looking at results that appear in the **Best** and **Worst** fields. This page features audio status of the **Successful %** field when you place a check mark in the **Sound** check box. A successful link should be at least 99%.

Discovering the Distant CBL

The CBL dynamically discovers one other CBL station in range. Each time the CBL places the distant node's information into an internal database. Alternatively, the CBL removes information for a distant CBL when it is out of range.

The NODE DISCOVERY page displays one distant CBL within range. The page displays a table with two main tabs:

- Station List
- Connectivity

Station List

The Station List tab shows the CBL that is in range. The list is a table with a number of columns. The table shows the following columns:

Name

This column displays the station name of the distant CBL.

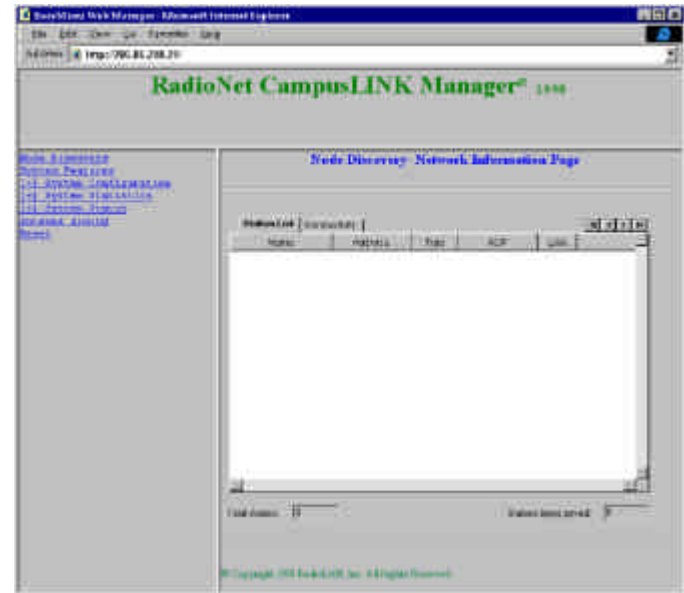


Figure 19: Node Discovery

Address

This column displays the station's MAC Address.

Type

This column displays the stations type. The only type found is: ***CBL Campus BridgeLINK-II***

ACP

This column is not applicable for a CBL.

Link

The Link column shows the connectivity quality for the station. The connectivity is rated with a number between 0 and 5 that represents the readability of the radio signal for the CBL indicated. Table 1 below shows the meaning of the quality designation.

Score	Color	Antenna Orientation
5	Green	Best Quality
4	Green	Good Quality
3	Yellow	Improve if possible
0,1,2	Red	Need to improve

Table 1: Link Quality Ratings

Connectivity

When you click on the Connectivity tab, the page shows the Connectivity table. This table includes the following headings:

- Name
- Link

Name

This column displays the station name of the distant Campus BridgeLINK.

Link

The Link column shows the connectivity quality for the station. The connectivity is rated with a number between 0 and 5 that represents the readability of the radio signal for the Campus BridgeLINK indicated.

Table 1 above shows the meaning of the quality designation.

Setting Up Security Features

The ACCESS SECURITY PAGE allows you to specify up to three sets of user names and passwords, which allow entry into the configuration and diagnostic pages. To get to this page, select **Access Security** from the System Configuration menu.

User Logon Name Fields

The **User Logon Name** fields allow you to enter from 1 to 12 characters to specify a user name. You can use letters and numbers for this entry. This entry is case-sensitive, so be sure to note the user name exactly as you enter it here. Make your entry, then press the **Tab** key to move to the **User Logon Password** field.

The User Logon Password Fields

The **User Logon Password** and **Retype User Logon Password** fields allow you to enter from 1 to 12 characters to specify the user password. You can use letters and numbers for this entry. This entry is a case-sensitive field, so be sure to note the user password exactly as you enter it here, and make sure the two fields match.

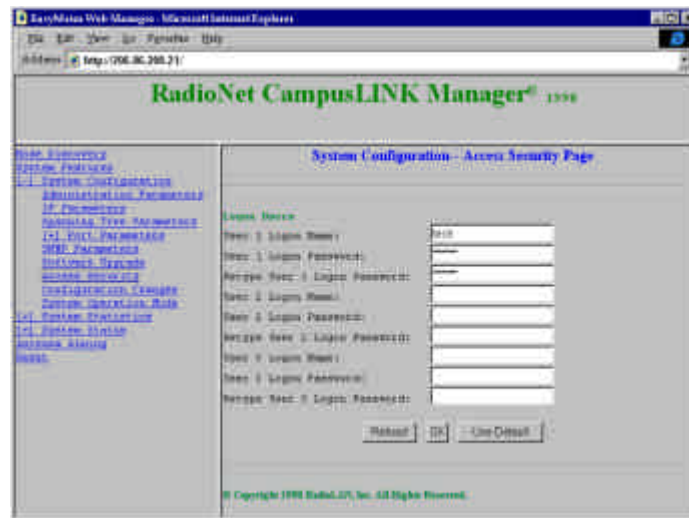


Figure 20: Access Security Page

Setting Up SNMP Capabilities

The CPU contains an SNMP agent, which processes information from the CPU MIB. The MIB (Management Information Base) contains system status information, which allows for remote queries for system status and control with SNMP management applications from remote locations on the network.

There are three basic information pages related to SNMP management:

- Administration Parameters
- IP Parameters
- SNMP Parameters

After configuring each of these pages, you will be able to access the CPU from any location on the network if you have rights to do so.

System Name

System Contact

System Location

[illegible]

Figure 21: Administration Parameters Page

- IP Address
- Subnet Mask
- Default Gateway IP Address
- DHCP Operation Mode radio buttons
- DHCP Server IP Address

IP Address

The first number can be zero to 223. Each of the next numbers can be zero to 255. For example, 192.168.0.200 could be an IP Address. Within an isolated network, you can assign IP Addresses at random as long as each one is unique. If you are connecting the CPU directly to the Internet, standards require using a registered IP Address to avoid duplicates.

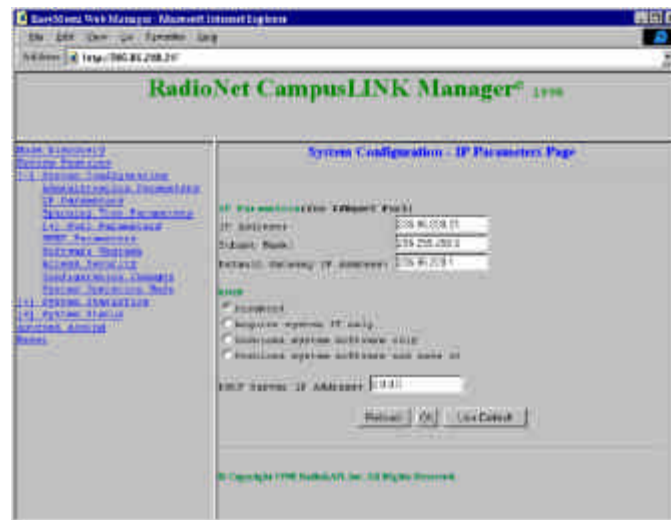


Figure 22: IP Parameters Page

Subnet Mask

The **Subnet Mask** determines the IP Network for the CPU. This number, combined with the IP Address identifies the station on the network. An example for a Class C IP network is 255.255.255.0.

Default Gateway IP Address

The gateway is a combination of hardware and software that links two different types of networks. Gateways between networks, for example, allow users on different e-mail systems to exchange messages.

The gateway IP Address could identify a router that controls the flow of data packets to the node (computer, printer, etc.).

Type in the gateway IP Address using the following format: The first number can be zero to 223. Each of the next numbers can be zero to 255, each separated by a period. The address looks similar to the following: 192.168.0.1

DHCP Support

Short for **D**ynamic **H**ost **C**onfiguration **P**rotocol, this protocol assigns dynamic IP Addresses to devices on a network. Dynamic addressing allows a device to have a different IP Address each time it connects to the network. In some systems, the device's IP Address can change even while it is still connected.

Dynamic addressing makes network administration easier because the software tracks issued IP Addresses rather than requiring an administrator to perform this task.

Disabled Radio Button

The **Disabled** radio button disables DHCP support. This must be selected so the static IP address, and subnet mask entered above are in effect.

Acquire System IP Only Radio Button

Select this button to cause the CPU to automatically receive its IP Address from a DHCP Server. The CPU will accept a DHCP address from any DHCP server, unless a specific DHCP server IP address is set below. Any static IP address shown above is ignored.

Acquire IP and Download System Software Only Radio Button

Select this button to cause the CPU to automatically receive its IP Address from a DHCP Server as stated above.

In addition, the CPU will attempt to download system software from the DHCP Server. The DHCP server must also be a TFTP Server, and the file to download is set on the DHCP/TFTP Server. The CPU does not store the software permanently in its memory, it is only stored until a rest.

Acquire IP, Download System Software and Save It Radio Button

Select this button to cause the CPU to automatically receive its IP Address from a DHCP Server as stated earlier.

In addition, the CPU will attempt to download system software from the DHCP Server. The DHCP server must also be a TFTP Server, and the file to download is set on the DHCP/TFTP Server. The CPU stores the software permanently in its memory, overwriting any previous version.

DHCP Server IP Address

Type in the DHCP Server IP Address, if you want the CPU to only select a specific DHCP Server. If that server is not available, no IP Address will be assigned.

SNMP Parameters

The SYSTEM CONFIGURATION -SNMP PARAMETERS PAGE contains fields that specify the SNMP management and notification parameters. The local agent can allow up to five SNMP Managers to read from and/or write to the CPU. The CPU may also send traps or messages to those SNMP Managers.

The following items are found on these pages:

- Read Community field
- Write Community field
- Authentication Trap Enabled Check Box
- SNMP Managing Hosts Edit button

Read Community

The **Read Community** field contains up to 31 characters. You can use numbers and letters to create a string. Remote managers use this string as a password to enable read rights for objects on the CPU.

Write Community

The **Write Community** field contains up to 31 characters. You can use numbers and letters to create a string. Remote managers use this string as a password to enable the ability to make changes on system objects on the CPU.

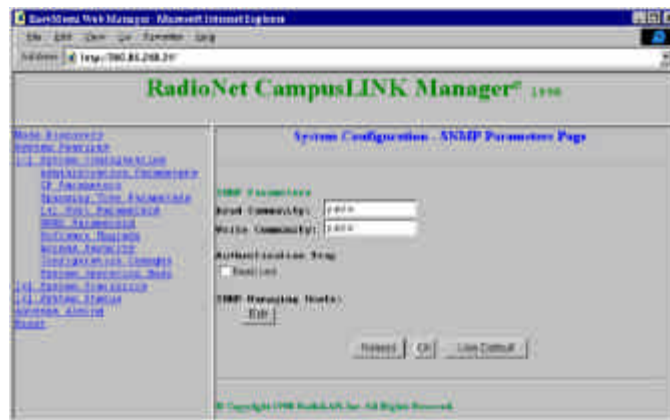


Figure 23: SNMP Parameters Page

Authentication Trap Enabled

The **Authentication Trap Enabled** parameter sends a message to the Read Community when an unauthorized remote manager attempts to access the local agent, someone tries to logon to the CPU, and inputs the wrong user name password combination 3 times.. There are two selections:

Checked enables Authentication Trap messages.

Unchecked disables Authentication Trap messages.

Edit Button displays the SYSTEM CONFIGURATION-CONFIGURE SNMP Host page. Use the page to set up managing hosts IP addresses and rights.

Configuring SNMP Managers for the CPU

The screen offers five **Host Address** fields, allowing you to designate the IP Addresses for up to five SNMP Manager Stations. See IP Address on page 47 for information on the format of an **IP Address**.



Figure 24: Configure SNMP Host Page

Setting Access Rights for SNMP Managers

The **Access Right** column contains radio buttons that allow you to select the following options:

Get Allows the SNMP Manager Station at the selected IP Address to retrieve information from the CPU. When this is selected, the CPU will not allow the Manager to make changes.

Get/Set Allows the SNMP Manager Station at the selected IP Address to retrieve information from, and make changes to the CPU's configuration.

Directing Traps to Manager Stations

The **Receive Trap** column contains radio buttons that allow you to select the following options:

Yes Instructs the CPU to send Trap messages to the selected Manager Station. This must be set for Authentication Traps to be sent.

No Prohibits the selected Manager Station from receiving Trap messages from the CPU.

Directing the System Log to Manager Stations

Yes No effect.

No No effect.

This feature is not yet implemented.

After pressing OK to save the information, press OK on the next screen also.

Setting the CPU's Mode of Operation

The SYSTEM CONFIGURATION – SYSTEM OPERATION MODE PAGE allows you to set up the method that you will use for operating the CPU. This screen displays software options that are currently enabled, and allows you to select one. By default, the screen allows you to use only one option:

- Point-to-Point Mode

Point-to-Point Mode

Point-to-Point Mode sets the CPU into a mode of operation suitable for Campus BridgeLINK-II applications.



Figure 25: System Operation Mode Page

System Features

The System Features page allows you to enable new features Such as SecureLINK Data Encryption. SecureLINK offers both 40-bit and 128-bit encryption capability to Campus BridgeLINK-II users. You must contact RMG to obtain these new features. RMG will provide you with an enabling key based on the Serial Number of your device. After the key is accepted a new configuration screen may appear to support your new feature.

This page contains the Software Upgrade Key field to enter the enabling key. Some of the features are displayed on this page. Other features appear on the System Operation Mode page.

After entering the key, press OK. If the key is correct, the new feature will be available. If the key is not correct, there will be no change to this or any screen.

Please see the SecureLINK users manual for more information on installing, configuring, and operating SecureLINK.

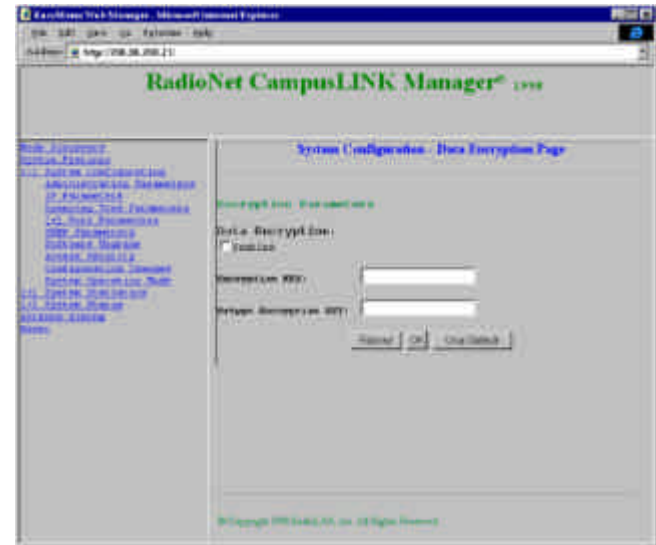


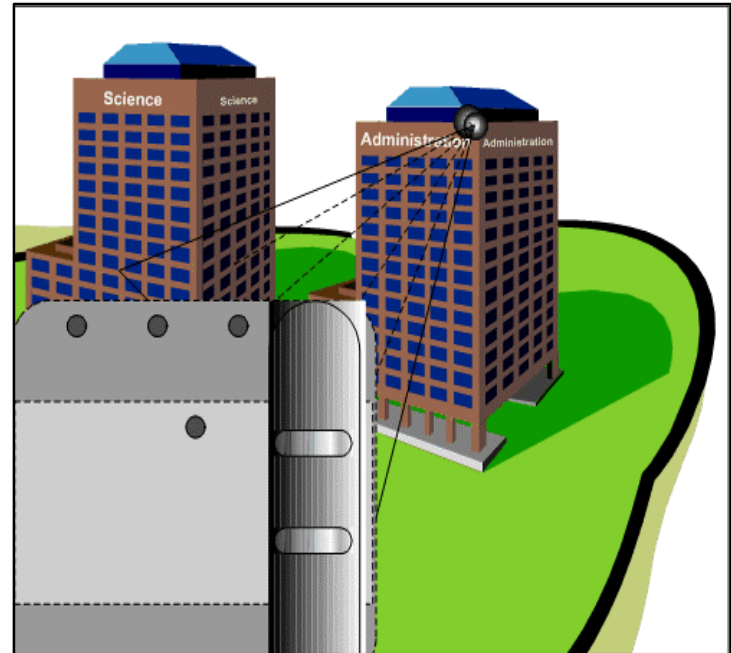
Figure 26: Data Encryption Page

Bridging the Link and 10BaseT Networks

Because the CPU is a bridging device that connects a 10BaseT Network to a wireless link, the CPU must learn about the network. The CPU dynamically learns MAC Addresses of distant network nodes.

The CPU learns the MAC Addresses of a large number of stations on the 10BaseT side of the network, and only passes data packets on to the wireless link that are not addressed to these nodes. When a data packet is addressed to a node on the 10BaseT side of the network, it is not forwarded to the distant CBL.

This method of filtering keeps the wireless link free from unnecessary messages, so that the wireless link provides the maximum performance and speed possible.



There are two configuration pages on the CPU that allow you to further limit packets to improve performance:

- 10BaseT Port MAC filter page
- Radio Port MAC filter page

These are explained on the following page.

To reach the filter pages, you must first access the port parameters pages. To access these pages expand the port parameters sub menu.

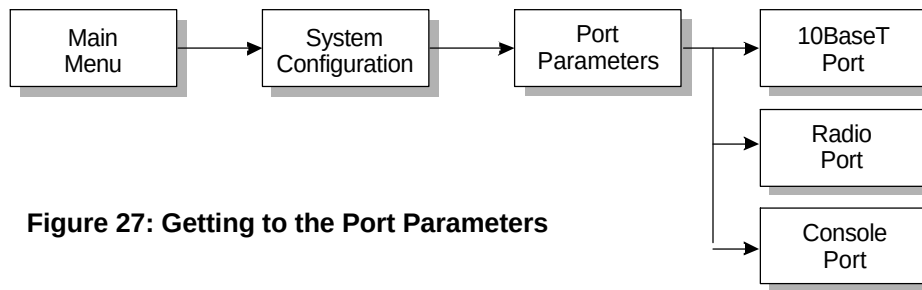


Figure 27: Getting to the Port Parameters

10BaseT Port Parameters

The 10BASET PORT PARAMETERS PAGE displays and allows you to change the 10BaseT port's name, allows you to enable or disable the port and network filters, and allows you to enter the MAC Address filter page. This page contains the following selections:

- Port Name
- MAC Address Filter
- Block IP Packets
- Block IPX Packets
- Block NetBEUI Packets
- Block NetBIOS Packets

Besides the standard buttons, there are two additional buttons at the bottom of this page:

Enable All Places a check mark in all check boxes.

Disable All Removes the check mark from all check boxes.

Port Name..... This allows you to change the Port Name to a descriptive name. The default value is the MAC Address.



Figure 28: Port Parameters

MAC Address Filter

The MAC Address Filter check box allows you to enable or disable MAC Address Filtering on the BackboneLINK. The MAC Address Filter is a database of MAC Addresses you set. Once information is stored in the database, you can allow or disallow packet flow to or from remote addresses in the database.

Unchecked Clearing a check mark from the check box disables MAC Address filtering. This allows any data to pass through the 10BaseT port.

Checked Placing a check mark in the check box enables MAC Address Filtering. This allows data to pass through according to the MAC filter table.

Edit Button

The **Edit** button displays the MAC Address Filter database. You can allow or disallow the receipt or transmission of data packets by MAC Address.

Block IP Packets

The **Block IP Packets** check box allows you to enable or disable the sending of Internet Protocol (IP) packets.

Unchecked Clearing a check mark from the check box enables IP packet forwarding.

Checked Placing a check mark in the check box blocks IP packet forwarding.

Block IPX Packets

The **Block IPX Packets** check box allows you to enable or disable communication of IPX packets.

Unchecked..... Clearing a check mark from the check box enables IPX packet forwarding.

Checked Placing a check mark in the check box blocks IPX packet forwarding.

Block NetBEUI Packets

NetBEUI is a protocol that may be used on Windows or LAN Manager networks.

Unchecked..... Clearing a check mark from the check box enables NetBEUI packet forwarding.

Checked Placing a check mark in the check box blocks NetBEUI packet forwarding.

Block NetBIOS Packets

NetBIOS allows you to connect to networks that use the Network Basic Input Output System. Windows File sharing may use NetBIOS.

Unchecked..... Clearing a check mark from the check box enables NetBIOS packet forwarding.

Checked Placing a check mark in the check box blocks NetBIOS packet forwarding.

Radio Port Parameters

The Radio Port (Wireless Link) Parameters page displays and allows you to change the Radio port's name and Subnet ID. It also allows you to enable or disable the port and network filters, and allows you to enter the MAC Address filter. This page contains the following selections:

- Port Name
- Subnet ID
- MAC Address Filter
- Block IP Packets
- Block IPX Packets
- Block NetBEUI Packets
- Block NetBIOS Packets

Besides the standard buttons, there are two additional buttons at the bottom of this page:

Enable All Places a check mark in all check boxes.

Disable All Removes the check mark from all check boxes.



Figure 29: Radio Port Parameters

Port Name

The **Port Name** field allows you to enter up to 12 characters that identify the name of the CPU. This appears as the CPU's name on the ANTENNA AIMING page (see *Selecting the Distant Campus BridgeLINK-II's Address* on page 39 for more information).

Subnet ID

The **Subnet ID** field allows you to enter the wireless network name. Both CPUs must use the same Subnet ID designation to communicate. You can use up to four characters for this entry.

Filters

For an explanation of the following parameters, see 10BaseT Port Parameters on page 59. These parameters are the same, but apply to the Radio Port.

MAC Address Filter

Edit Button

Block IP Packets

Block IPX Packets

Block NetBEUI Packets

Block NetBIOS Packets

Setting the Baud Rate for the Console (Local) Port

The Console Parameters page allows you to set the baud rate to connect and manage the CPU with a local terminal. Set the baud rate so it is the same as the terminal. Select from the following available baud rates:

- 9600 baud
- 19200 baud
- 38400 baud
- 57600 baud

Set the VT100 terminal software for the following:

- Baud Rate (selected here)
- 8 data bits
- No parity
- 1 stop bit
- No flow control

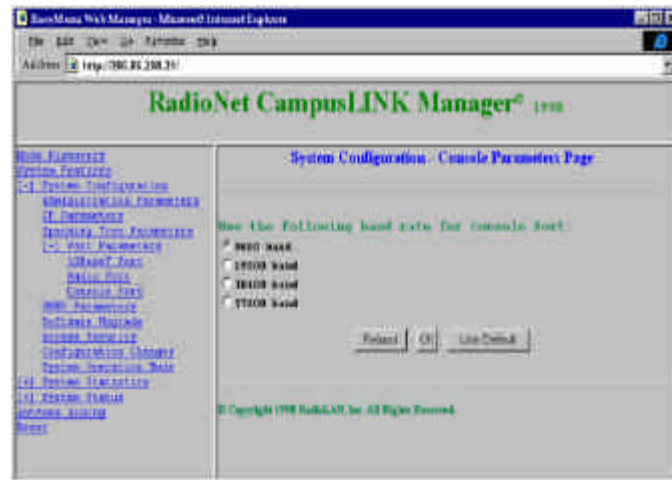


Figure 30: Console Parameters Page

Managing Packet Flow Through the CPU

The CPU can selectively allow or disallow traffic to or from the 10BaseT Network and the wireless link. Proper packet flow management improves the speed of the wireless link by eliminating unwanted network traffic.

The CPU is set for optimum performance by default. Only advanced users with special circumstances should use the entries on MAC Filter screens.

The CPU contains and manages two identical filtering databases:

- 10BaseT Port MAC Filter List
- Radio Port MAC Filter List

Each of these databases is configured in the same way. Each List allows you to add up to 32 MAC Addresses or wildcards and to allow or disallow the receipt or transmission of data packets to specified MAC Addresses.

Item	MAC Address	Mask Bytes	Source/Dest	Accept/Reject
1	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
2	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
3	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
4	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
5	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
6	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
7	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
8	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
9	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
10	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
11	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E
12	00:00:00:00:00:00	00:00:00:00:00:00	F3:CD	F.A.C.E

Figure 31: MAC Address Table

The databases contain the following columns:

- Item
- MAC Address
- Mask Bytes
- Source/Dest.
- Accept/Reject

Item

The **Item** column shows the order in which the CPU stored the database entry.

MAC Address

The **MAC Address** column displays the MAC Address (in six, two-character octets) for the remote network node. Enter the MAC Address of the device that you want to enter into the database.

Although you can use **00** as a specific value for an octet, you can also use **00** when creating a “wildcard” octet. Using wildcards allows you to specify a range of addresses, as opposed to just a single address.

For example, the first three octets of the MAC Address for all RadioLAN products is **00 A0 D4**. If you want to allow all RadioLAN products access to the CPU, set the **MAC Address** field to **00 A0 D4 00 00 00**, and the **Mask Bytes** field to **ff ff ff 00 00 00**. The wildcard is a result of a relationship between the MAC Address and the **Mask Bytes** field.

Mask Bytes

As an alternative to placing wildcards (00) in the **MAC Address** field, the **Mask Bytes** column allows you to select which octets in the **MAC Address** field will be read by the CPU (see Figure 33).

Entering **ff** into a mask bytes octet instructs the CPU to allow only MAC octets with a value matching the same location in the **MAC Address** field to pass. The CPU rejects any other entry in the octet position.

Entering a **00** into a mask bytes octet instructs the CPU to “mask” the octet. When the octet is masked, the CPU allows any entry to pass.

Entering an **ff** into a mask bytes octet, and a **00** in the same octet position of the MAC Address instructs the CPU to allow an entry matching only **00** to pass.

	Assigned to a Manufacturer			Assigned by a Manufacturer		
Byte Position:	1	2	3	4	5	6
MAC Address:	00	A0	D4	00	00	00
Mask Bytes:	ff	ff	ff	00	00	00
ff = the byte in this position must match 00 = allow any digit in this section						

Figure 32: Working with Mask Bytes

Source/Dest.

The **Source/Dest.** column allows you to specify whether the action upon packets will occur if that node is sending or receiving packets.

Accept/Reject

The **Accept/Reject** column permits you to allow or disallow transmission of the packet, depending on the entry in the **Source/Dest** column. For example, if **Source** is enabled in the **Source/Dest** column, and the **Reject** radio button is enabled in the **Accept/Reject** column, the CPU will not allow a message sent from that MAC Address to pass through. If **Destination** is enabled in **Source/Dest**, and the **Reject** radio button is enabled in the **Accept** column, the CPU will not allow the message intended for that MAC Address to pass through.

Alternatively, if **Source** is enabled in the **Source/Dest** column, and the **Accept** radio button is enabled in the **Accept/Reject** column, the CPU allows the message sent from that MAC Address to pass through. If **Destination** is enabled in the **Source/Dest** column, and the **Accept** radio button is enabled in the **Accept/Reject** column, the CPU allows the message intended for that MAC Address to pass through.

Adding MAC Filters

To add up to 32 MAC filters, select the first available **Item**:

1. Fill in the **MAC Address** and subnet **Mask Bytes** fields.
2. In the **Source/Dest** column, select whether the filter will be invoked when the address is sending a packet or when it is receiving a packet:

Choose **Source** if you want to filter messages that are sent from the MAC Address.

Choose **Destination** if you want to filter messages that are sent from other nodes and intended for receipt by the MAC Address.

3. In the **Accept/Reject** column, you can allow or disallow the passage of the packet through the CPU based upon the broadcast type (source or destination) in the **Source/Dest.** column:

Choose **Accept** to allow the passage of packets to/from the MAC Address.

Choose **Reject** to disallow the passage of packets to/from the MAC Address.

After adding all desired MAC Addresses, click the **OK** button to return to the previous screen, and be sure to select **OK** on that page also. If you wish to cancel your changes, click on **Cancel** to return to the previous screen.

Modifying MAC Filters

To modify a MAC filter, select the desired MAC Address. Make changes to the address fields and selections in the **Source/Dest.** and **Accept/Reject** columns.

After modifying all desired MAC Addresses, click the **OK** button to return to the previous screen, and be sure to select **OK** on that page also. If you wish to cancel your changes, click on **Cancel** to return to the previous screen.

Deleting MAC Filters

To delete a MAC filter, select the address of the undesired MAC Address and mask bytes and type **00.00.00.00.00.00** in both fields.

After deleting all desired MAC Addresses, click the **OK** button to return to the previous screen, and be sure to select **OK** on that page also. If you wish to cancel your changes, click on **Cancel** to return to the previous screen.

Spanning Tree Parameters

When you connect two or more networks to increase the number of users, or enhance the ability for users of two (or more) networks to communicate with one another, you can control the routing of data to maximize the efficiency of the traffic between the networks.

Bridging characteristics allow you to route necessary messages between two networks and to eliminate unnecessary traffic to other networks when messages are only intended for use within the local network.

Furthermore, you can set up redundant paths for bridging, which reduces the potential for data path losses due to bridging network outages. You can establish a path redundancy for bridging networks and redundancy for ports on the same bridging network.

Path redundancy creates a loop by means of which data packets can potentially travel indefinitely if the bridge root network were unable to dynamically “prune” pathways between each network. The spanning tree protocol, which is always on for a CPU, interacts with other bridge devices to eliminate loops in the network. The **SPANNING TREE PARAMETERS** PAGE allows you to set configuration items that allow the establishment of the root, redundancy of root networks, redundancy of root network ports to other networks, and dynamic pruning between network loops.

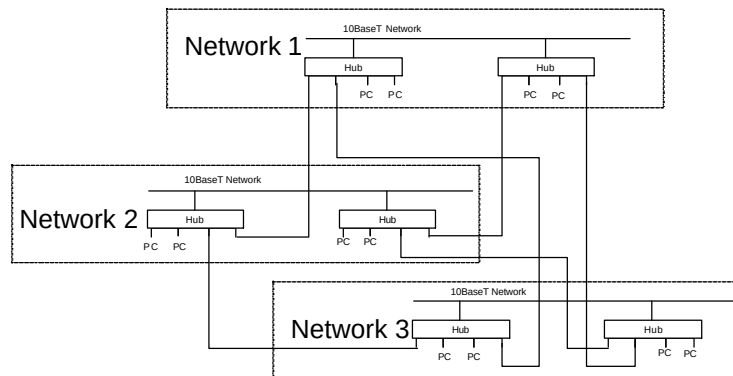


Figure 33: Bridging Networks

The SYSTEM CONFIGURATION - SPANNING TREE PARAMETERS PAGE allows you to set up bridging characteristics for the CPU that conform to Spanning Tree 802.1D protocol. The page displays the following items:

- Bridge Priority (0–65535)
- Hello Time (1–10)
- Forward Delay Time (4–30)
- Max. Age Time (6–40)
- Port Priority (0–255)
- Port Path Cost (1–65535)

Each bridge has a unique bridge identifier. **Priority** is a part of that identifier; it determines the topology. Smaller priority entries increase the probability of the CPU being selected as the root or primary bridge between other networks.

Hello Time (1–10)

When no root bridge is present, the CPU sends a message that notifies other bridges of its request to be the root bridge. If no other bridge responds to this “Hello” message, the CPU establishes itself as the root bridge between its connected networks.



Figure 34: Spanning Tree Parameters Page

When a bridge is established as being the root bridge, it sends the “Hello” message at the interval, in seconds, that you select in the **Hello Time** field.

Forward Delay Time (4–30)

Only the active root bridge uses this value. Any bridge not acting as the root bridge uses a dynamic value for **Forward Delay** set by the root bridge.

Enter the number of seconds that the bridge will wait to listen and learn the network before forwarding packets. It also waits this amount of time after a topology change (a bridge is added or removed).

Max. Age Time (6–40)

The CPU maintains a routing database, containing unique source addresses of frames that it receives from the 10BaseT network to which it is connected. The CPU compares each new frame's source address to entries within its internal routing database. If the CPU does not find a new frame's source address in the routing database, it adds the new frame's source address to the database.

The **Max. Age Time** field sets the amount of time in seconds that the CPU stores any source address. When the CPU stores a frame's source address, the address remains in the routing database for the length of time specified in **Max. Age Time**. If the CPU receives a frame, and finds the frame's source address in the database, it automatically resets the aging timer for that entry. If the aging timer for an entry in the database expires before the CPU receives another frame with the same source address, it removes the source address from its internal routing database. This prevents the database from storing information about inactive network stations.

Port Priority (0–255)

Bridges associate ports with physical devices, such as a 10BaseT port. Each port is associated with a port priority, which contributes to determining which ports forward packets on the network. The lower the number in this field, the higher the chance for this CPU to become the designated bridge.

Port Path Cost (1–65,535)

Each port is associated with a port cost, which contributes to determining which ports forward packets on the network. The lower the number in this field, the higher the chance for this CPU to become the designated bridge.

Interrogating the CBL for Performance Information

Performance is a combination of speed and accuracy. When the CPU transmits at higher rates, and retransmits packets fewer times, it has a higher rate of performance. Most users discover performance issues when sending large files from one CBL to the other.

Although multiple users can send information across the link at the same time, lower shared network resources can cause slower file transfer time. While data packets are being transferred, available link resources shared by all users decrease, so when the CPU finishes the job faster, increased shared link resources are made available for other packet transfers, making file transfer faster.

It is important to query the CPU for performance information occasionally. This allows you to determine when performance issues arise over time and indicates where you can make changes to improve performance.

One change might require the adjustment of a directional antenna to improve signal strength. Another adjustment might be filtering unnecessary packets to disallow passage into the wireless link. This type of fine-tuning is intuitive and one can determine actions, based upon statistics found in the following pages.

Checking 10BaseT Port Statistics

The SYSTEM STATISTICS - 10BASET PORT STATISTICS PAGE reports the CPU's ability to communicate with 10BaseT Network stations. The information on this page is automatically updated every ten seconds. This section describes the 10BASET PORT STATISTICS PAGE.



Total Packets Transmitted

Total Packets Transmitted counts and stores the total number of packets that the CPU sends to 10BaseT stations on the network. This number represents all transmitted packets.

Total Packets Received

Total Packets Received counts and stores the total number of packets that the remote 10BaseT stations send to the CPU. This number represents all received packets.

Total Error Packets

This field displays the total number of Ethernet errors accumulated.

CRC Error Packets

This field displays the total number of frames that reported a bad cyclical redundancy check.

Collision Error Packets

This field displays the number of packets that failed due to a collision—two stations attempting to access a media at the same time.

Overrun Packets

This field totals the number of frames that exceeded Ethernet maximum size specifications.

Figure 35: 10BaseT Port Statistics Page

Runt Packets

This field totals the number of frames that were smaller than Ethernet minimum size specifications.

This page also contains a **Clear Counters** button. Clicking this button resets all counters on this page to zero.

Checking Radio Port (Wireless Link) Statistics

The SYSTEM STATISTICS - RADIO PORT STATISTICS PAGE reports the Campus BridgeLINK's ability to communicate with the distant Campus BridgeLINK. The information on this page is automatically updated every ten seconds. This section describes the RADIO PORT STATISTICS PAGE.

The page has two major sections:

- Packet Transmission
- Packet Reception

The screen also contains a **Clear Counters** button. Clicking this button resets all counters on this page to zero.



Figure 36: Radio Port Statistics Page

Packet Transmission

The **Packet Transmission** section stores information about packets that are sent from the CBL to the distant CBL.

Total Packets Transmitted

The **Total Packets Transmitted** field counts and stores the total number of packets that the CPU sends to the distant CBL across the wireless link. This number represents all transmitted packets.

Average Transmit Rate (Packets/Sec.)

Sometimes packets are transmitted more rapidly than at other times. The **Average Transmit Rate** field indicates the average number of packets sent each second. Typical networks range from 100 to 5000 frames transmitted each second, and will vary with time. If you observe the rate consistently higher than 10,000 fps, you may have broadcast storms on your 10BaseT Network segment. These broadcast storms can be caused, for example, by a defective Network Interface Card.

Total Retransmission

When the distant Campus BridgeLINK does not acknowledge the receipt of a packet sent by the local CBL, the local CPU resends the packet a number of times until the distant CBL acknowledges receipt of the packet or a time out occurs. The **Total Retransmission** field counts and stores the number of retransmissions, based upon the total number of packets transmitted.

A number higher than total transmissions in this field may indicate the need to correct the alignment of a CBL's directional antenna. You may also need to remove objects that block the line-of-site of the two directional antennas to improve signal quality.

Packet Reception

The **Packet Reception** section indicates the CPU's ability to receive packets from the distant CBL.

Total Packets Received

The **Total Packets Received** field counts and stores the total number of packets that the remote CPU sends to the local CPU. This number represents all received packets.

Average Receive Rate (Packets/Sec.)

Sometimes packets are received more rapidly than at other times. The **Average Receive Rate** field indicates the numbers of average packets received each second. You should see approximately 100 – 5000 fps under normal conditions. . If you observe the rate consistently higher than 10,000 fps, you may have broadcast storms on your distant network.

Upgrading System Software

The CPU contains a running operating system, and a file containing configuration items. The SYSTEM CONFIGURATION – SOFTWARE UPGRADE PAGE allows you to download new operating system software to the CPU. On this page you can upgrade from a file or from a TFTP server.

When you perform an upgrade, the downloaded file replaces the current operating system. You can upgrade system software three ways:

- Using a local file on your PC (see Figure 41).
- Using a TFTP server (see Figure 42 on page 80).
- Using XMODEM through the CPU local port.

Upgrade from File

Selecting this button allows you to pick a file on your local PC. When selected, the **File to Upload** field appears, allowing you to enter the name of the file you wish to upload.

File to Upload

This field allows you to enter the file name of the operating system file that you want to

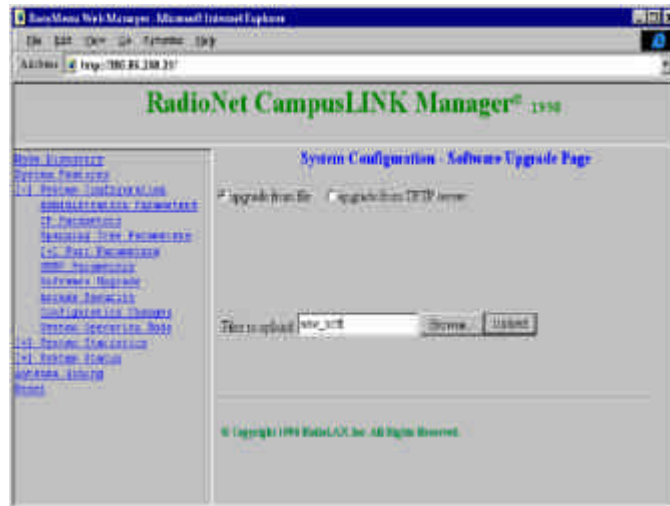


Figure 37: Software Upgrade (from file) Page

download. If you do not know where the file is located, click the **Browse** button to display a directory hierarchy. After selecting the file press **Upload**.

Upgrade from TFTP Server

Selecting this radio button displays some new fields allowing you to enter the IP Address where the update file is stored and the system software file name.

System Software File Name

The **System Software File Name** field allows you to enter the name of the file to download.

Set TFTP Server IP Address

This field allows you to enter the IP Address of the TFTP server.

Download Button

Download causes the CPU to retrieve the specified software file from the specified location. The downloaded file is written into system memory after the CPU receives it. After downloading and doing a reset, the new operating system loads.



Figure 38: Software Upgrade (from TFTP) page

Saving or Rejecting Configuration Setting Changes

The Configuration Changes menu item displays the SYSTEM CONFIGURATION – CONFIGURATION CHANGES PAGE. This page allows you to save your changes, reject changes you have made, or reset the configuration to default parameters.

This page contains the following objects:

- **Save All Changes and Reset** radio button
- **Reload Last Saved Configuration** radio button
- **Reset Configuration To Factory Default** radio button

After making your choice, click the **OK** button to cause the CPU to act.

Save All Changes and Reset

This radio button causes all changes that you have made during this session to overwrite existing program Reload Last Saved Configuration

Reload Last saved Configuration



Figure 39: Configuration Changes Page

This radio button causes all changes that you have made to revert back to their original settings.

Reset Configuration to Factory Default

This radio button causes the CPU to change all configuration items to their factory default settings. You must go back and save all changes and reset to make this permanent.

Resetting the CPU

Any time you download a new version of the CPU's operating system, you must reset the CPU. One method of resetting the CPU is to remove power from the unit for approximately five seconds. Another method for resetting the CPU is found on the RESET PAGE.

To access the RESET PAGE, select the **Reset** menu item. All configurations changes will be lost, unless you save all changes and reset as explained in the previous section.

Click the **OK** button to reset the CPU.

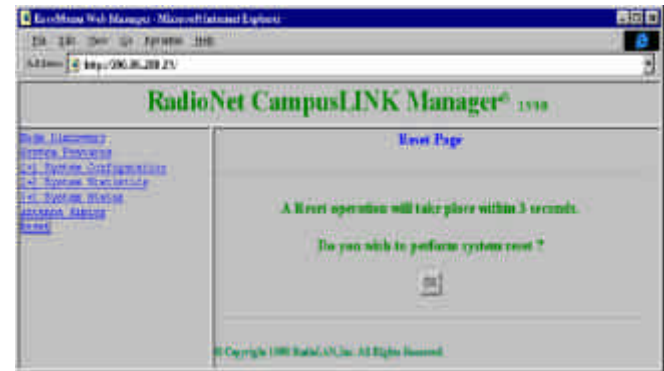


Figure 40: Reset Page

Recording Important System Information

Having system information on hand is essential to proper system management. The Campus BridgeLINK-II™ Manager makes it easy to keep information on hand, recording configuration information that was last saved (see *Saving or Rejecting Configuration Setting Changes* on page 81). To retrieve system information, open the SYSTEM STATUS - SYSTEM INFORMATION PAGE, then print it on your local printer. File the resulting printout in a safe place.



The screenshot shows a web browser window titled "EasyMenu Web Manager - Microsoft Internet Explorer". The address bar shows "http://206.00.254.21/". The main content area displays the "RadioNet CampusLINK Manager® 1998" logo at the top. On the left is a navigation menu with links: Home, Features, System Configuration, System Information, System Status, System Log, Add/Remove Linking, and Reset. The "System Status - System Information Page" is selected. The main content area contains a table with system information.

System Status - System Information Page	
Product Name	CampusLINK
System Name	Western Bridge
System Contact	Administrator
System Location	RadioLAN
Radio Port Mac Address	00:00:00:00:00:00
Ethernet Port Mac Address	00:00:00:00:00:00
Subnet ID	1234
IP Address	206.00.254.21
Subnet Mask	255.255.255.0
Default Gateway IP Address	206.00.254.1
Host Software Version	01.00
System Software Version	2.01 (Jan 22 1998 17:52:18)
System Software File Name	wsa201
Hardware Revision	AA
System Serial Number	00A0D43603B5
System Up Time (HH:MM:SS)	0 3:54:28

© Copyright 1998 RadioLAN, Inc. All Rights Reserved.

Figure 41: System Information Page

The SYSTEM INFORMATION PAGE includes the following information:

Product Name	States the product name.
System Name	States the system name entered on the ADMINISTRATION PARAMETERS PAGE.
System Contact	States the system contact entered on the ADMINISTRATION PARAMETERS PAGE.
System Location	States the system location entered on the ADMINISTRATION PARAMETERS PAGE.
Radio Port MAC Address	This information is loaded into the CPU from the factory. The information in this field should match the MAC Address noted on the bottom of the CPU.
10BaseT Port MAC Address	This information is loaded into the CPU from the factory. The information in this field should match the MAC Address noted on the bottom of the CPU.
Subnet ID	This information was entered on the RADIO PORT PARAMETERS PAGE.
IP Address	States the IP Address entered on the IP PARAMETERS PAGE, or DHCP assigned IP Address if DHCP support is enabled.
Subnet Mask	States the subnet mask entered on the IP PARAMETERS PAGE.
Default Gateway IP Address	States the default gateway entered on the IP PARAMETERS PAGE.
Boot Software Version	States the boot software version stored in the CPU.
System Software Version	States the system software version that the CPU is currently using.

System Software File Name	States the system software file name.
Hardware Revision	States the hardware version of the CPU.
System Serial Number	States the CPU's serial number.
System Up Time	States the day, hours, minutes and seconds that the system has been in operation.

Viewing the System Log

The SYSTEM LOG PAGE collects system events like system starts, restarts, and password authentication messages. The screen displays a list with the following columns:

Item Displays the item number on the list. As new events appear, the CPU issues a new number.

Task Lists the task that initiated the message.

Time (sec.) This column lists the number of seconds since boot that the event occurred.

Error Message Lists a verbose error name.

The screen only displays 16 items of the 64 item System Log at a time. Old items are overwritten if the log extends past 64 items. The screen also contains three buttons:

Previous Page Load the previous page of the log.

Reload Reload the current page.

Next Page Load the next page.



Figure 42: System Log Page

Managing the CPU Locally

You can connect a serial device such as a VT-100 terminal, a PC using terminal software, or dial-up modem to the CPU as an alternative method of managing the CPU.

Using this method, you can communicate with the CPU to make configuration changes or to interrogate the CPU for performance statistics.

The Campus BridgeLINK-II uses a standard DB-9 serial cable, Female to Male, all pins connected straight through.

Popular PC terminal Emulation software, such as HyperTerm, or the very reliable TeraTerm, are ideal tools for configuring the BackboneLINK-II. Hyperterm comes bundled with Windows, and Tera Term is a freeware Terminal Emulator which can be found at www.download.com.

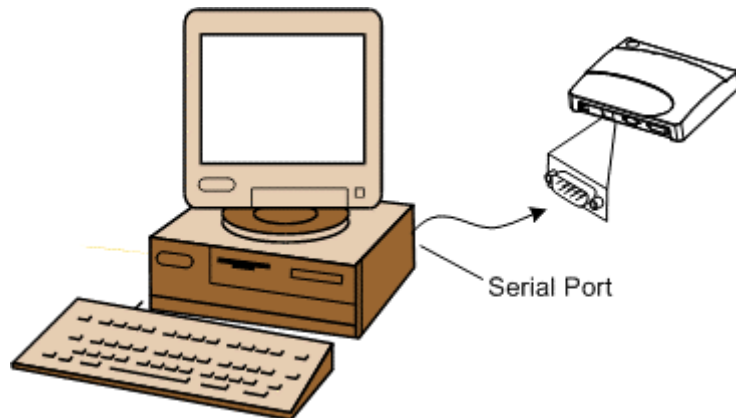


Figure 43: Connecting the VT-100 Terminal or Emulator to the CPU-II

CPU Local Management

The CPU Local Management menu allows you to view screens that contain configuration information about the CPU. Using this menu, you can assign passwords, set up IP Addresses for the CPU and SNMP Managers, set address filters, test system performance, and view system performance statistics.

When using the CPU Local Management software to make changes, edit your choices on the screens, then accept all session changes by accessing the SYSTEM CONFIGURATION - CONFIGURATION CHANGES PAGE. This causes the CPU to store configuration changes.

Hot Keys

Throughout the program you will find **hot keys**. These specific keyboard combinations allow you to move about the program easily and quickly. Each screen contains a specific grouping of hot keys. Options available through the program are:

- | | |
|-----------------------|---|
| Enter | Make a selection from available options by highlighting the item you want and pressing the <ENTER> key. You should also use this key to enter your response. |
| Backspace | The <BACKSPACE> key on your keyboard allows you to move to the screen displayed previously. |
| UP/DOWN Arrows | Use the arrow keys to select a menu item. |

Logging onto the CPU Configuration Screen

The LOGON SCREEN provides security to CPU configuration items. There are three fields on the screen:

- Serial Number
- Enter User Name
- Enter Password

If the password is not set, the following message will appear at the bottom of the screen:

Password is not set, hit any key to proceed)

If this message appears, press any key to enter the program, then set the access security features by going immediately to the SYSTEM CONFIGURATION - ACCESS SECURITY PAGE.



Figure 44: Logon Menu

Serial Number

The **Serial Number** field is a read-only field that reports the CPU's serial number.

Enter User Name

The **Enter User Name** field is an entry field into which you enter your user name to gain access to the configuration and diagnostic screens. Only entries matching those programmed into the SYSTEM CONFIGURATION - ACCESS SECURITY PAGE are allowed access to the program. Press **<ENTER>** after keying in the User Name.

Enter Password

The **Enter Password** field allows you to enter your user password for access to configuration and diagnostic screens. Enter your password here and then press **<ENTER>** to start the program.

If the user name and password match those stored in the ACCESS SECURITY PAGE, you will be allowed to view and edit items on the screen. If you make entries that do not match those stored in the program, you will remain on the LOGON SCREEN.

Using the Main Menu

After gaining access from the LOGON SCREEN, the main menu appears. This menu lists all major sections of the program.

Node Discovery	Displays the signal quality of the wireless link.
System Features	Takes you to the SYSTEM FEATURES menu, where you can select the CPU unit's mode of operation and Data Encryption. See <i>SYSTEM OPERATION MODE</i> on page 108 for more information about this selection.
System Configuration	Leads you to configuration items, such as access security, SNMP parameters, and port parameters. See <i>Working with the System Configuration Menu</i> on page 93 for more information about this selection.
System Statistics	Allows you to see the historical performance of the CPU. See <i>SYSTEM STATISTICS MENU</i> on page 108 for more information about this selection.

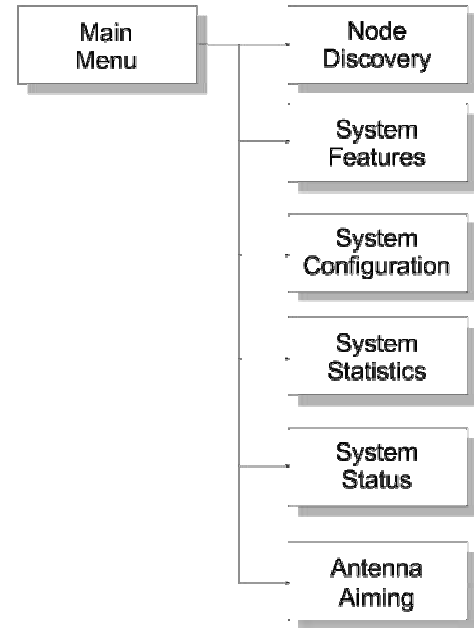


Figure 45: The Main

System Status

Allows you to interrogate the CPU for current system performance information. See *SYSTEM STATUS MENU* on page 109 for more information about this selection.

Antenna Aiming

Allows you to fine-tune the alignment between directional antennas. See *DIAGNOSTICS-ANTENNA AIMING MENU* on page 109 for more information about this selection.

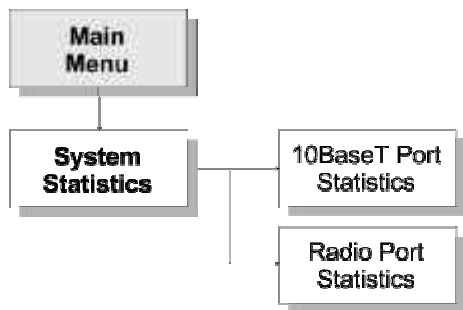


Figure 46: Systems

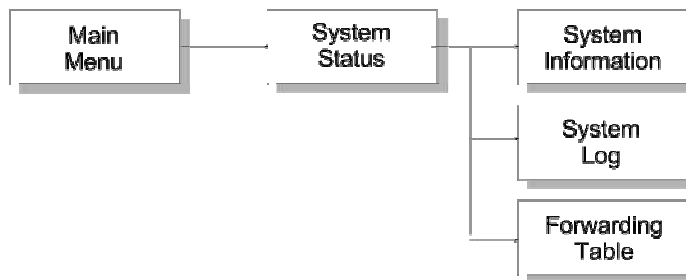


Figure 47: System Status Menus

Working with the System Configuration Menu

After selecting **System Configuration** on the main menu, the System Configuration menu appears, allowing you to set up a number of CPU network functions. The menu contains the following items.

Administration Parameters

This selection leads you to the **ADMINISTRATION PARAMETERS** menu, from which you can identify the system name, the person who is responsible for the CPU, and the location where the CPU is installed. This information is useful when you access the CPU from remote locations using SNMP and HTML communication. See *ADMINISTRATION PARAMETERS MENU* on page 98 for more information about this selection.

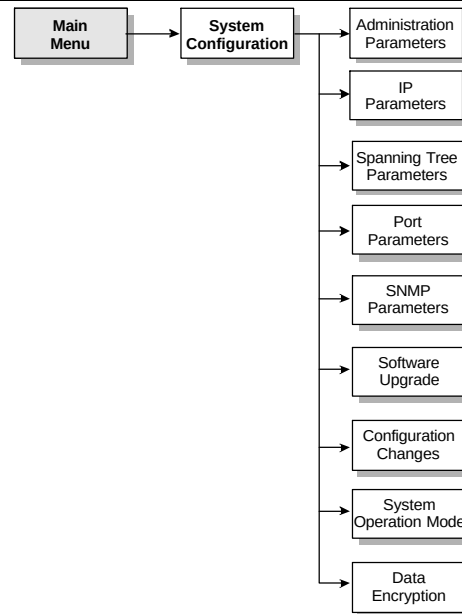


Figure 48: System Configuration Menu

IP Parameters

This item displays the IP PARAMETERS menu, from which you assign the CPU's IP Address for the 10BaseT Network. You can also enable DHCP support here. See *IP PARAMETERS* on page 98 for more information about this selection.

Spanning Tree Parameters

This item displays the BRIDGING PARAMETERS menu, where you can set up options for Spanning Tree Parameters. See *SPANNING TREE PARAMETERS MENU* on page 99 for more information about this selection.

Port Parameters

Selecting this item displays the PORT PARAMETERS menu, from which you can choose to set up 10BaseT or radio port (wireless link) options. See *10BASET (AND RADIO) PORT PARAMETERS MENU* on page 101 for more information about this selection.

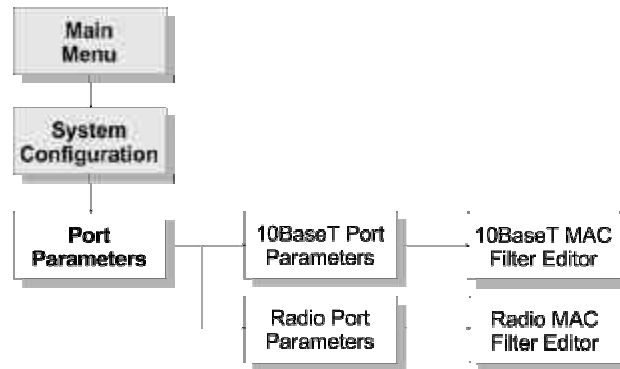


Figure 49: Port Parameters Menus

SNMP Parameters

This item displays the SNMP PARAMETERS menu, where you can set IP Addresses and other items related to SNMP management.

Software Upgrade Parameters

Selecting this item displays the SOFTWARE UPGRADE menu, at which you can specify the IP Address of a TFTP server where you can download software updates and add new features to the CPU. See *SOFTWARE UPGRADE MENU* on page 105 for more information about this selection.

Access Security

This selection leads you to the ADMINISTRATION PARAMETERS menu, from which you can assign logon names and passwords for up to three users. See *SYSTEM CONFIGURATION – ACCESS SECURITY MENU* on page 106 for more information about this selection.

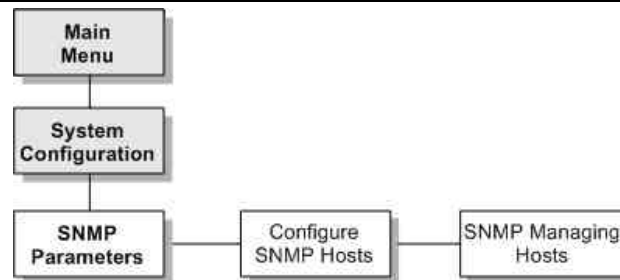


Figure 50: SNMP Parameters Menus

Configuration Changes

After making changes to selections on menus, select this option to display the CONFIGURATION CHANGE menu, from which you can permanently save your changes, or revert back to the last saved settings. See *SYSTEM CONFIGURATION – CONFIGURATION CHANGES MENU* on page 106 for more information about this selection.

System Operation Mode

This selection displays the SYSTEM FEATURES menu, from which you can set the operational characteristics of the CPU. Here, you can configure the CPU as an access point, or a 10BaseT Network interface card translator to wireless networking. See *SYSTEM OPERATION MODE* on page 108 for more information about this selection.

Data Encryption

This selection leads you to the BRIDGING PARAMETERS menu, from which you can enable Data Encryption and set the encryption key. See *page* for more information about this selection.

Configuration Manager Menu Items

The following table lists each menu name and menu item, and gives a brief note for items in the Configuration Manager menus. For a further explanation of an item on the list, see the **Refer to** column, which states the section name and page number where you can find the explanation.

Menu Name	Menu Item	Refer to:	Notes
NODE DISCOVERY MENU		<i>Discovering the Distant CBL on page 41</i>	Provides information about the distant CBL.
SYSTEM FEATURES MENU		<i>System Features on page 55</i>	Allows you to add new features.
	Software Upgrade Key	<i>See page 55</i>	Allows you to enter a key to enable new features.

Menu Name	Menu Item	Refer to:	Notes
ADMINISTRATION PARAMETERS MENU		<i>Administration Parameters</i> on page 46	Allows you to specify system identification information for SNMP management.
	System Name	<i>System Name</i> on page 46	Enter from 1 to 15 letters or numbers.
	System Contact	<i>System Contact</i> on page 46	Enter from 1 to 15 letters or numbers.
	System Location	<i>System Location</i> on page 46	Enter from 1 to 15 letters or numbers.
IP PARAMETERS		<i>IP Parameters</i> on page 47	Allows you to set IP network addresses.
	IP Address	<i>IP Address</i> on page 47	Identifies the CPU on a TCP/IP network.
	Subnet Mask	<i>Subnet Mask</i> on page 48	Determines the IP Network for the CPU. This number together with the IP Address identifies the CPU on the network.

Menu Name	Menu Item	Refer to:	Notes
SPANNING TREE PARAMETERS MENU	Default Gateway IP Address	<i>Default Gateway IP Address</i> on page 48	The IP Address of the device that allows access to outside networks.
	DHCP Operation Mode	DHCP Support on page 48	Enables and disables DHCP support. By default, DHCP is enabled.
	DHCP Server IP Address	DHCP Server IP Address on page 50	The IP Address of the only DHCP server you wish to receive IP Addresses from.
		<i>Spanning Tree Parameters</i> on page 69	Allows you to set up bridging characteristics for the CBL.
	Bridge Priority (0-65535)	<i>Bridge Priority (0-65535)</i> on page 69	Enter a number from 0 to 65,535.
	Hello Time (1-10)	<i>Hello Time (1-10)</i> on page 70	Enter a number from 1 to 10.
	Forward Delay Time (4-30)	<i>Forward Delay Time (4-30)</i> on page 71	Enter a number from 4 to 30.

Menu Name	Menu Item	Refer to:	Notes
SYSTEM CONFIGURATION N - PORT PARAMETERS MENU	Max. Age Time (6–40)	<i>Max. Age Time (6–40) on page 71</i>	Enter a number from 6 to 40.
	Port Priority (0–255)	<i>Port Priority (0–255) on page 72</i>	Enter a number from 0 to 255.
	Port Path Cost (1–65,535)	<i>Port Path Cost (1–65,535) on page 72</i>	Enter a number from 1 to 65,535.
		<i>Bridging the Link and 10BaseT Networks on page 56</i>	This menu leads to port parameters menus for the Radio and 10BaseT ports.
	10BaseT Port Parameters Menu	<i>10BaseT Port Parameters on page 58</i>	Displays the 10BASET PORT PARAMETERS menu.
	Radio Port Parameters Menu	<i>Radio Port Parameters on page 61</i>	Displays the RADIO PORT PARAMETERS menu.
	Console Port Baud Rate	<i>See page 63</i>	Allows you to change the baud rate for the Local Port.

Menu Name	Menu Item	Refer to:	Notes
10BASET (AND RADIO) PORT PARAMETERS MENU		<i>10BaseT Port Parameters</i> on page 58, or <i>Radio Port Parameters</i> on page 61	Displays the port's name, allows you to enable or disable port and protocol filters, and allows you to add, modify, and delete MAC Address filters.
	Port Name	Port Name on page 61	Enter up to 12 letters or numbers.
	Subnet ID	<i>Subnet ID</i> on page 62	Available in RADIO PORT PARAMETERS menu only. Enter four characters.
	Block MAC Packets	See on page 58	Choose Yes or No .
	Edit MAC Filters	Edit Button on page 59	This item leads to the EDIT MAC FILTERS menu.
	Block IP Packets	Block IP Packets on page 59	Choose Yes or No .
	Block IPX Packets	<i>Block IPX Packets</i> on page 60	Choose Yes or No .
	Block NetBEUI Packets	<i>Block NetBEUI Packets</i> on page 60	Choose Yes or No .

Menu Name	Menu Item	Refer to:	Notes
	Block NetBIOS Packets	<i>Block NetBIOS Packets</i> on page 60	Choose Yes or No .
MAC FILTERS MENU			Allows you to add, modify or delete filters.
	Filter Physical Address	<i>MAC Address</i> on page 65	Type the MAC Address to filter.
	Filter Mask Address	<i>Mask Bytes</i> on page 66	Enter the Mask address for choosing wildcards.
	Source or Destination Address Filtering	<i>Source/Dest.</i> on page 66	Allows you to specify whether the action upon packets will occur if that node is sending or receiving packets.
	Accept or Reject The Packet When Satisfied	<i>Accept</i> on page 67	Allows you to allow or disallow transmission of the packet depending upon the entry in the Source/Dest. field.
	List all Filters Configured	<i>Adding MAC Filters</i> on page 67	Selecting this item displays the filter list.

Menu Name	Menu Item	Refer to:	Notes
10BASET (AND RADIO) MAC FILTER LIST		<i>Managing Packet Flow Through the CPU</i> on page 64	Allows you to see the entire Filter List.
SNMP PARAMETERS MENU		<i>SNMP Parameters</i> on page 51	Contains fields that specify the SNMP management and notification parameters.
	Read Community	Read Community on page 51	Enter up to 31 letters or numbers.
	Write Community	Write Community on page 51	Enter up to 31 letters or numbers.
	Enable Authentication Trap	<i>Enable Authentication Trap</i> on page 51	Choose Yes or No .
	Configure Managing Hosts		Leads to CONFIGURE SNMP HOST menu.

Menu Name	Menu Item	Refer to:	Notes
CONFIGURING SNMP HOST MENU		<i>Configuring SNMP Managers for the CPU on page 52</i>	Allows you to add up to five SNMP Manager stations that can control, interrogate, and receive Traps from the CPU.
	Managing Host IP Address	<i>Configuring SNMP Managers for the CPU on page 52</i>	The IP Address of the SNMP Manager.
	Managing Host Access Right	<i>Setting Access Rights for SNMP Managers on page 53</i>	Choose Get only or Get and Set .
	Enable Trap Receiving	<i>Directing Traps to Manager Stations on page 53</i>	Choose Yes or No .
	Enable System Log Receiving	<i>Directing the System Log to Manager Stations on page 53</i>	This parameter currently has no effect.
	Add this Managing Host	See page 53	Adds the management station settings to the CPU's management database.
	List Configured Managing Hosts	See page 53	Lists all the SNMP managers for this BBL.

Menu Name	Menu Item	Refer to:	Notes
SNMP MANAGING HOST			Displays information about CPU configured Manager stations.
SOFTWARE UPGRADE MENU		<i>Upgrading System Software on page 79</i>	Allows you to download a new configuration to the CPU.
	Download Mode	<i>Upgrading System Software on page 79</i>	Allows you to choose the Download mode. Choices are serial (Xmodem) and TFTP.
	TFTP Server IP Address	See TFTP Server IP address on page 79	Allows you to enter the IP Address of the TFTP server where the CPU will retrieve the file.
	System Software Filename	File to Upload on page 79	Allows you to enter the file name of the operating system file that you want to download.

Menu Name	Menu Item	Refer to:	Notes
	Perform Download	<i>See Perform Download on page 79</i>	Causes the CPU to retrieve the specified software file from the specified TFTP server IP Address or from the serial port.
SYSTEM CONFIGURATION – ACCESS SECURITY MENU		Setting Up Security Features on page 43	Allows you to set menu logon names and passwords for access to menus.
	User 1-3 Logon Name	User Logon Name Fields on page 44	Enter from 1 to 12 letters or numbers.
	User 1-3 Password	<i>The User Logon Password and Retype User Logon Password Fields on page 44</i>	Enter from 1 to 12 letters or numbers.
SYSTEM CONFIGURATION – CONFIGURATION CHANGES MENU		<i>Saving or Rejecting Configuration Setting Changes on page 81</i>	Allows you to save your changes, use default settings or to reject changes you have made.

Menu Name	Menu Item	Refer to:	Notes
	Save All Configuration Changes	<i>Save All Changes</i> and Reset on page 81	All changes that you have made during this session overwrite previous program entries and the CPU resets.
	Reload All Previous Configurations	<i>Reload Last Saved Configuration</i> on page 81	Abandons all changes that you have made and change entries back to their original settings.
	Reset All Configuration Changes	<i>Reset Configuration</i> to Factory Default on page 82	Resets all configuration items to their factory default settings, you must still save these settings.

SYSTEM CONFIGURATION MENU	SYSTEM OPERATION MODE		Allows you to set up the method that you will use for operating the CPU.
	Point-to-Point	<i>Point-to-Point Mode on page 54</i>	Sets the CPU for use in Campus BridgeLINK-II™ applications.
SYSTEM STATISTICS MENU		<i>Interrogating the CBL for Performance Information on page 72</i>	This menu leads you to port statistics menus for the 10BaseT and radio port.
	10BaseT Port Statistics	<i>Checking 10BaseT Port Statistics on page 73</i>	This item displays the 10BASET PORT STATISTICS menu.
	Radio Port Statistics	<i>Checking Radio Port (Wireless Link) Statistics on page 76</i>	This item displays the RADIO PORT STATISTICS menu.
10BASET PORT STATISTICS MENU		<i>Checking 10BaseT Port Statistics on page 73</i>	Allows you to interrogate the system about current traffic statistics on the 10BaseT port.

RADIO PORT STATISTICS MENU	<i>Checking Radio Port (Wireless Link) Statistics on page 76</i>	Allows you to interrogate the system about current traffic statistics on the radio port.
SYSTEM STATUS MENU	<i>Recording Important System Information on page 83</i>	Leads you to SYSTEM INFORMATION and SYSTEM LOG.
System Information	<i>Recording Important System Information on page 83</i>	Displays the System Information menu, at which you can collect version, contact, and other information about the CPU.
System Log	<i>Viewing the System Log on page 86</i>	Displays the System Log. The log stores and displays system events such as system start, warm start, or password authentication.
DIAGNOSTICS- ANTENNA AIMING MENU	<i>Aiming the Directional Antennas on page 39</i>	Allows you to fine-tune the alignment of two directional antennas.

PING Destination	<i>Selecting the Distant Campus BridgeLINK-II's Address on page 40</i>	Allows you to enter the Radio Port MAC Address for the Distant CPU.
PING Frame Size	<i>Setting the Frame Size on page 40</i>	Sets the size of the frames transferred during the PING test.
Distance	<i>Setting the Estimated Distance Between Antennas on page 40</i>	Allows you to select the estimated distance between directional antennas. You must save this parameter, for it to be permanent.
Perform PING	<i>Starting and Stopping the Test on page 40</i>	Select Start to begin, or Stop to end the test.
Current Successful Rate	<i>Viewing or Hearing Status of the Link on page 40</i>	Displays the percentage of frames that successfully reached the distant antenna.
Best Success Rate	<i>Viewing or Hearing Status of the Link on page 40</i>	Displays the best transfer rate detected during the test.
Worst Success Rate	<i>Viewing or Hearing Status of the Link on page 40</i>	Displays the worst transfer rate detected during the test.

**System Configuration
Menu**

Reset

Rest on page

Press <ENTER> here to reset
the CPU.

Troubleshooting

This section discusses ways to eliminate trouble on the wireless link. We will provide cross-references to other sections of the manual, which support corrective action.

The CPU bridges traffic between the wireless link and wired-backbone network. The unit provides several indicators of its status and, with either a serial terminal or Web-based access, a user can use the tools built into the CPU to further examine the network connection and help troubleshoot a problem report.

Indicators

In normal operation, verify that the power, 10BaseT, and radio connectors are attached. Verify that the Power LED is illuminated, and that the Radio LED is illuminated. If any of these do not operate as described, it may indicate a problem. For more information about indicators, see *LED Indicators* on page 13. Contact your distributor for assistance. If you cannot reach your distributor, or purchased the units directly from RMG, contact RMG Support.

Problem: No traffic for anyone

Using either the VT100, or Web management tools, check that the configuration is set correctly. Verify that the filters are not set to block all traffic, or stop a specific protocol (see *Bridging the Link and 10BaseT Networks* on page 56). Examine the statistic counters (see *Interrogating the CBL for Performance Information* on page 72), and use the ANTENNA AIMING page (see *Aiming the Directional Antennas* on page 39) to “see” the quality of the wireless link’s signal. Verify that the Subnet ID on each CPU is set to the same value.

Problem: Radio Range seems less than it should be.

Check the placement of the directional antenna. Generally, the higher on the wall it is placed, the better the signal pattern will be. If this link has been working for some time, inspect the antenna to see if it has been moved out of alignment. Check the line of site between directional antennas to verify that no new construction or tree growth has occurred, blocking the directional antenna link

If the problem persists and you have access to another CBL, try replacing the CBL piece by piece. If this makes a difference, it is possible a piece of the CBL may have become damaged, reducing its effectiveness. Contact your distributor for assistance.

Problem: Retransmissions are excessive.

Verify that you selected and saved the correct **Estimated Distance** on the ANTENNA AIMING page (see *Aiming the Directional Antennas* on page 39). This also sets internal CPU transmission timers. Using an incorrect setting can cause retransmissions, which reduce the link's efficiency and speed.

Glossary

Agent	SNMP software at the device being controlled. The agent monitors the status of objects in an information base called the MIB. The agent can be programmed to act on status changes and send notification messages, called Traps, to designated IP Addresses called Trap communities. The agent can also take instructions from a remote manager to make changes to objects in the MIB. For example, the manager might instruct the agent to change the system date and time.
Bridge	A network device that connects two separate physical networks into one logical network. Both sides of the bridge are on the same sub-network.
DHCP Server	A PC running a protocol that manages and tracks the assignment and use of IP Addresses to devices attempting to connect to a network.
DNS	The Domain Name System or Service, a system used by a network to transcribe the name or letter address of a site or location on the Internet entered by a user into the site's corresponding numerical IP Address.
Domain	A grouping of devices that are members of a specific realm or location on a network. Each device is identified on the Internet by a specific extension attached to the location's IP Address, which is shared among all devices within the domain.
Gateway	A door in the Internet that allows a member of one domain to access another domain. (The domains are different IP sub-networks.)

IP Address	Internet Protocol address, the numerically based address of Internet sites. It is composed of four numbers (0-255) that are linked by a period. For example: 214.8.44.155. Such an address can be assigned by a private network administrator for a private network but, for use on a larger scale one should obtain an address from the InterNIC Registration Service which assigns a different address to each user.
MAC Address	Media Access Control Address. Basic numerical address used to identify all types of nodes on networks based on the IEEE 802 standards. Protocols may assign to nodes different addresses that coincide with their system. Ultimately, however, that address can be traced to the node's MAC Address. This address is also referred to as a Data Link Control address by OSI Reference-based networks.
Manager	SNMP software used to control and manipulate the Management Information Bases (MIB) through communication with the agent.
MIB	Management Information Base. A database of information about a particular community within a network including information about the activities of that community. This information can be reviewed for understanding of activities of the MIB and troubleshooting.
Node	Any device connected to a network. It is assigned either a MAC Address (IEEE 802 Standard network) or a DLC Address (OSI Reference network).
Packets	A portion of a file being sent over the Internet. The portion contains part of the original file and the destination IP Address for the document.

PING	Packet Internet Groper. A program used for verifying/testing network connectivity between two or more computers by transmitting a special diagnostic packet to those stations on the network. It forces the receiving station to send a reply indicating that the packet reached its destination. It obtains information about the connection, by determining the amount of time for packet delivery and station response.
Routing	The path chosen by the user over which to send a packet of information from one computer or station to another via the network.
Spanning Tree	A network protocol for bridges that eliminates redundancy in a network. Also called IEEE 802.1d.
Subnet Mask	A network address that numerically represents the IP Address, including the network address and the sub-network of which the IP Address is a member.
TCP/IP	Transport Control Protocol/Internet Protocol. The combination of protocols that are used on the Internet to transfer data from one address to another.

Appendix A: Indicators, Switches, and Connectors

Indicators

10BaseT Port LEDs

There are two built-in LEDs located on the 10BaseT connector, which provide link and port activity information.

- The green CAR LED (on the left) is active when the port is connected to another powered 10BaseT port whose signaling meets the requirements for an IEEE 802.3i 10BaseT device (for example, valid link test pulses are detected on the receive pair).
- The green ACT LED (on the right) is active when receive activity is detected or during a packet transmission.

Power LED

The Power LED (green) is active when power is provided to the unit.

Fault LED

The Fault LED (amber) is active when a fault is detected and during power up diagnostics.

Radio LED

The green Radio LED illuminates when the CPU detects the presence of the distant CBL.

MDI/MDI-X

Interconnection on a 10BaseT Network must always be between MDI to MDI-X. The transmitter of each device must connect to the receiver of the other device. The reversal of the transmitter and receive assignments is called a ***crossover function***. Every 10BaseT interconnection requires a crossover function. Generally, 10BaseT ports on an adapter card are configured as MDI, and 10BaseT ports on a repeater/hub are configured as MDI-X.

The CPU automatically configures its 10BaseT port as an MDI or MDI-X port depending on the cable connected. The abbreviation MDI stands for Media Dependent Interface, and is specified by the IEEE 802.3i 10BaseT standard to be the electrical and mechanical interface to the UTP wire. An MDI port transmits out to the UTP wire on pins 1 and 2, and receives from the UTP wire on RJ-45 pins 3 and 6.

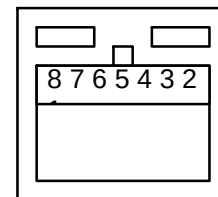
The MDI/MDI-X function automatically swaps the pin assignments of transmit and receive data wire pairs for the 10BaseT port. MDI-X configuration is used when the remote end of the wire is connected to a network station (for example, a 10BaseT adapter card) or to an MDI port on a 10BaseT concentrator. MDI configuration is used when the remote end of the wire is connected to a 10BaseT concentrator.

I/O Connectors

10BaseT connector

The 10BaseT interface is provided through a shielded RJ-45 connector, which is set to automatically detect MDI/MDI-X. The pin-out is described in the following table and figure:

Pin #	Signal (MDI configuration)	Signal (MDI-X configuration)
1	TX+ (Transmit to UTP)	RX+ (Receive from UTP)
2	TX- (Transmit to UTP)	RX- (Receive from UTP)
3	RX+ (Receive from UTP)	TX+ (Transmit to UTP)
4	No connection	No connection
5	No connection	No connection
6	RX- (Receive from UTP)	TX- (Transmit to UTP)
7	No connection	No connection
8	No connection	No connection



Serial Port Connector

The Serial port interface is provided through a DB-9 connector. The pin-out is described in the following table and figure:

Signal Description	DB-9F	DB-9M	Signal Description
Ground	2	2	Ground
Serial Out (from computer)	3	3	Rx In
Serial In (to computer)	5	5	Tx out

Appendix B: Technical Specifications

Network Protocol

10 Mb/s Manchester encoded (IEEE 802.3 CSMA/CD)

10BaseRadio™ Pulse Modulated (CSMA/CA)

Standards Support

IEEE 802.3i Type 10BaseT

Electrical Specifications

	Domestic	International
Input Power:	25 Watts	25 Watts
AC Line Frequency:	60 Hz	50-60 Hz
Input Voltage:	110VAC	100-240VAC
Volt Amperes Rating:	1A @ 100VAC	0.5A @ 240VAC

Physical Specifications

Dimensions:

Weight:

Environmental Specifications

Operating Temperature: 5 C to 40 C

Storage Temperature: -25 C to 70C

Operating Humidity: 85% max. relative humidity, non-condensing

Storage Humidity: 95% max. relative humidity, non-condensing

Operating Attitude: 10,000 ft (3,000m) maximum

Electromagnetic Emissions

Meets requirement of:

FCC Part 15, Subparts A and B, Class A

EN55 022 (CISPR 22:1985), Class A

General License VDE 0871, Class A (AmtsblVfg No. 243/1991 and Vfg 46/1992)

VCCI Class 1 ITE

Safety Agency Approvals

UL-listed, ULC-listed, CSA-certified, TUV-licensed

Getting Technical Support

If you have technical questions or have determined that your equipment is damaged, RMG offers a number of ways to get assistance:

1. Contact your local RMG reseller from which you purchased the product.
2. See the RMG Web Site for technical assistance:

<http://www.radiolan.com>

When your browser accesses the Web Site, click Technical Support.

3. You can reach RMG Technical Support directly at the following e-mail address:
 - support@radiolan.com,
4. Alternatively, you can reach our technical staff by dialing (408) 365-6200

Please have the following information available and ready:

- Your name, address, and phone number
- The serial number of the RadioLAN Marketing Group part in question
- A description of the problem that you are experiencing

Technical Support may ask you to run tests and give results of those tests. It is therefore best if you are located as close as possible to the CPU when you call.

Index

1

10BaseT (and Radio) MAC Filter List menu, 96
10BaseT (and Radio) Port Parameters menu, 93
10BaseT LED indicators, 6
10BaseT Networks, 47. *See also* networks
 browser requirements, 24
 configuring, 49
 connections, 6, 55
 getting performance information, 64, 55
10BaseT Port Parameters menu, 93
10BaseT Port Parameters Page, 49
10BaseT Port Statistics command, 103
10BaseT Port Statistics menu, 103
10BaseT Port Statistics Page, 64

A

AC line frequency, 116
Accept Packet command, 96
access rights
 SNMP Managers, 44
Access Security menu, 101
Access Security Page, 35

ACT LED, 6
activity information, 112
Add this Managing Host command, 98
adding user names and passwords, 35
addresses. *See* IP Address; MAC address
Administration Parameters menu, 84, 89
Administration Parameters Page, 37
administrators, 37
 dynamic addressing and, 39
agent, 23
 assigning IP Address, 38
 configuring, 36
 creating IDs for system, 37
aligning antennas, 21
amperes rating, 116
anchoring devices, 17
angle of operation, 2
antenna, 2, 8
 attaching to CRM, 7
 grounding, 18
 improving signal quality, 30
 mounting, 19
 siting, 20
Antenna Aiming menu, 104
Antenna Aiming page, 30

antenna cable, 8
 attaching to CRM, 17
assigning access rights
 SNMP Managers, 44
assigning IP Address
 default gateway, 39
 to SNMP agent, 38
attaching to CPU, 26
authentication, 24

B

Best command, 105
Block IP Packets command, 95
Block IPX Packets command, 95
Block MAC Packets command, 94
Block NetBEUI Packets command, 95
Block NetBIOS Packets command, 95
bridge, 60, 106
 configuring, 61
 port priority setting, 63
bridge priority, 61
Bridge Priority command, 92
Bridging Parameters menu, 92
browser, 24

C

cables, iii, vi, 1, 8, 18
Campus BridgeLINK
 operational modes, 45
 setting up, 9, 10, 15, 20
 system components, 4
 technology overview, 1
Campus BridgeLINK Manager, 25
 getting system information, 74
 keyboard shortcuts, 79
 main menu, 28, 82
 main screen, 29
Campus BridgeLINK Processor Unit. *See* CPU
CAR LED, 6
case sensitivity, 35
changing system configuration, 72
 preventing SNMP Manager from, 44
collision error packets, 65
communications
 getting performance information, 64, 67
 optimizing, 64
Companion Radio Module. *See* CRM
configuration
 10BaseT networks, 49
 changing, 72

- preventing SNMP Manager from, 44
- DHCP Server, 39
- hard-wired bridge, 61
- local connections, 6
- reverting to previously saved, 73
- saving changes, 72
- SNMP agent, 36
- upgrades and, 70
- VT100 terminals, 54
- Configuration Changes menu, 102
- Configuration Changes Page, 72
- Configure Managing Hosts command, 97
- Configuring SNMP Host menu, 97
- connections, 2, 47
 - 10BaseT networks, 6, 55
 - attaching to CPU, 26
 - CPU to hardware, 18
 - local configurations, 6
 - multiple users and, 60
 - remote stations, 23
 - VT-100 terminals, 23, 78
- connectors, 7
 - I/O pin assignment, 114
 - troubleshooting, 106
- contacting RadioLAN Technical Support, 119
- CPU, 4, 47, 70
 - 10BaseT interface, 6

- accessing from network, 26
- addressing, 53
- alternative management devices, 78
- electrical connections, 5
- getting performance information, 64
- hardware connections, 18
- installing, 15
- mounting, 7, 16, 17
- operational modes, 45
- packet retransmission, 68
- powering up, 22
- selecting name and address, 31
- system requirements, 24
- CRC error checking, 65
- CRM, 7
 - attaching antenna cable, 17
 - mounting, 17
- CRM port, 7
- crossover function, 113
- customer assistance, 119
- cyclical redundancy checks, 65

D

- D connector, 7
- Data Encryption, 23. *See also* security

Data Encryption menu, 87

data filters

- adding, 58

- caution for setting, 55

- changing MAC, 59

Data Link Control address. *See* MAC Address

data loss precautions, 60

data transfers, 47, 60

- enabling/disabling, 55

- for remote users, 50

- large files and performance, 64

- remote performance and, 65, 68

- transmit rates, 68

Default Gateway IP Address command, 90

default settings, 73

Destination Address Filtering command, 96

devices, 78

- hard-wire external, 6

- networks and, 39

- port priority, 63

DHCP Operation Mode command, 90

DHCP Server

- assigning IP Address, 39

DHCP Server IP Address command, 91

directional antenna. *See* antenna

distance guidelines, 10, 15

documentation, iv, vi, 1

typographic conventions, v, vi, 1

Download Mode command, 99

dynamic addressing, 39

Dynamic Host Configuration Protocol. *See* DHCP Server

E

Edit MAC Filters command, 95

electrical connections, 5

electrical specifications, 116

electromagnetic emissions, 117

Enable Authentication Trap command, 97

Enable System Log Receiving command, 98

Enable Trap Receiving command, 98

encryption, 23. *See also* security

entering user name and password, 27, 81

environmental specifications, 117

Estimated Distance command, 105

Ethernet Networks. *See also* networks

- accumulated error count, 65

- LED indicators, 6

- packet transfers, 66

events, 77

Explicit Address command, 104

external devices, 6

F

- factory default settings, 73
- Fault LED, 4
- FCC compliance, ii, vi, 1
- files, transmitting large, 64
- Filter Mask Address command, 96
- Filter Physical Address command, 95
- filtering databases, 55
- filters
 - adding MAC Address, 58
 - caution for setting, 55
 - changing MAC Address, 59
- Forward Delay Time command, 92
- Frame Size command, 105
- frames, resizing, 29
- frequency, iii, vi, 1, 116

G

- gateway
 - default IP Address, 39
 - getting default, 75
- geographic locations (system IDs), 37
- ground, 18

H

- hardware version information, 76
- hard-wired external devices, 6
- hard-wired link, 60, 106
 - configuring, 61
- Hello Time command, 92
- hosts, 39
- hot keys, 79
- hub, 6
 - CPU connections, 18

I

- I/O connectors, 114
- improving signal quality, 30
- indicators, 4, 6, 7
 - troubleshooting, 106
- input, 116
- installation, 15
 - directional antenna, 19
 - location requirements, 2, 9, 10, 15, 19
- interference, ii, vi, 1
- Internet, 38
- IP Address
 - assigning

- default gateway, 39
 - to SNMP agent, 38
- getting current, 75
- specifying for network devices, 39
- IP Address command, 89
- IP filters, 50
- IP Parameters menu, 85, 89
- IP Parameters Page, 38
- IPX filters, 51
- isolated networks, 38

K

keyboard shortcuts, 79

L

LAN. *See* networks

LED indicators, 4, 6, 7

- troubleshooting, 106

line frequency, 116

List All Filters Configured command, 96

local area networks. *See* networks

Local Management menu, 79

location requirements, 2, 9, 10, 15

- directional antenna, 19

Logon page, 80

logs, 77

M

MAC Address, 47

- remote stations, 56
- wildcards and, 56

MAC Address filters

- adding, 58
- caution for setting, 55
- changing, 59
- deleting, 59

MAC Filters menu, 95

main menu, 28, 82

Management Information Base. *See* MIB

Manager, 25

- getting system information, 74
- keyboard shortcuts, 79
- main menu, 28, 82
- main screen, 29

Managing Host Access Right command, 98

Managing Host IP Address command, 97

mask bytes, 57

Max. Age Time command, 92

menus, 28, 82

accessing items, 29
MIB, 23, 36
mode of operation, 45
modems, 23
mounting assemblies, 19
mounting bracket, 7
mounting height, 20

N

N connector, 7
network browser. *See* Web browser
network devices, 39
network hub, 6
 CPU connections, 18
networks, 47. *See also* specific type; wireless stations
 administering remote stations, 37
 attaching to CPU, 26
 dynamic addressing and, 39
 isolated and IP Addressing, 38
 multi-building locations and, 10
 optimizing performance, 60
 protocol for, 116, 117
 shared resources and, 64
nodes, 47
 MAC Address assignment, 56

notification messages, 62. *See also* Traps

O

operating frequency, iii, vi, 1, 116
operational modes, 45
outages, 60
overrun packets, 66

P

packets, 47, 60
 collision counter, 65
 enabling/disabling transfers, 55
 for remote users, 50
 receiving from distant CPU, 69
 remote transfer checks, 65, 68
 retransmitting, 68
 shared network resources and, 64
 transmit rates, 68
passwords, 24
 adding, 35
 entering, 27, 81
 not set, 80
Perform Download command, 100
performance, 55, 64

performance information, 23
 getting, 64
pin-outs
 I/O connector, 114
Point-to-Point command, 103
Point-to-Point Mode, 45
Port Name command, 94
Port Parameters menu, 85, 93
 10BaseT Port options, 49
Port Path Cost command, 92
Port Priority command, 92
ports
 hard-wired link priority, 63
 network-specific connections, 49
 serial access, 23
Power LED, 4
power ratings, 116
power transformer, 5
powering up the CPU, 22
Processor Unit. *See* CPU
protecting wireless stations, 23, 24

R

Radio Module. *See* CRM
Radio Port Parameters menu, 93

Radio Port Statistics command, 103
Radio Port Statistics menu, 103
Radio Port Statistics Page, 67
Radio Unit
 getting performance information, 67
 locating, 9
RadioLAN MAC Address assignment, 56
RadioLAN Technical Support, 119
Read Community command, 97
reception, ii, vi, 1, 21
 testing, 31
registered IP Addresses, 38
Reject Packet command, 96
Reload All Previous Configurations command, 102
reloading previous configurations, 73
remote stations, 23, 25
 administration, 37
 data transfer performance, 65, 68
 enabling/disabling data transfers, 50
 getting performance information, 23
 viewing MAC Address, 56
Reset All Configuration Changes command, 102
Reset Page, 73
resizing frames onscreen, 29
resources, 64
retransmissions, 68
RJ11 compatibility, 6

routing database, 62
runt packets, 66

S

safety approvals, 118
Save All Configuration Changes command, 102
saving system configurations, 72
screens, resizing frames, 29
security, 23, 24, 80
 setting up, 35
serial devices, 78
serial number, getting, 76, 81
serial port, 23
service tables, 55
setting up Campus BridgeLINK, 9, 10, 15, 20. *See also*
 configuration
shared resources, 64
signal quality, 30
signals
 I/O connector, 114
Simple Network Management Protocol. *See* SNMP
SNMP agent, 23
 assigning IP Address, 38
 configuring, 36
 creating IDs for, 37

SNMP Manager, 23
 Administration Parameters options, 37
 IP Parameters options, 38
 notification parameters, 42
 setting access rights for, 44
SNMP Managing Hosts menu, 98
SNMP Parameters menu, 86, 96
SNMP Parameters Page, 42
Software Upgrade menu, 98
Software Upgrade Page, 70
Source Address Filtering command, 96
Spanning Tree Parameters Page, 60, 61
specs, 116, 117
standards, 116
Start command, 105
startup procedure (first time), 26
startup screen (Manager), 29
status indicators, 106
status information
 reception, 31
Status LEDs, 4
submenus, 29
Subnet ID command, 94
Subnet IDs
 getting current, 75
subnet mask, 39
 getting current, 75

- Subnet Mask command, 89
- Successful % command, 105
- system agent IDs, 37
- system components, 4
- system configuration
 - 10BaseT networks, 49
 - changing, 72
 - preventing SNMP Manager from, 44
 - DHCP Server, 39
 - hard-wired bridge, 61
 - reverting to previously saved, 73
 - saving changes, 72
 - SNMP agent, 36
 - upgrades and, 70
 - VT100 terminals, 54
- System Configuration menu, 84
- System Configuration screen
 - 10BaseT Port Parameters Page, 49
 - Access Security Page, 35
 - Administration Parameters Page, 37
 - Configuration Changes Page, 72
 - IP Parameters Page, 38
 - SNMP Parameters Page, 42
 - Software Upgrade Page, 70
 - Spanning Tree Parameters Page, 60, 61
 - System Operations Mode Page, 45
- system contact, 37

- System Contact command, 89
- system indicators, 4, 6, 7
 - troubleshooting, 106
- system information, 74, 77
- System Information command, 104
- System Information Page, 74
- System Location command, 89
- System Log command, 104
- System Log Page, 77
- system logs, 77
- System Name command, 89
- system names, 37
- System Operation Mode command, 87
- System Operations Mode Page, 45
- system requirements, 24
- System Software Name command, 100
- System Statistics menu, 103
- System Statistics screen
 - 10BaseT Port Statistics Page, 64
 - Radio Port Statistics Page, 67
- System Status menu, 104
- system upgrades, 70

T

- technical specifications, 116, 117

technical support, 119
temperature, 117
testing reception, 31
TFTP Server IP Address command, 99
transmit rates, 68
transmitting large files, 64
Traps
 sending/receiving, 44
troubleshooting tips, 106

U

unauthorized users, 23, 24
upgrades, 70
User Logon Name command, 101
user names
 adding, 35
 entering, 27, 81
User Password command, 102

V

version, getting, 75, 76

voltage, 116
VT100 terminal
 setting up, 54
VT-100 terminal
 connecting to, 23, 78

W

Web browser, 24
Web Site, 25
 RadioLAN technical assistance, 119
wildcards, 56
wireless networks. *See* wireless stations
wireless stations, 47, 55
 bridging to hard-wired, 60, 106
 getting performance information, 23, 68
 optimizing performance, 64
 protecting from unauthorized users, 23, 24
 troubleshooting tips, 106
Worst command, 105
Write Community command, 97

RadioLAN Marketing Group

185 Lewis Road
San Jose, CA 95111
Phone: (408) 365-6200
Fax: (408) 365-7675
www.radiolan.com