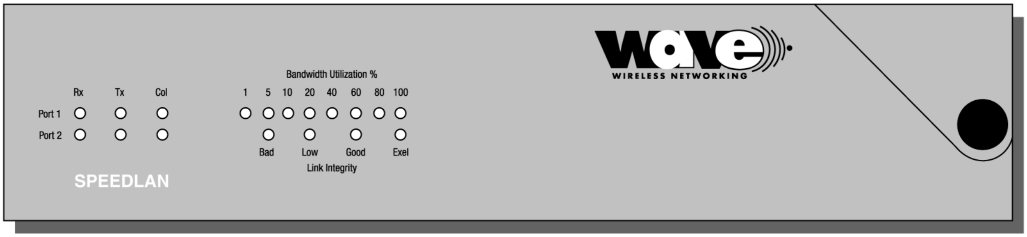
SPEEDLAN Shelf Mount Manual

Product ID NCBSLXE2



Installation and Operation User Guide

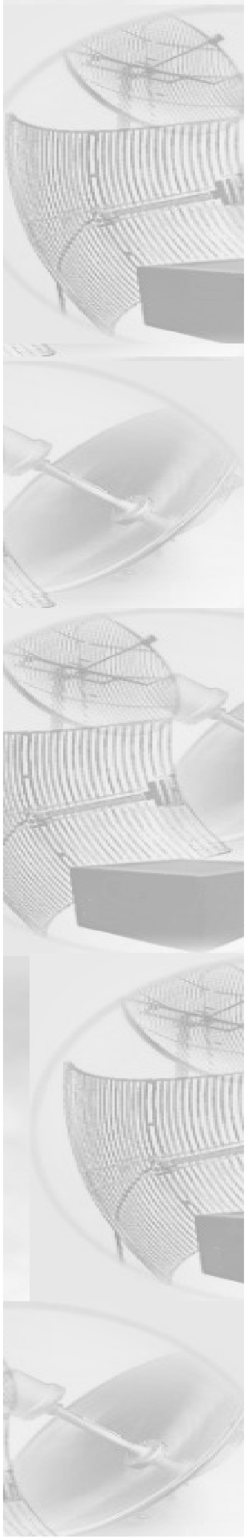
Version 1.1 / Last Revised July 15, 2001

Wave Wireless Networking
a *SPEEDCOM* Wireless Company
1748 Independence Blvd., C-5
Sarasota, FL 34234
941-358-9283
www.wavewireless.com

Wave Wireless Networking, a SPEEDCOM Wireless Company, shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. Wave Wireless Networking, a SPEEDCOM Wireless Company, reserves the right to revise this publication from time to time and make changes in content without obligation to notify any person of such revision changes.

Contents of this publication may be preliminary and/or may be changed at any time without notice and shall not be regarded as a warranty.

Chapter 1
Introduction



What’s New in This Manual?

- All references formely known as "CampusPRC" are now refered to as "SectorPRC."
- SPEEDLAN products include the silver 64-bit encryption card and the gold 128-bit encryption card. For more information, see *Security Button - 11 Mb RF Security Setup, page 5-12*.

Features and Benefits

The SPEEDLAN shelfmount products are high performance 11 MB wireless bridges that create interconnectivity between buildings and provide an alternative to Telco leased and fiber optic lines. The SPEEDLAN shelfmount bridges present unparalleled performance and features for any organization needing high-speed connectivity between enterprise LAN-to-LAN applications such as school or campus network connections, banking, manufacturing, hospitals and clinics. This enables a central Ethernet LAN to be connected with one or more branch office LANs up to 25 miles apart.

The SPEEDLAN bridges present a significant breakthrough in LAN connectivity by offering these high performance bridges that outperform other wireless spread spectrum systems in the industry. These bridges contain full remote SNMP management and security in an affordable package. This enables you to monitor a number of SPEEDLAN parameters including RF-signal quality and noise level, as well as transparent bridging with advanced filtering for security and network reliability.

The central base station and CPE are mounted inside the building and connect to the outdoor antenna using up to 200 feet of low loss RF antenna cable.

Transparent Ethernet Bridging with Advanced Filtering for Security and Network Reliability

SPEEDLAN brouters support what is known as Transparent Ethernet Bridging with no Spanning Tree or Source Routing support. Since the SPEEDLAN brouters provide network security between a local LAN and a campus or enterprise wide network, and since using multiple bridges in a Spanning Tree could compromise this security, the Spanning Tree scenario is not supported. In addition, the SPEEDLAN brouters can filter packets based on protocol type or MAC address pairings. These features can add a significant measure of security and network reliability to a network interconnection.

IP Routing with Advanced Filtering for Security

The SPEEDLAN brouters support IP Routing in addition to bridging. It can be used to add routing capability when an IP router may be a more appropriate choice.

SNMP Management

SNMP wireless and wired link management may be administered from any Ethernet network or remotely from the Internet. The SNMP MIB II, Bridge MIB, and Ethernet-Interface MIB come with the brouters, so you can use SNMP to monitor a number of SPEEDLAN parameters, including RF-signal quality and noise level.

Wireless Multipoint Protocol

Campus Cell PRC features provide multipoint networking, improved performance, and increased reliability. In multipoint networks, a SPEEDLAN base station acts as a central base station with responsibility to manage the flow of data within the radio cell. When necessary, packets are repeated or retransmitted by this brouter, allowing communications between multiple remote networks by using SPEEDLAN CPE.

ISP Functionality

The SPEEDLAN shelfmount ISP products are tailored to fit the needs of Internet Service Providers and Broadband Telecommunications Providers. Two features particularly useful to Internet Service providers are the additional of Network Address Translation (NAT) and Dynamic Host Server Protocol (DHCP). NAT helps to ensure network security and allows an entire company to share a single global IP address for communication on the Internet. For example, a company can provide its clients with just one IP address, allowing access to the company’s firewall only. DHCP servers provide efficient use of IP addresses by assigning them dynamically or statically to the wireless brouter location. DHCP allows network administrators to assign dynamic IP addresses for the period of time needed to connect to the Internet or network, whereas static IP addresses are beneficial to users that need to maintain a "constant" connection. This reduces the load on the entire wireless network.

Features

- 10/100BASE-T Ethernet Interface
- SPEEDLAN 11 Mb Wireless Radio Interface
- Bridging Features
- Protocol Transparent Bridging
- IP Routing
- Filtering by Ethernet Multicast, Broadcast and Bad Packets
- Filtering by Protocol
- Filtering by Ethernet Address Pair
- Generic Ethernet Tunneling through IP Networks
- Learned Table Lockdown
- Expanded IP ARP Support
- Automatic Broadcast Storm Protection and Notification
- Supports up to 48 Remote Buildings

SNMP Features

- IP "ping" Support
- IP SNMP Support (MIB II, Ethernet, Interface, SNMP, and Bridge MIB)
- IP SNMP WaveLAN
- IP SNMP Trap Support
- SNMP Access Lists

ISP Features

- DHCP Server
- Outgoing and Incoming NAT

SNMP Management

SNMP wireless and wired link management may be administered from any Ethernet network or remotely from the Internet. The SNMP MIB II, Bridge MIB, and Ethernet-Interface MIB come with the bridges, so you can use SNMP to monitor a number of SPEEDLAN brouter parameters, including RF-signal quality and noise level.

IP-Router Features

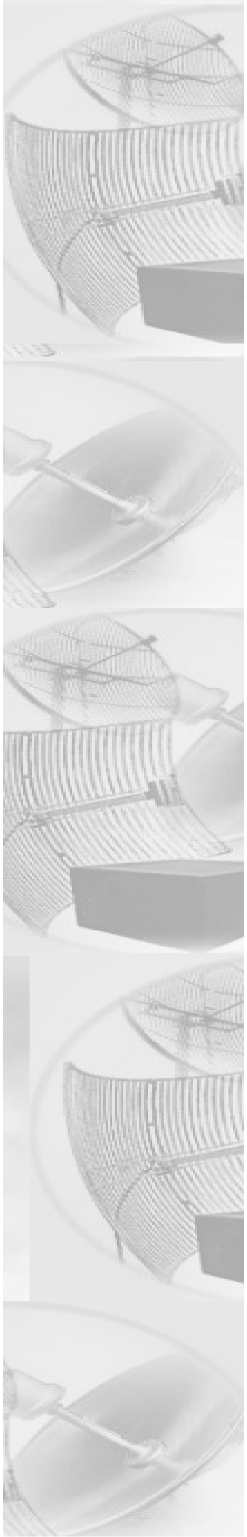
- IP Static Routing with Direct and Static Routes
- ICMP Messages, Default Router, and Subnet Support
- SNMP Support for All Router-Related MIB Variables
- RIP Support

Encryption Features (Add-on Option)

- Data Encryption of Wireless Packets

Notes:

Chapter 2
Quick Start



System Description

The SPEEDLAN brouters are high speed, long range wireless LAN brouters that provide connectivity to remote Ethernet networks. For single point-to-point links, a SPEEDLAN CPE can be used in each building to create a wireless communication line. For multipoint links, a SPEEDLAN acts as the central base station, which controls the communication between multiple SPEEDLAN brouters acting as CPE. The local brouter communicates with a remote brouter on another LAN. This effectively creates an extended wireless network, spanning sites situated up to 25 miles apart. This enables a central Ethernet LAN to be connected with one or more branch office LANs. A single brouter with an omnidirectional antenna may communicate with multiple brouters to create multipoint wireless site-to-site connectivity.

Rooftop and Tower Installations Warning

Rooftop, tower and mounted equipment (brouters) installations are extremely dangerous and incorrect installation can result in death, injury, or property damage. **These installations must be performed by professional antenna installers only.**

Package Contents

Note: Certain items are only available when purchased with the SPEEDLAN Installation Kit.

- SPEEDLAN brouter
- Product registration card
- SPEEDLAN CD containing:
    - Product manual
    - Configuration management software
- *Electrical tape
- *U-bolt antenna mounting hardware
- *Cable sealant putty
- *Lightning arrestor
- *Grounding clamps
- *Ethernet surge protector

- *Wire zip ties
- *Antenna (specialized upon request)
- *Amplifier (specialized upon request)

* **Note:** Items can be purchased separately or as part of an Installation Kit.

Installation Steps

Installation instructions are specific to customers who purchased Installation Kits from Wave Wireless. To view a diagram of the installation listed below, see *Installation Diagram, page 2-7*.

The directions below contain installation procedures for the items included in the SPEEDLAN brouter antenna (and amplifier) kit. If you do not have an item included in the instructions below, contact Wave Wireless.

TIP

If you are having trouble and need a full site installation, contact Wave Wireless Networking for services and fees.

To install the SPEEDLAN, do the following:

Step 1. Line of Sight

Before installing the antennas and bridges, make sure a clear line of sight exists. Line of sight can be defined as each antenna being able to clearly see the other antenna or being able to see the remote locations when viewing from the SPEEDLAN base station location. Be sure to look level with the center of origin of the transmission (the middle of the antenna). Do the same from the remote location. Any disruption of the signal path due to trees, buildings or any other obstructions may cause the link to function improperly. If you see any such obstruction between the two antennas, move one or both antennas elsewhere.

Step 2. Mount the Antenna

a) On a side building mount, as in the diagram at the end of this section, position the bracket so there will be at least three feet (one meter) above the roof line of the building where the pole is attached; this leaves room for the antenna and reduces signal loss from building reflection.

b) Allow for as much space between the wall brackets as possible while still maintaining the antenna height necessary. For extended poles, additional wall brackets may be necessary.

c) Assemble the antenna and mount it to the pole using the included U-bolt hardware. On larger dish-type antennas, align the grid on the dish to run parallel with the grid on the tip of the antenna horn. Preferably, the grid should be horizontal (or parallel) to the ground. Make sure all bolts and screws are fastened tightly.

d) Fasten the pole to the brackets. Position the antenna, point it in the appropriate direction, and tighten the screws.

Step 3. Run the Cabling

The installation kit comes with two lengths of cable with ready made connectors that fit your particular installation.

a) Attach the shorter cable to the antenna, making sure the connectors are screwed on tightly.

b) Attach the lightning arrestor to the end of the shorter cable.

c) Attach the longer cable to the lightning arrestor.

d) Drill the hole needed to get through the wall, being very careful not to drill into power conduits or other utilities in the wall.

e) Feed the cable through the wall and run it to the SPEEDLAN base station brouter.

f) Fasten all cabling securely to the pole and walls using clamps and zip ties. Do not run cable over electrical devices such as fluorescent lights because these devices will interfere with the operation of the brouter. Be careful when pulling or fastening the cable that unnecessary pressure does not break your connectors.

g) Seal all outdoor connections with the black electrical tape and black sealant insulation putty that comes in the installation kit. First, wrap the connectors tightly with the tape. Then, carefully wrap the connectors evenly with the insulation putty, making certain to leave no cracks that would allow water to penetrate the seal.

Step 4. Ground the Antenna

a) Mount the lightning arrestor to a solid surface.

b) Run the grounding wire from the lightning arrestor to a proper ground source such as a grounding rod or roof ground wire.

c) Seal the entire lightning arrestor with the black waterproof sealant insulation putty that comes in the installation kit. **Note:** The lightning arrestor is **NOT** waterproof.

Step 5. Connect the Wireless Bridge to the Power Supply

a) Make sure the switch on the power supply is set to the proper voltage (110V or 230V AC).

b) Connect the power cord's IEC 320 female outlet to the IEC 320 male power inlet on the back panel of the SPEEDLAN brouter.

c) Connect the power cord to an external power outlet (110V or 230V AC).

Step 6. Connect the Wireless Bridge to any Available Outlet of the Ethernet LAN

a) Connect the RJ-45 connector on a standard Ethernet cable to the RJ-45 port on the back panel of the brouter.

b) Connect the other end of the Ethernet cable to your Ethernet hub, switch or router.

Step 7. Repeat If Needed

Repeat Steps 1-6 for all of the SPEEDLAN brouters that will be communicating with this one.

Step 8. Check Functionality Using the LED Indicators.

When the installation is complete, activate the SPEEDLAN brouter. The radio will automatically transmit a “hello” packet to the other brouter(s) to initiate communication. When a remote brouter is located, the brouters will synchronize themselves with each other once communication is established. Then, the brouters will start forwarding data packets to the wireless LAN that is connected to them. When the brouters are “handshaking” correctly, you will see the receive and transmit lights blink on and off as they communicate.

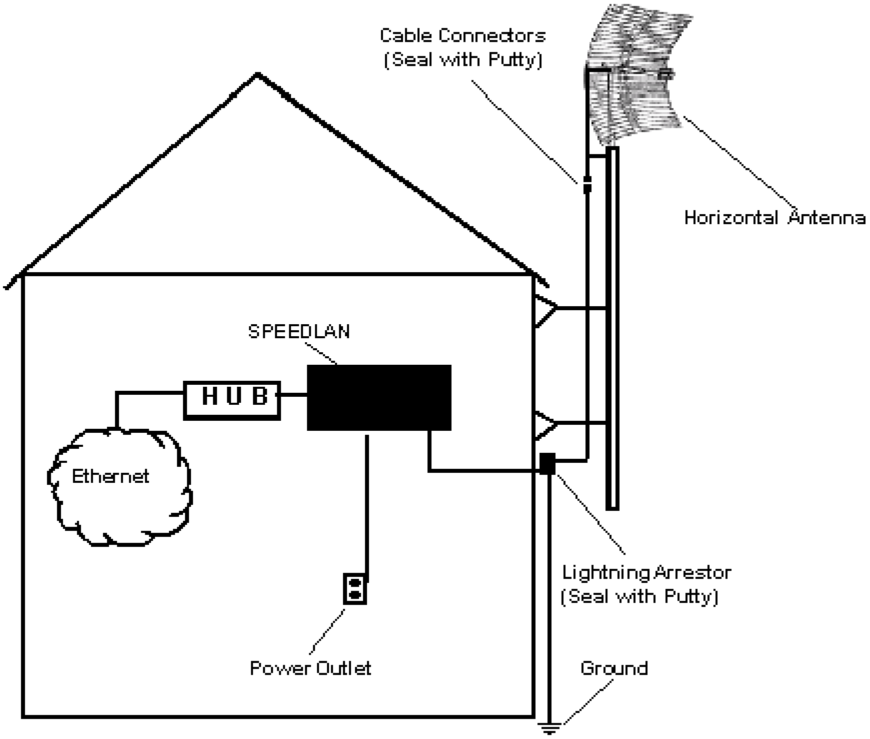
As the brouters forward data back and forth to one another, you may occasionally see a collision light on the display panel. This is a normal aspect of networking. A solid collision light displayed on the front panel indicates that the particular interface is not able to detect a link.

TIP

If you think the brouter is not configured or operating properly, try troubleshooting the problem by seeing *Appendix B Startup LED Patterns, page Appendix B-1*.

Installation Diagram

The diagram below displays where the main components are located.

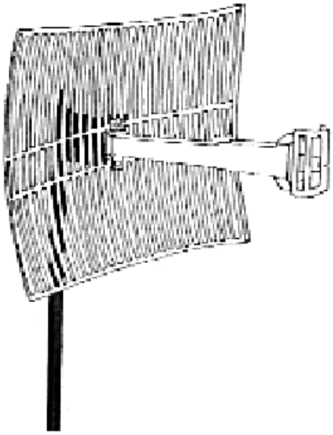


All outdoor cable connections and lightning arrestors must be insulated with waterproof electrical putty.

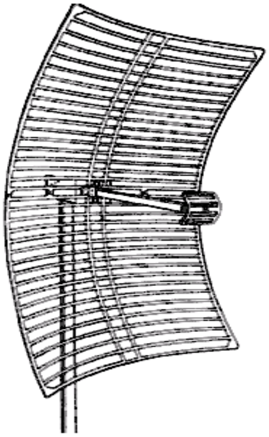
Polarizations on a Grid Antenna

The antenna must be aimed so that when you look out from the center of the antenna it is pointing toward the receiving antenna on the other building. The radio signal radiates from the end of the antenna like a wide-beamed flashlight.

Vertical Polarity



Horizontal Polarity

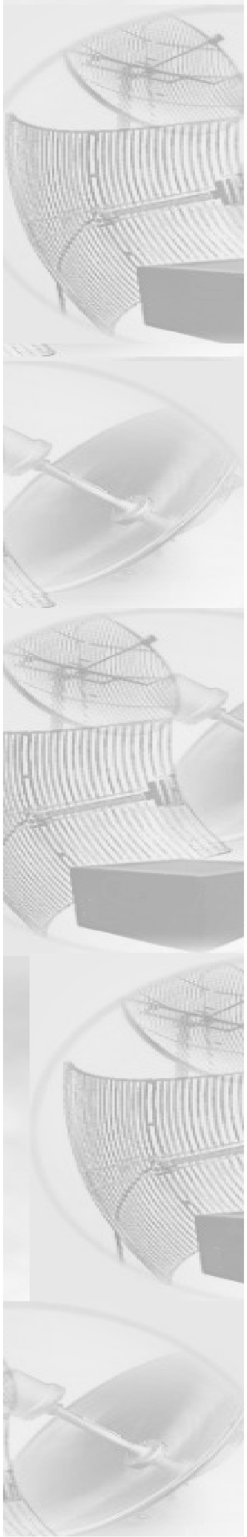


In order for the antennas to operate correctly, the polarities must match!

TIP

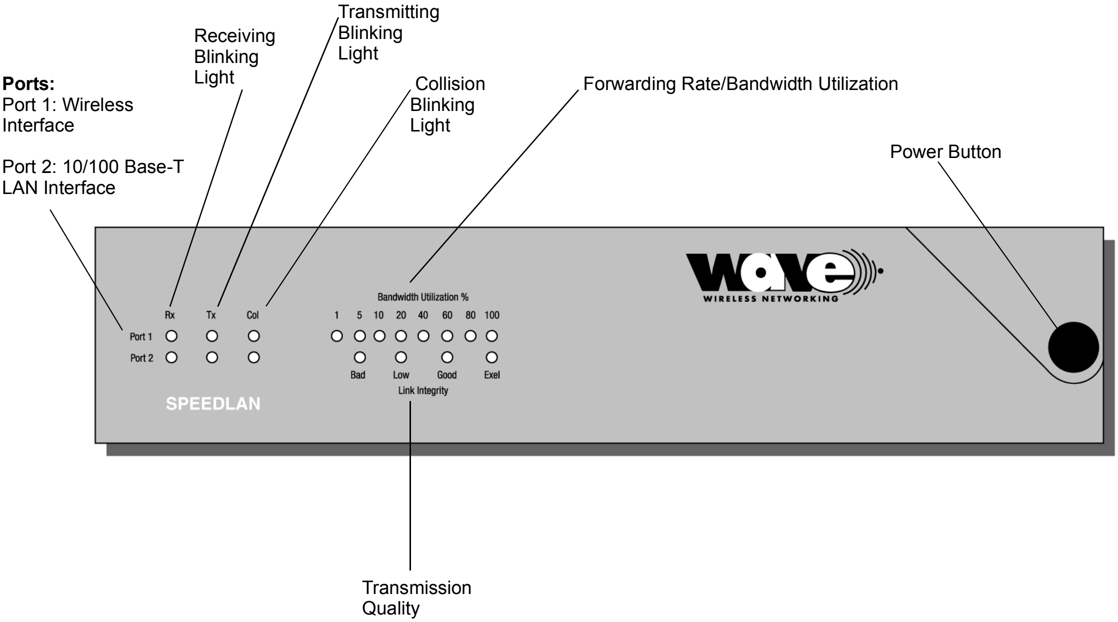
For most applications we have found that horizontally polarized antennas work best. This is because most other signals that may cause interference are vertically polarized. If you use horizontal polarization, you can reduce the interference caused by those other signals.

Chapter 3
Hardware



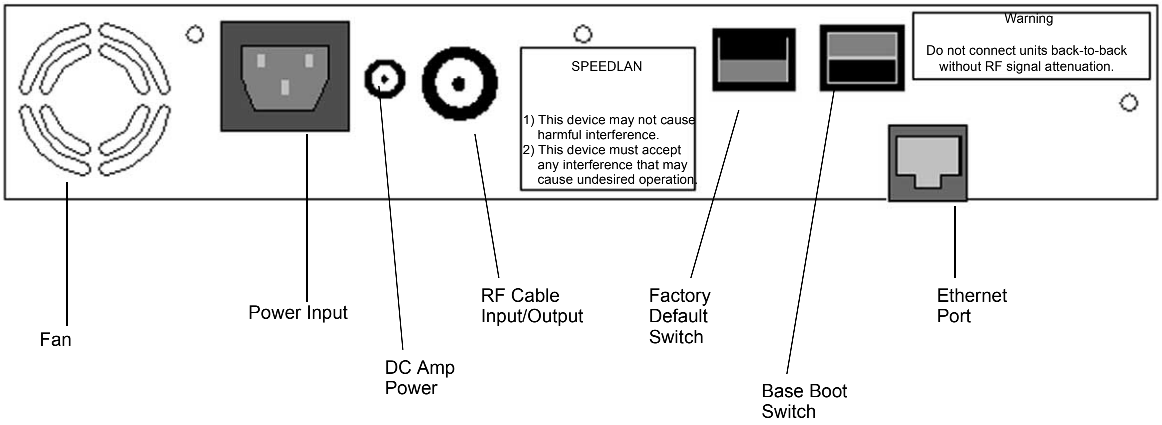
Drawings of Components

SPEEDLAN Front Panel



- Rx
  This light will blink whenever a packet is received on the related interface
- Tx
  This light will blink whenever a packet is transmitted on the related interface
- Collision
  This light will blink whenever a collision occurs. It will remain “solidly lit” when a link cannot be established on that interface
- Port 1
  Wireless Interface
- Port 2
  10/100 Base-T LAN Interface
- Forwarding Rate/Bandwidth Utilization
  Percentage of wireless bandwidth currently being used
- Link Integrity
  Gives a visual indication of the RF signal strength
- Power Switch/Button
  Used to activate power to the brouter

SPEEDLAN Back Panel


Warning
Do not connect units back-to-back without RF signal attenuation.
SPEEDLAN
1) This device may not cause harmful interference.
2) This device must accept any interference that may cause undesired operation.
Fan
Power Input
DC Amp Power
RF Cable Input/Output
Factory Default Switch
Base Boot Switch
Ethernet Port

- **Power Input**
  AC power input
- **DC Amp Power**
  Provides power for optional external amplifier.
- **RF Cable Input/Output**
  Interface for RF cable. The connector used for this port is a reverse TNC bulkhead.
- **Factory Default**
  Places the SPEEDLAN into a factory default mode for troubleshooting purposes.
- **Base Boot**
  Puts the brouter in a mode to accept a firmware upgrade. Not to be used for any other purpose.
- **10/100Base-T Ethernet Port**
  Standard RJ-45 Ethernet port. The Ethernet interface is capable of operating either 10 or 100 Mbps. By default it is configured for 10 Mbps Ethernet.
- **Serial Number**
  The silver sticker on the back of the SPEEDLAN is where you will find the serial number of your brouter. All products are tracked using their respective serial numbers. If you ever need technical assistance, we will need the serial number to determine the exact build of your equipment.

Restoring Factory Default Settings on the SPEEDLAN

To restore the factory default settings on the brouter, do the following:

1. Turn off the SPEEDLAN unit.
2. Connect the PC to the brouter using a crossover Ethernet cable or using 2 Straight-through cables and a hub.
3. Under the Network Neighborhood on your PC, change your IP address to **198.17.74.195** and assign a Subnet Mask of **255.255.255.0**. You will also need to remove any gateways that were defined in your TCP/IP properties.
4. You will be asked if you want to reboot your PC. Click **Yes**.
5. On the back panel of each brouter, depress the small black **Factory Default** switch to the UP position. For normal operation the switch should be depressed in the down position. Power-up the brouter and let it reboot.
6. The brouter is temporarily in factory default mode.
7. On your PC, start the SPEEDLAN Configurator.
8. From the **File** menu, choose **Open Remote Config**.
9. In the space for IP Address, enter **198.17.74.254**. This is the IP Address of the brouter while in factory default mode. Click on **OK**, and then **OK** again. You should see a message confirming that the bridge configuration was read properly.
10. From the **File** menu, choose **Save Remote Config**.
11. All the configuration settings on the brouter have now been returned to a factory default state. You may now configure the brouter for operation on your network.

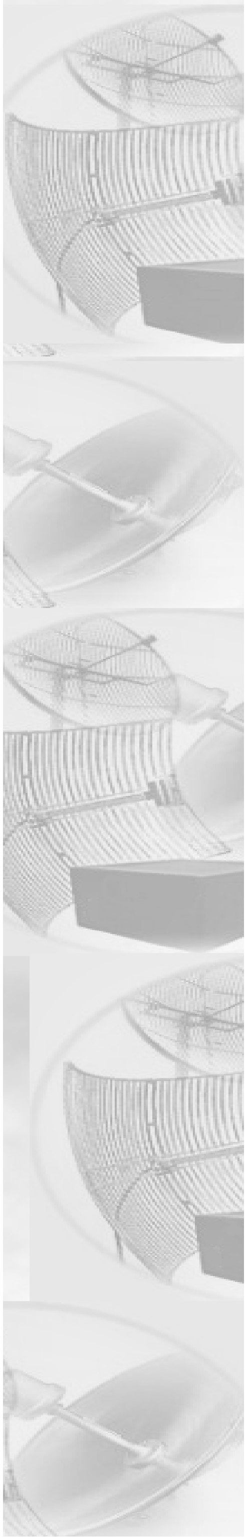
Upgrading the Firmware

You will need to update your firmware if the old one is damaged or additional functionality has been added. To upgrade the firmware, do the following:

1. Turn the SPEEDLAN unit off.
2. Connect the PC to the brouter using a crossover Ethernet cable, or using 2 Straight-through cables and a hub.
3. Under the Network Neighborhood on your PC, change the IP address to **198.17.74.195** and assign a Subnet Mask of **255.255.255.0**. You will also need to remove any gateways that were defined in your TCP/IP properties.
4. You will be asked if you want to re-boot your PC. Click **Yes**.
5. On your PC, start the SPEEDLAN Configurator.
6. From the **File** menu, select **Open Config**. Then, select the appropriate .Bin file.
7. Then from the **File** menu, choose **Upload Software**. A dialog box will appear with an IP address in it. Click **Scan**; this will bring up another dialog box with the IP Address of the SPEEDLAN. This IP Address will be 198.17.74.254. At this point click **OK**, and confirm the IP Address in the first dialog box is 198.17.74.254. Then, click **OK** again.
8. Next a menu will appear requesting a MAC Address, as well as a Passkey. You can only receive these from Wave Wireless. You will enter these two variables and click the **OK** button. There will be a sequence of dialog boxes, which will warn you that you are about to reload the Flash ROM with a new .Bin file. Click **OK** for all of them. This will cause the brouter to reboot.
9. Allow the brouter to reboot normally.
10. The brouter has now been updated with a new .Bin file. You may now configure the brouter to operate on your network.

Notes:

Chapter 4
Overview of Configurator



Installation and Setup

Windows 95/98/NT 4.0 SPEEDLAN Configurator

To install the SPEEDLAN Configurator, do the following:

1 Shut down all programs and applications.

Note: The SPEEDLAN Configurator uses library files, which reside on your Windows 95/98/NT 4.0 PC. If a program or application is open, the Setup will not install correctly. If the Configurator is not installed correctly, the brouter could be rendered and inoperable after saving a configuration.

2 Insert the CD into your floppy drive (i.e., Drive E, F, etc.).

3 If the **setup.exe** program does not execute automatically, click **Start** + **Run**. The Run dialog box appears. Click **Browse** and locate the setup.exe where your CD-ROM drive is located. Then, click **Open** and **OK**.

4 Follow the installation prompts.

5 After the installation is complete, restart your computer.

Toolbar and Menus

File Menu

The Windows 95/98/NT 4.0 Configurator will configure either a remote Flash ROM in the brouters or configure a SPEEDLAN file saved on your computer. You can configure a SPEEDLAN file on your computer and download it to the brouters later after you have verified that all settings are correct. This can make reconfiguring your brouter a quick operation if you have the completed configuration already saved to your computer.

Configuring a SPEEDLAN Brouter

To configure a remote (network attached) brouter, you can use the Open Remote Config and Save functions. You must have a brouter configuration opened with the Configuration Utility before any configuration functions are performed. After you have opened the remote device and configured it, you can then save your configuration back to the open device. When you `Save' back to the remote device, its Flash ROM will be erased and reprogrammed with the new configuration. After you save the configuration, wait the required 15-second period. This allows the Flash ROM to be fully programmed and enables the brouter to reboot with the new configuration.

Turning off the brouter, or otherwise interrupting the reprogramming of the Flash ROM, can damage the programming of the brouter, and render it inoperable.

Note: Anytime you make changes in Frequency, IP Routing, or Network ID, start with the brouter furthest away from your current location. This will allow you to complete your changes without having to physically go to each location.

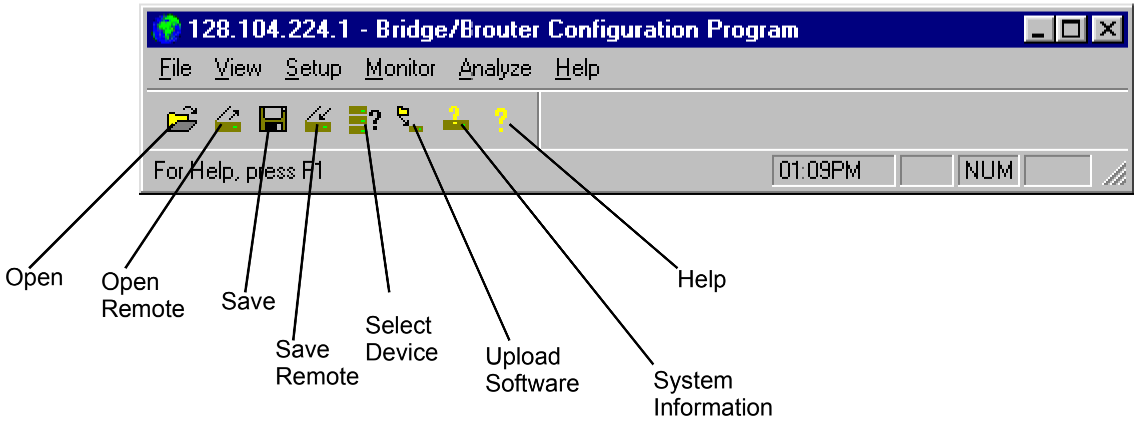
Configuring a Saved Configuration File

To configure a saved CNF file (configuration file), open it from the **File** menu by using the **Open** function. Then, configure the file just as if you were configuring a remote brouter. When you are finished configuring the file, save it to disk from the **File** menu using the "**Save Config File As**..." function. The "Open Remote Config..." and "Save Config" functions are used for accessing and saving directly to the brouter without using a file saved on diskette. Be careful when you save the configuration file that you do not save the configuration directly to the SPEEDLAN; otherwise, you will be configuring the brouter and may not be able to re-access it after uploading the incorrect configuration to it.

Exporting and Importing a Configuration

Once you have opened a remote brouter, you can take a "snapshot" of the current configuration with the "Save Config File As..." function. This function will result in creating a CNF file. The extension .CNF is used to denote the special exported binary configuration file. The CNF file created with the "Save Config File As..." function can later be imported into another brouter by using the "Import Config File..." function, then saving the configuration to the brouter using the "Save Config" function.

The Toolbar



Note: The functions on the toolbar can also be accessed from the menus on the Configurator (i.e., Save can be accessed from the File menu).

The Menu Bar

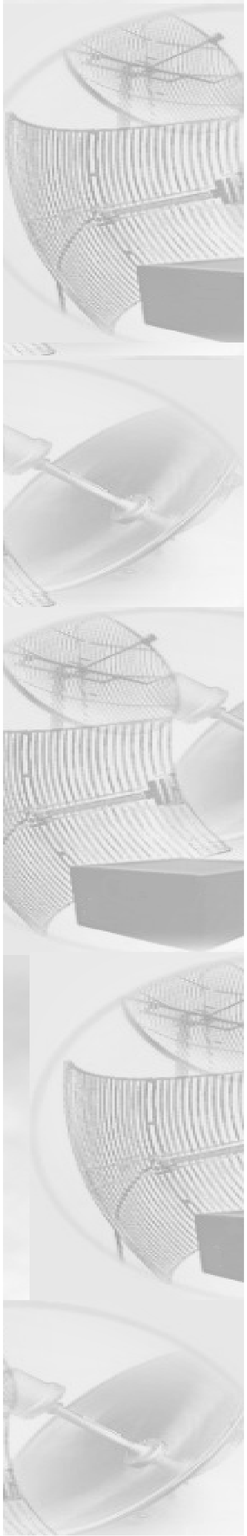
- The File Menu - This is the most common menu and is used to perform the following functions:
- Open Config File - This opens a configuration file from disk.
- Open Remote Config - This opens the configuration file directly from a remote device.
- Save Config - This saves the configuration you are working on to the place where you opened it.
- Save Config File as - This saves the current configuration into a file on disk. This file will have the extension .CNF.
- Import Config File - This opens a configuration file from disk. This function is used when you are going to save the configuration from disk to a remote brouter.
- Upload Software - This enables you to load a raw and unconfigured binary file to the brouter. This is done only in the event that the brouter's firmware has been damaged.
- Reboot Remote - This is used to reboot a brouter from a remote location.
- Exit - This closes the SPEEDLAN Configurator.

Quick Overview of Other Menus

- View Menu - This menu is used to change the display of the Configurator's various items.
- Setup Menu - This menu is used to modify all aspects of the brouter.
- Monitor Menu - This menu is used to monitor the brouter's performance and monitor another brouter.
- Analyze Menu - This menu is used to select another brouter and perform various tests (i.e., interval test, wireless link test, or antenna alignment test)
- Help Menu - This menu is used to troubleshoot questions pertaining to the SPEEDLAN Configurator.

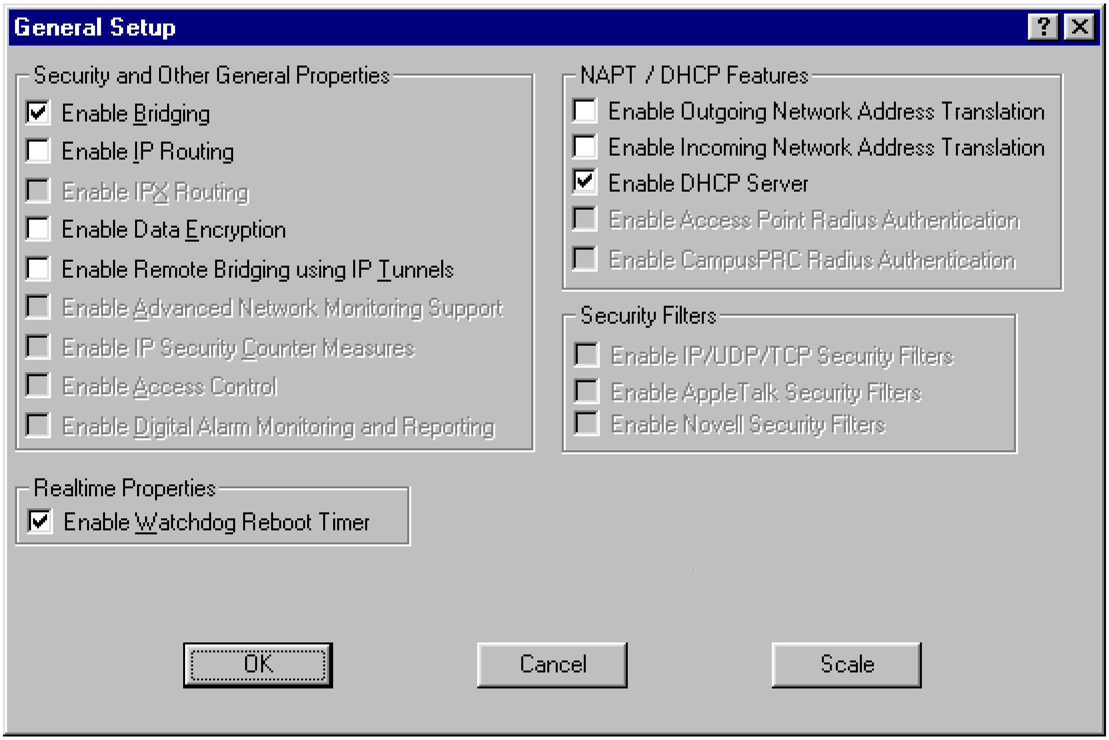
Notes:

Chapter 5
Configuring SPEEDLAN



General Setup

This dialog box activates the features to configure your brouters. To select this dialog box, choose **General Setup** from the **Setup** menu of the SPEEDLAN Configurator. Select the appropriate check boxes as described below:



General Setup

Security and Other General Properties

- ☑ Enable Bridging
- □ Enable IP Routing
- □ Enable IPX Routing
- □ Enable Data Encryption
- □ Enable Remote Bridging using IP Tunnels
- □ Enable Advanced Network Monitoring Support
- □ Enable IP Security Counter Measures
- □ Enable Access Control
- □ Enable Digital Alarm Monitoring and Reporting

NAPT / DHCP Features

- □ Enable Outgoing Network Address Translation
- □ Enable Incoming Network Address Translation
- ☑ Enable DHCP Server
- □ Enable Access Point Radius Authentication
- □ Enable CampusPRC Radius Authentication

Security Filters

- □ Enable IP/UDP/TCP Security Filters
- □ Enable AppleTalk Security Filters
- □ Enable Novell Security Filters

Realtime Properties

- ☑ Enable Watchdog Reboot Timer

- **Enable Bridging**
  The transparent bridging function will be enabled when this is item is selected. If you want the brouters to perform the bridging function, you must select this check box. When bridging is enabled, the Bridge Setup dialog box will be accessible. Bridging should be enabled for nearly all applications of the brouter. The default is ON.

- **Enable IP Routing**
  The transparent routing function will be enabled when this is item is selected. IP Routing will work properly only if the routes are set up in the IP Route dialog box. **If the routes are not set up properly before you save the configuration, the router will become inoperable.** The default is OFF.

- **Enable Data Encryption**
  This optional feature allows you to encrypt wireless data transmissions on top of the encryption provided by the radio. It provides 56-bit DES encryption. It is not shipped standard as part of the brouter. If you did not purchase it when you originally bought the brouter, it can be purchased later as a software upgrade. Data encryption is disabled by default. Select the box labeled **Enable Encryption** to enable the encryption features. You will still need to define at least one encryption key before your wireless traffic will be transmitted using wireless data encryption. To do this, return to the drop-down menu presented when you click on **Setup**. Now you will see a Data Encryption Setup item added to the menu list. Select **Data Encryption Setup**. Click the **DES Encryption** button and enter an 8 digit alhpanumeric string in the range of "a-z", "A-Z", and "0-9".
  Examples:
  Alphanumeric: a5F2z4wK

Warning: This setting must be set to the same value for the brouters that will be communicating together. Failure to set them to the same value will prevent any communications from taking place. For example, in order to use a multipoint link, you must use the same Encryption setting on the base station and on the CPE brouter.

- **Enable Remote Bridging using IP Tunnels**
  SPEEDLAN brouters support a special feature which will enable Ethernet packets of any protocol type to be encapsulated in IP packets and sent to other brouters (purchased from Wave Wireless) for de-encapsulation. This method can be used to setup virtual Ethernet LANs between several points using an IP network as the transport layer.
- **Enable Advanced Network Monitoring Support**
  This option is not available at this time.
- **Enable IP Security Counter Measures**
  This option is not available at this time.
- **Enable Access Control**
  This option is not available at this time.
- **Enable Digital Alarm Monitoring and Reporting**
  This option is not available at this time.
- ***Enable Outgoing Network Address Translation**
  This option enables a company to map the private network's IP address into one or more global network IP addresses. This means outsiders will only view the single (or more if designated) IP network address assigned for global viewing on the Internet. For more information, see *Part III - Setting Up NAT, page 7-20*.

- *Enable Incoming Network Address Translation

  This option enables a company to unmap public network IP addresses into network IP addresses. For more information, see *Part III - Setting Up NAT, page 7-20*.

- *Enable DHCP Server

  This option enables the DHCP Server on the SPEEDLAN. For more information, see *Part III - Setting Up NAT, page 7-20*.

- Enable Access Point Radius Authentication

  This option is not available at this time

- Enable SectorPRC Radius Authentication

  This option is not available at this time.

- Enable IP/UDP/TCP Security Filters

  This option is not available at this time.

- Enable AppleTalk Security Filters

  This option is not available at this time.

- Enable Novell Security Filters

  This option is not available at this time.

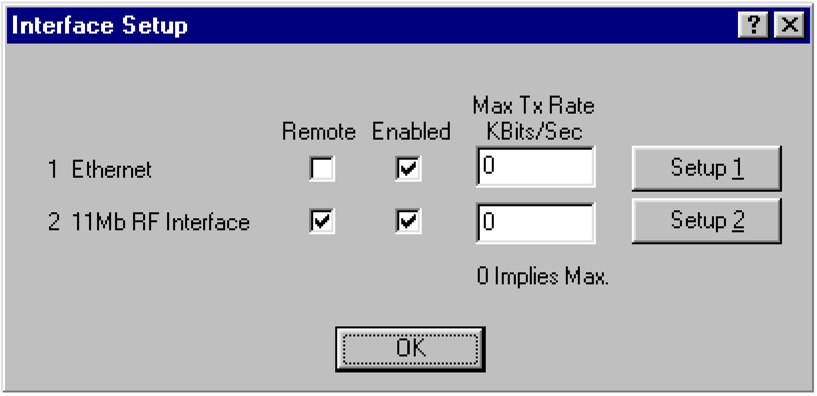
- Enable Watchdog Reboot Timer

  This feature instructs the brouter to reboot in the event that the brouter fails to receive any incoming packets, from any port, for a period of 10 minutes. The brouter will assume an error has occurred and will reboot. If, after the brouter reboots, it does not receive an incoming hello signal, the brouter will listen for the hello signal until the user reboots the brouter manually. The Watchdog will recognize when a signal has been re-established and will reset the timer accordingly.

Interface & Advanced Interface Setup

Interface Setup

To set up the basic interface, choose **Interface Setup** from the **Setup** menu on the SPEEDLAN Configurator. The interfaces that are installed in your brouter will be represented on this dialog box. The Remote check box is used to designate which interfaces will be considered local and remote. **The local interface is considered to be the interface that connects directly to the local LAN with respect to the brouter. The remote interface is considered to be the interface that connects with the remote LAN.** The set up buttons are used to access the portion of the configuration which controls how the individual interfaces are configured.



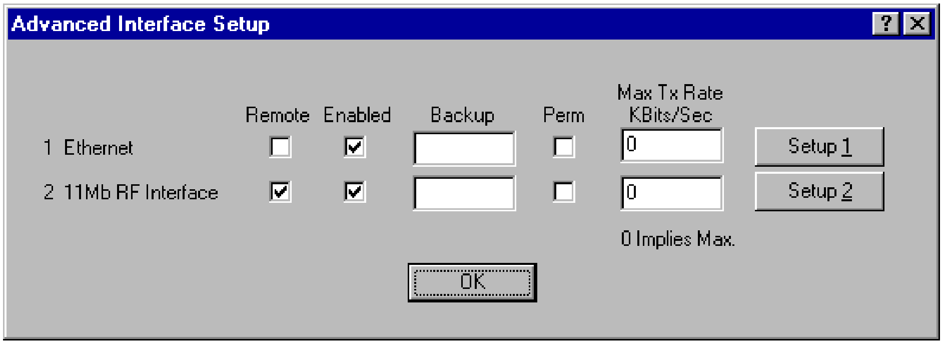
Interface Setup

	Remote	Enabled	Max Tx Rate KBits/Sec	
1 Ethernet	☐	☑	0	Setup 1
2 11Mb RF Interface	☑	☑	0	Setup 2

0 Implies Max.

Advanced Interface Setup

To set up the advanced interface, choose **Advanced Interface Setup** from the **Setup** menu on the SPEEDLAN Configurator. The Advanced Interface Setup contains a few more advanced settings, but they are set up in the same manner. Note that the Max Tx rate is available on both the Interface Setup and Advanced Interface Setup. Max Tx Rate is useful to ISPs that want to regulate the maximum bandwidth provided to each customer. These settings should not be changed without the assistance of a Wave Wireless Networking Technical Support Engineer.



Advanced Interface Setup

	Remote	Enabled	Backup	Perm	Max Tx Rate KBits/Sec	
1 Ethernet	□	☑		□	0	Setup 1
2 11Mb RF Interface	☑	☑		□	0	Setup 2

0 Implies Max.

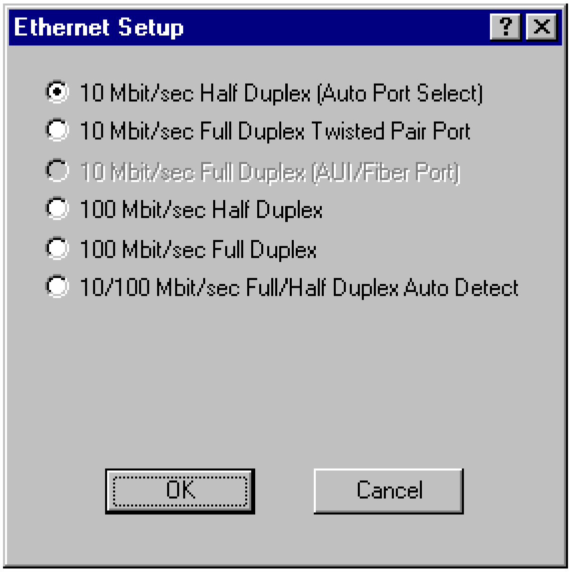
The Setup Buttons

Setup 1 Button - Ethernet Setup

To modify the Ethernet Setup, click the **Setup 1** button on the Interface Setup or Advanced Interface Setup dialog box. SPEEDLAN brouters come standard with a 10/100 Base-T interface to connect to your wired network. Although the interface is capable of operating at both 10 Mbps and 100 Mbps, it does not use autosensing or autoswitching functionality. The default setting is for 10 Mbps half-duplex operation. If you want to connect your brouters to a 100 Mbps port, the Ethernet interface can be manually switched to 100 Mbps in this portion of the setup.

The interface also supports full-duplex operation when connected to either a 10 or 100 Mbps LAN port. The default setting is for half-duplex. The interface can be configured to operate in the full-duplex mode by selecting it on this dialog box.

Clicking the Setup buttons (1 and 2) on the Interface & Advanced Interface Setup dialog box will open the Setup dialog box (for the interface selected).



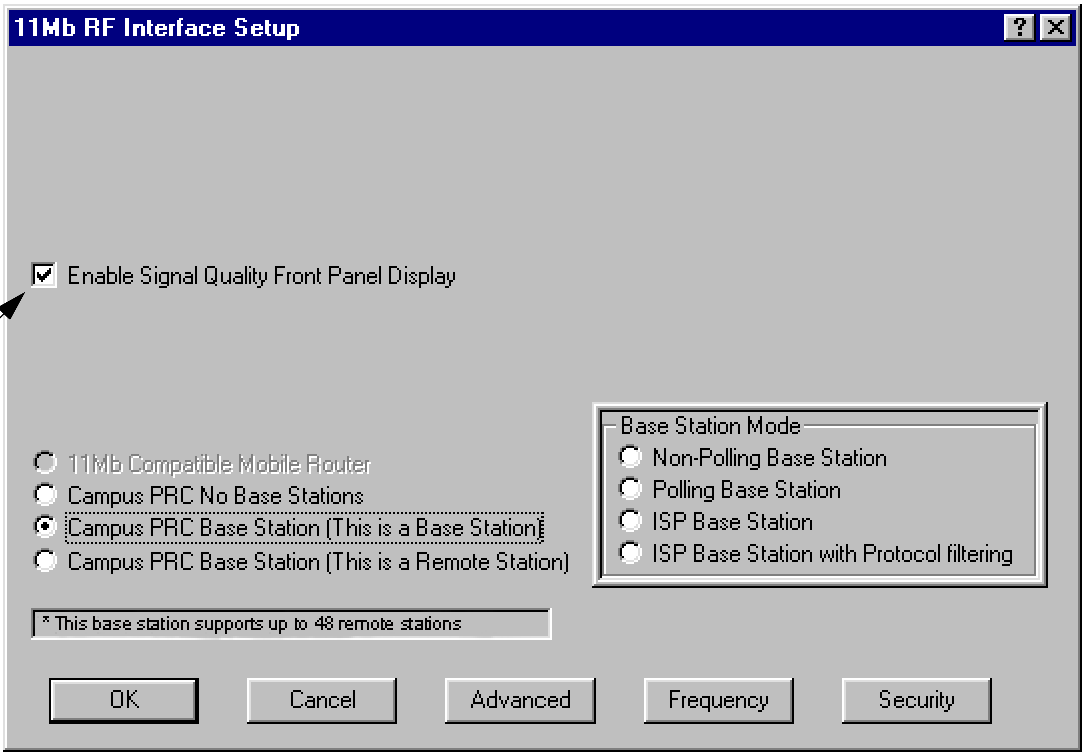
Ethernet Setup

- ● 10 Mbit/sec Half Duplex (Auto Port Select)
- ○ 10 Mbit/sec Full Duplex Twisted Pair Port
- ○ 10 Mbit/sec Full Duplex (AUI/Fiber Port)
- ○ 100 Mbit/sec Half Duplex
- ○ 100 Mbit/sec Full Duplex
- ○ 10/100 Mbit/sec Full/Half Duplex Auto Detect

Setup 2 Button - 11 Mb RF Interface Setup

To modify the 11 Mb RF Interface Setup, click the **Setup 2** button on the Interface Setup or Advanced Interface Setup dialog box. This dialog box displays the configuration settings that control the individual interfaces and how they communicate with each other. On the next page, you will find a description of the settings, as well as how they affect the brouter's performance of the interfaces.

This actually controls the "Link Integrity" lights on the front panel of the brouter, and it is turned ON by default. Wave Wireless highly recommends that you leave it enabled.



11Mb RF Interface Setup

☑ Enable Signal Quality Front Panel Display

○ 11Mb Compatible Mobile Router
○ Campus PRC No Base Stations
● Campus PRC Base Station (This is a Base Station)
○ Campus PRC Base Station (This is a Remote Station)

Base Station Mode
○ Non-Polling Base Station
○ Polling Base Station
○ ISP Base Station
○ ISP Base Station with Protocol filtering

* This base station supports up to 48 remote stations

Transport Methods

The industry compatible method of transmitting and receiving data over wireless networks will cause data packets to frequently be lost. This is due to the fact that a wireless network does not have the ability to detect collisions like a wired Ethernet network. On an Ethernet network, collisions can be detected by the hardware and are automatically retransmitted. Ethernet is referred to as CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Wireless networks are CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Collisions cannot be detected because wireless cannot receive and transmit at the same time. This means brouters are not able to listen for collisions. A brouter that is operating properly in a point-to-point network will loose, due to collisions, less than 1% of the transmitted packets. This packet loss is not normally a problem with protocols such as Novell IPX (without the Burst Mode NLM), but may cause networks using most other protocols to experience poor performance. Campus Cell PRC helps to alleviate this problem by placing multiple packets into one larger packet, which saves bandwidth by eliminating the extra overhead. The transport methods are described:

- **Campus Cell PRC Mode (No Base Station/Brouter)**
  This method of transportation is used only for point-to-point links. If any of the brouters are unable to see each other, a base station must be used to repeat traffic from one brouter to next brouter in line. This point-to-point mode utilizes Campus Cell PRC packet bundling, which reduces the amount of overhead caused by sending smaller individual packets across the wireless network. This greatly improves the performance of the connection.
- **SectorPRC Mode (This is a Non-Polling Base Station/Brouter)**
  This setting should be used if this is the only base station in the wireless network cell. SPEEDLAN has a special mode where one wireless brouter can be configured as a base station and each additional wireless node is setup as a CPE brouter. In this configuration the only requirement is that each SPEEDLAN be able to communicate directly with the SPEEDLAN base station. The SPEEDLAN base station is responsible for repeating packets that need to travel between the SPEEDLAN CPE. The Non-Polling Base does not allocate dynamically bandwidth to each remote brouter.

TIP

The performance of this approach is greatly improved if the SPEEDLAN base station is connected to the heaviest network or network server.

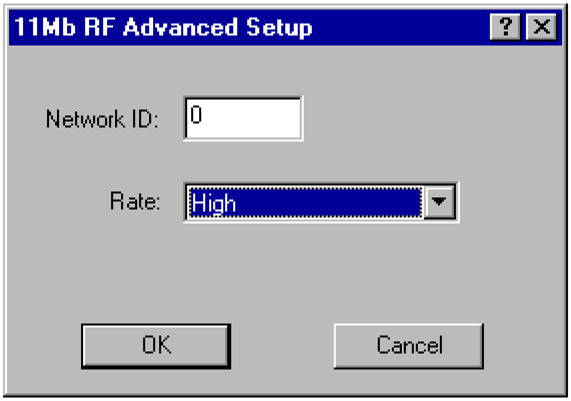
- **SectorPRC Mode (This is a Polling Base Station/Brouter)**
  This is the recommended mode of operation for a wireless base station. When the number of CPE exceed 3 or 4, the non-polling base station may not be able to keep up with the wireless traffic that needs to be forwarded. The polling base station alleviates this problem by continuously communicating with every SPEEDLAN CPE in its cell. It is also responsible for dynamically assigning how much bandwidth is allocated to each remote site based on the network traffic load.

This greatly improves the performance of a SPEEDLAN base station wireless network cell. As the number of SPEEDLAN CPE brouters increase, the importance of a polling base station increases and efficiency is proportionately improved.

- **SectorPRC (This is a Remote Station/Brouter)**
  This is the configuration required for remote brouters that will be installed as CPE into a multipoint wireless network. In this mode, a SPEEDLAN CPE will only communicate with a base station. This mode cannot be used for point-to-point links.

Advanced Button - 11 Mb RF Interface Setup

The Advanced button is located to the left of the Frequency button. Clicking this button will open a new dialog box that allows you to change the Network ID and rate of the interface.


11Mb RF Advanced Setup

Network ID: 0

Rate: High

- **Network ID**
  The Network ID is a security setting that allows the brouter to reject packets from other wireless brouters in the area. Although the bridging or routing table would reject the packet once it was processed, the Network ID allows the brouter to reject the packet with less processing. This improves the performance of the brouters in installations where many wireless brouters are co-located in the same area or where other organizations may be running wireless bridges of their own. The default setting is 0 and the valid range is 0 to 15.

This setting must be set to the same value for the brouters that will be communicating together. Failure to set them to the same value will prevent any communications from taking place. For example, in order to use a multipoint link, you must use the same Network ID setting on the base station and on each CPE brouter.

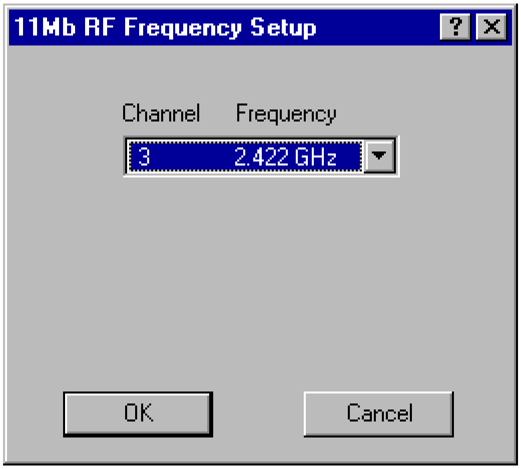
- **Rate**
  This setting refers to the RF data rate. The SPEEDLAN 11 Mbps radios have four data rates that can be used:
  - *High*
    This is the full 11 Mbps data rate. The interface default to this value and it is recommended that you operate using it for most installations. The receiver sensitivity of the radio with this setting is -82 dBm.
  - *Medium*
    This setting limits the card to providing 5.5 Mbps of bandwidth. The receiver sensitivity of the radio with this setting is -85 dBm.

- *Standard*
  This setting limits the card by providing 2 Mbps of bandwidth. The receiver sensitivity of the radio with this setting is -89 dBm.
- *Low*
  This setting limits the card by providing 1 Mbps of bandwidth. The receiver sensitivity of the radio with this setting is -92 dBm.

Warning: This setting must be set to the same value for the brouters that will be communicating together. Failure to set them to the same value will prevent any communications from taking place.

Frequency Button - 11 Mb Frequency Setup

The Frequency button is located to the right of the Advanced button. Clicking this button will open a new dialog box that allows you to change the operating frequency of the interface. All of the brouters expected to communicate with this device should be configured with the same frequency.

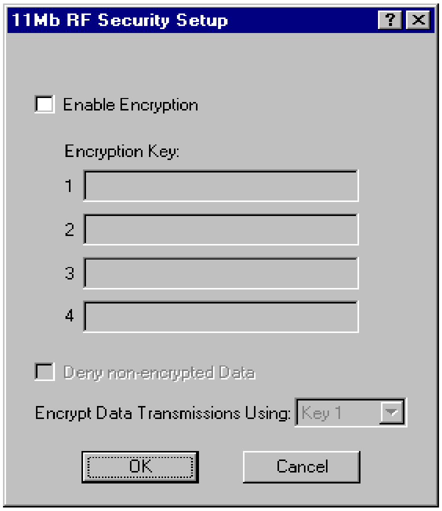


11Mb RF Frequency Setup

Channel 3 Frequency 2.422 GHz

Security Button - 11 Mb RF Security Setup

The Security button is located to the right of the Frequency button. Clicking this button will open a new dialog box that allows you to change the security options of the interface. These settings are used to encrypt data that will be transmitted by the 11 Mb RF port and also to decrypt data that is received by 11 Mb RF port. You may define up to 4 encryption keys to be used for decrypting incoming data and one key for encrypting outgoing data.



Check the box labeled **Enable Encryption** to enable the encryption features. You will still need to define at least one encryption key before your wireless traffic will be transmitted using wireless data encryption.

The Encryption Key can be defined using either:

- For silver cards (64-bit)- Five alphanumeric characters within the "a-z", "A-Z", and "0-9".
- For gold cards - 13 alphanumeric characters within the "a-z", "A-Z" and "0-9" range.

Note: The alphabetical characters that you entered are "case-sensitive". For example: silver card users would enter "Secu1" and gold card users would enter "Security Key1".

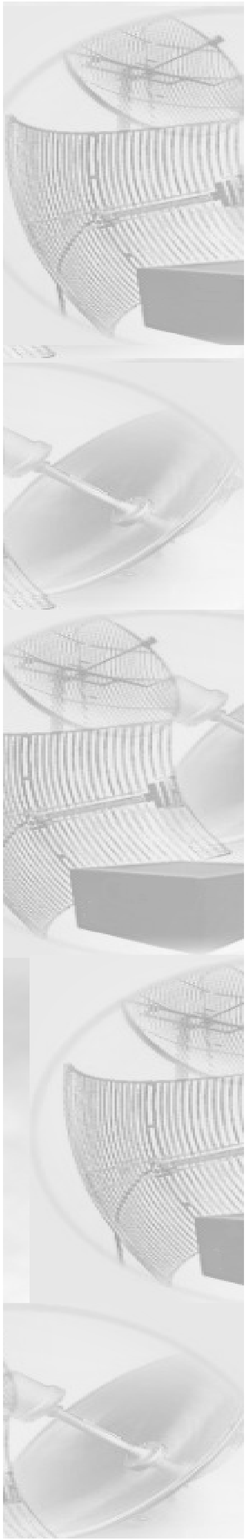
Write down the values you enter as Encryption Keys and store them in a secure place. The values you enter will only be visible when they are entered for the first time. Each time this option is displayed after the initial setup, the values will appear only as "xxxxxxxxxx"

Warning: This setting must be set to the same value for the brouters that will be communicating together. Failure to set them to the same value will prevent any communications from taking place. For example, in order to use a multipoint link, you must use the same Encryption setting on the base station and on the CPE brouter.

There is also an option to **Deny non-encrypted Data**. This feature is disabled by default and is designed primarily for multipoint SPEEDLAN installations where it may not be necessary to run using data encryption at all locations. If you enable this option, any data received by this brouter will not be passed to the wired network interface.

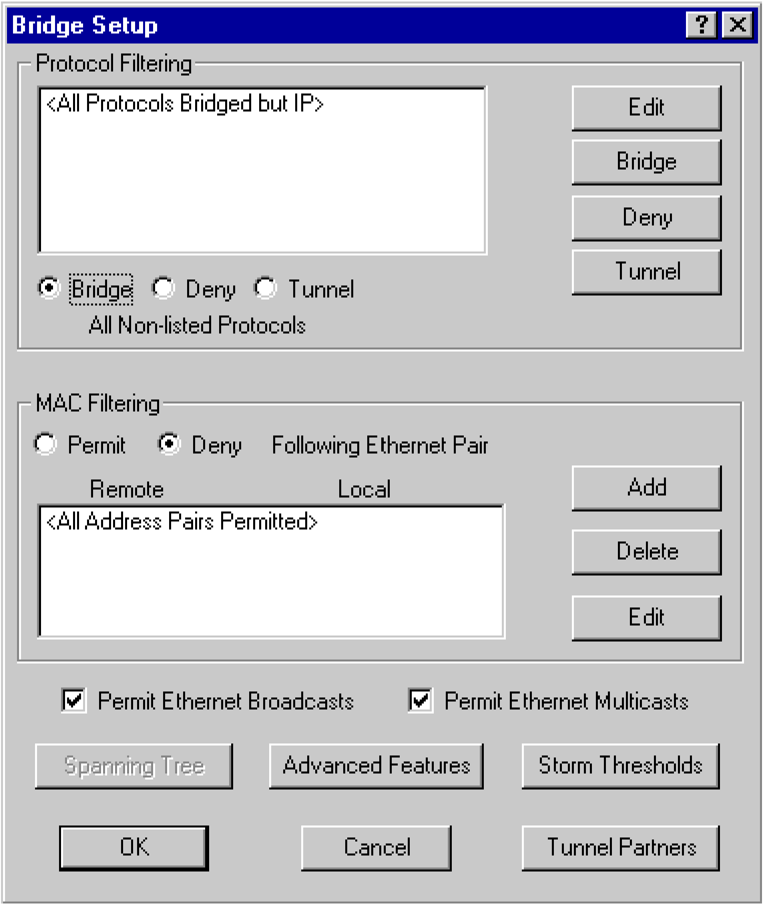
Notes:

Chapter 6
Bridging Setup



Bridge Setup

Each SPEEDLAN brouter contains an IEEE 802.3 MAC-layer bridging engine. The bridge can be configured to filter or pass any 802.3 frame type protocols, including Novell IPX, TCP/IP, AppleTalk, etc. The brouter can also be configured to filter packets by their destination and origin. This is done using the unique MAC (Media Access Control) addresses that all network interface devices have assigned to them at the factory. **Bridge Setup** is accessed from the main **Setup** menu of the SPEEDLAN Configurator.



<All Protocols Bridged but IP>

● Bridge ○ Deny ○ Tunnel
All Non-listed Protocols

○ Permit ● Deny Following Ethernet Pair

Remote Local
<All Address Pairs Permitted>

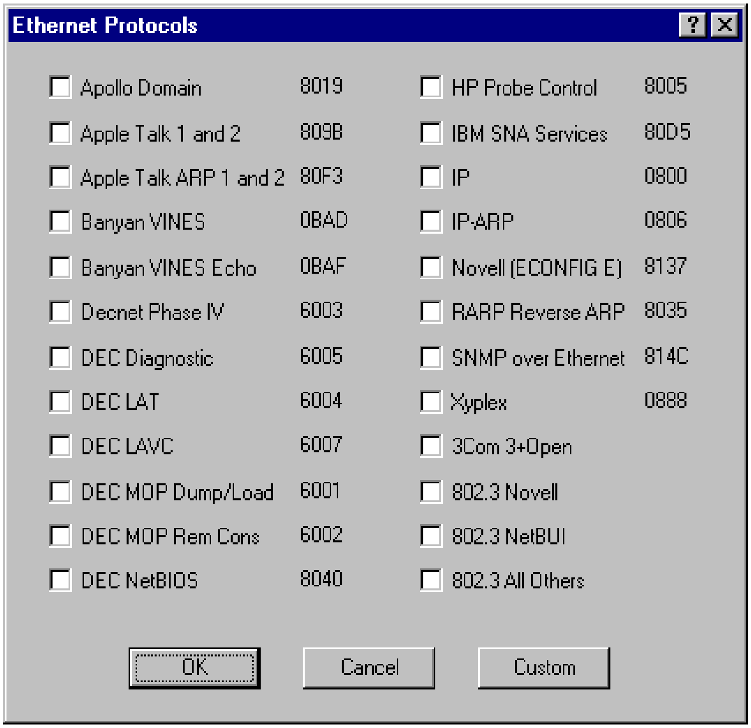
☑ Permit Ethernet Broadcasts ☑ Permit Ethernet Multicasts

Protocol Filtering

By default, the brouter is configured to pass all network protocols. When you click **Edit**, you will be presented with a list of protocols which you can select for filtering. After selecting the protocols, highlight them on this dialog box. Then, click **Bridge** or **Deny** to determine how each protocol will be treated. The radio buttons in the Protocol Filtering box determine how unselected protocols are treated.

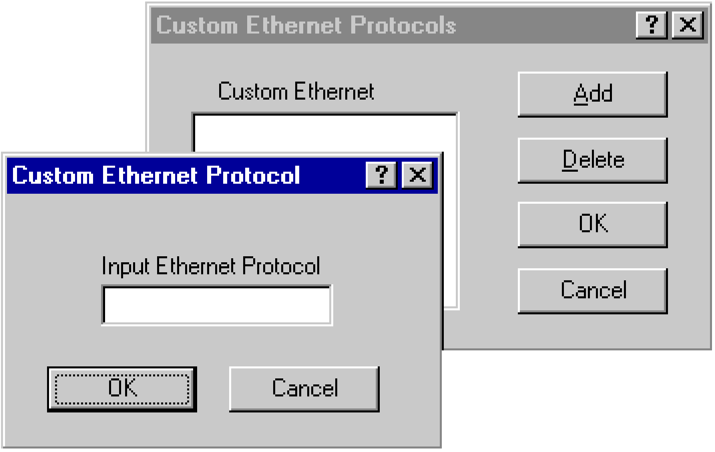
Edit Button - Ethernet Protocols

Some common Ethernet protocols and their associated ID numbers have been placed in this table. Select one from this list if you want to set a filter for it.



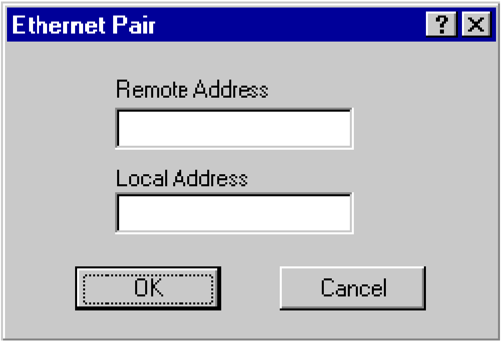
□ Apollo Domain	8019	□ HP Probe Control	8005
□ Apple Talk 1 and 2	809B	□ IBM SNA Services	80D5
□ Apple Talk ARP 1 and 2	80F3	□ IP	0800
□ Banyan VINES	0BAD	□ IP-ARP	0806
□ Banyan VINES Echo	0BAF	□ Novell (ECONFIG E)	8137
□ Decnet Phase IV	6003	□ RARP Reverse ARP	8035
□ DEC Diagnostic	6005	□ SNMP over Ethernet	814C
□ DEC LAT	6004	□ Xyplex	0888
□ DEC LAVC	6007	□ 3Com 3+Open	
□ DEC MOP Dump/Load	6001	□ 802.3 Novell	
□ DEC MOP Rem Cons	6002	□ 802.3 NetBUI	
□ DEC NetBIOS	8040	□ 802.3 All Others	

If the protocol you want to filter is not presented here, click **Custom**, **Add** and enter the hex ID for that protocol.



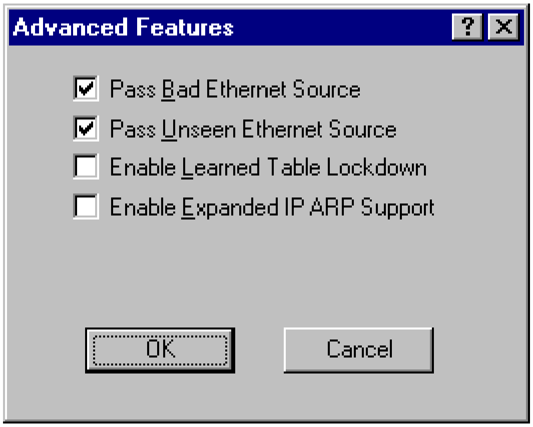
MAC Filtering

By default, the brouter is configured to pass all traffic between all MAC-Address pairs. To add an address pair into the filter, click **Add** on the MAC Filtering box. First, enter the Remote Address, which will be the MAC Address that resides on the remote side of the brouter. Second, enter the Local Address, which will be the MAC Address that resides on the local side of your connection. The local and remote interfaces are defined on either the Interface Setup or Advanced Interface Setup dialog box. It is recommended that you define the RF port as the Remote Interface (default setting).



Advanced Features Button

Clicking **Advanced** displays this dialog box. Select the appropriate check box for your network. The check boxes are described below:



☑ Pass Bad Ethernet Source
☑ Pass Unseen Ethernet Source
□ Enable Learned Table Lockdown
□ Enable Expanded IP ARP Support

- Pass Bad Ethernet Source
  The standard Ethernet bridges we have tested will pass Ethernet packets with a broadcast or multicast address as their source (i.e., packets with their first bit set to 1). The Ethernet specification for Transparent (i.e. Non-Source-Routing) bridges does not allow these types of packets, which are considered bad packets. Our studies have shown that a common failure mode of many Ethernet interfaces and networking software is to transmit packets like these. If you do not need to permit Source-Routing packets, we suggest that you deny these packets. The default setting is selected to permit these packets.
- Pass Unseen Ethernet Source
  Standard Ethernet bridges will always forward packets with destination addresses that have not been learned (i.e., have not previously been seen as a source address of a packet). This characteristic is needed in order for the Ethernet bridge to operate correctly. The downside to this, as our studies have shown, is the failure mode of many Ethernet interface cards will send out erroneous packets with good CRCs but with random Ethernet destination and source addresses. Standard bridges will permit these erroneous packets because they have not "learned" the random destination, and then add this packet's random source address to their finite learned table. This situation is not uncommon and can greatly hinder the operation of standard bridges. If you choose to deny unlearned packets, the brouter will not forward unicast packets to Ethernet addresses that have not already been seen as a source address. This scheme works for most protocols because it relies on the characteristics of most upper-layer protocols to transmit ARP requests or hello packets. **After careful testing and consideration, only qualified network engineers should select the Deny option.** The default value for this setting is selected.

- *Enable Learned-Table Lockdown*
  A standard bridge watches the source address of each packet it receives on any of its interfaces. As new addresses are seen, entries are added to the *learned table* that contains each source address and the interface number that address was received on. If a source address is later seen on a different interface, the bridge will immediately change the interface number in the learned-table entry. This condition could happen in a network that is operating well if someone moved a computer to a different part of the network. This could also happen if someone was trying to capture network packets by fooling the bridge. Enabling learned-table lockdown will prevent the interface number from being changed once the source address has been seen. A standard bridge will also time-out the learned-table records every 10 minutes. If learned-table lockdown is enabled, these records will not be timed out. Once a record is learned, it will not change or be deleted until either the bridge reboots or the learned table become completely filled and needs to be reset. (NOTE: A typical SPEEDLAN learned table can contain over 12,000 records.) The default value for this setting is disabled.

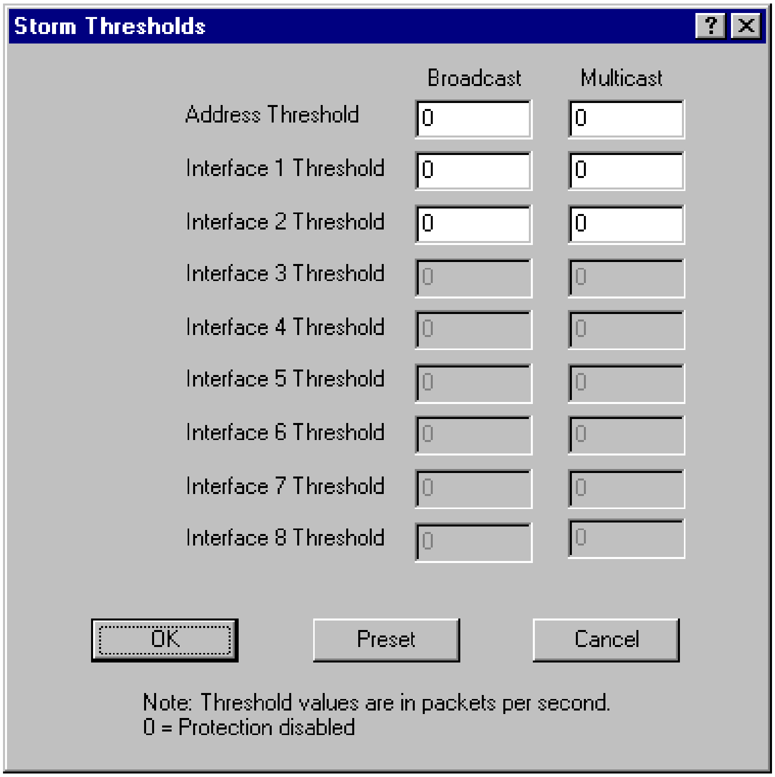
- *Enable Expanded IP ARP Support*
  Enabling this feature will cause the bridge to also watch the IP/ARP packets that occur on the network. The SPEEDLAN brouters take no action in response to IP/ARP packets (since that is the role of an IP router) except to add the IP address to its IP/ARP table. This feature is helpful on an IP network because it will build a database of MAC-layer-address-to-IP address pairs. An SNMP monitoring program, such as the SPEEDLAN Configurator, can at any time extract this information. NOTE: 1) The IP/ARP table is never timed out in this mode. 2) This feature is not available if the brouter is routing IP. The default value for this setting is disabled.

- **Permit Ethernet Broadcasts**
  Standard Ethernet bridges will always forward broadcast packets. Many protocols do not use broadcasts (e.g., AppleTalk Phase II, DECnet, and others). However, IP/ARP does use broadcasts. If you do not use IP or any other protocol that requires broadcasts, you can deny them. Shutting off broadcast packets will reduce the traffic being sent across your wireless network link. This will also greatly reduce the number of interrupts that each computer connected to your network experiences. Networks with a high number of broadcasts will slow down the processing of all attached computers, even those that aren't using the network.

- **Permit Ethernet Multicasts**
  Standard Ethernet bridges will always forward multicast packets. Some protocols do not use multicast packets, such as TCP/IP and Novell IPX. If you do not use protocols that use multicast packets, you can drop them by disabling multicast on the brouter. This will reduce the traffic that is sent across the wireless network link. In addition, it reduces the number of interrupts that each computer connected to your network experiences.

Storm Thresholds Button

Click **Storm Thresholds** to keep broadcast and multicast storms from spreading throughout the network. Network storms are common and can cause bridges, routers (brouters), workstations, servers, and PCs to slow down or crash. Storms occur if network equipment is configured incorrectly, if network software is not functioning properly, or if poorly designed programs such as network games are used. These settings are disabled by default.



	Broadcast	Multicast
Address Threshold	0	0
Interface 1 Threshold	0	0
Interface 2 Threshold	0	0
Interface 3 Threshold	0	0
Interface 4 Threshold	0	0
Interface 5 Threshold	0	0
Interface 6 Threshold	0	0
Interface 7 Threshold	0	0
Interface 8 Threshold	0	0

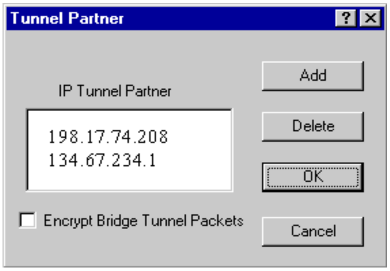
Note: Threshold values are in packets per second.
0 = Protection disabled

- **Address Threshold**
  This setting determines the maximum number of broadcast or multicast packets that can occur during a one-second period before a storm condition is declared for a particular Ethernet address (host). Once it is determined that a storm is occurring, any additional broadcast or multicast packets from that host address will be denied until the storm is determined to be over. The storm will be determined to be over when 30 seconds have passed in which every one-second period has less then the stated threshold in broadcast or multicast packets. The settings for broadcast packets and multicast packets are configured independently.

- **Interface Threshold**
  This setting determines the maximum number of broadcast or multicast packets that can occur during a one-second period before a storm is declared for the assigned interface. Once it is determined that a storm is occurring, any additional broadcast or multicast packets received on that interface will be denied until the storm is determined to be over. The storm will be determined to be over once a one-second period has occurred with no broadcast or multicast packets received on that interface. The settings for broadcast packets and multicast packets are configured independently.
- **Preset Button**
  This button sets the broadcast and multicast storm thresholds to the recommended values. These values have been determined to offer good protection without interfering with the operation of the typical network. These values may need to be tuned for your particular network.

Tunnel Partners Button

Click **Tunnel Partners** to encapsulate Ethernet packets received from the local interface in an IP/UDP packet and then send them to one or more tunnel partners. Tunneling can be used to set up virtual Ethernet networks. In the General Setup dialog box, if the **Remote Bridging using IP Tunnels** is enabled, Tunnel Partners can be set up. This dialog box specifies the IP addresses of each of the bridge/routers that are to participate in the tunnel group. Specify the addresses of all the bridges that are participating in the tunnel group but **DO NOT** specify the IP addresses on this brouter.



Tunnel Partner

IP Tunnel Partner

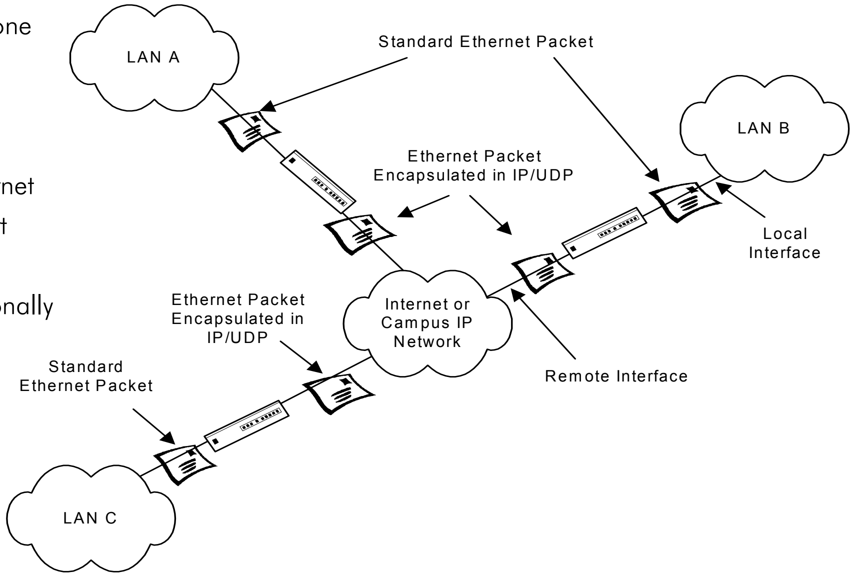
198.17.74.208
134.67.234.1

☐ Encrypt Bridge Tunnel Packets

- **Encrypt Bridge Tunnel Packets**
  If purchased, a brouter (from Wave Wireless) may contain a special software-encryption algorithm that is distinct from the optional SPEEDLAN encryption chip on the brouter. If **Data Encryption** is enabled on the General Setup dialog box and if an Encryption Key is set up in the Data Encryption menu, enabling encryption here will cause all Ethernet packets transmitted to tunnel partners to be encrypted and encapsulated inside IP packets. The IP packet itself cannot be encrypted because industry-standard IP routers, like those on the Internet, would not be able to forward the encrypted packets.

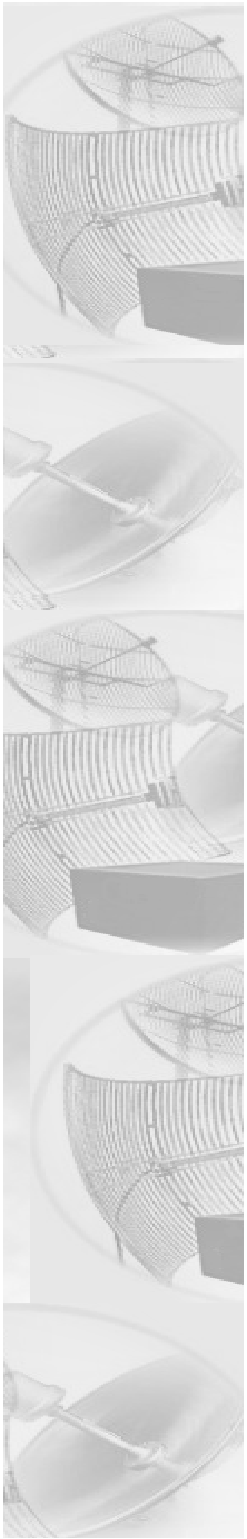
The three brouters are set up to tunnel one or more protocols and each is a tunnel partner to the other two brouters. This configuration allows LAN A, LAN B, and LAN C to become a virtual private Ethernet network with the Internet as the transport mechanism for data between them. The encapsulated data packets can be optionally encrypted to make the virtual private network more secure.

Generic Ethernet Tunneling (Through an IP Network)


LAN A
Standard Ethernet Packet
LAN B
Ethernet Packet Encapsulated in IP/UDP
Local Interface
Ethernet Packet Encapsulated in IP/UDP
Internet or Campus IP Network
Standard Ethernet Packet
Remote Interface
LAN C

Notes:

Chapter 7
Setting Up the IP Addresses
(IP Host Setup)



If you do not understand the basics of IP addressing, DHCP, or NAT, please read the next section, Part I - Quick Overview of IP Addressing, below. Otherwise, skip to *Part II - Setting Up the IP Address, page 7-13*.

Part I - Quick Overview of IP Addressing

IP Addressing is important because it tells the network how to locate the computers or network equipment connected to it. IP addresses are given so each computer or equipment on the network contains a unique address. In addition, network addresses and node addresses, depending on the Class (A, B, C, etc.), contain their own unique address as well. IP addressing provides the following information:

- Provides communication between different platforms and diverse systems
- Provides universal data transfer over large geographic distances
- Has been "adopted" as a standard in the computer industry

What is an IP address?

An IP address contains 32 bits of information, which is divided into the following:

- Two sections: the network address and the node address (also known as the host address)
- To keep it simple, lets call it four bytes (octets)

Note: Each octet contains 8 bits, which are equivalent to 1 byte. Each octet is separated by a period (.).

The following examples show the conversion of the same IP address into several different formats:

- Decimal (130.57.30.56)
- Hexadecimal (82.39.1E.38)
- Binary (10000010.00111001.00011110.00111000).

Internet Address Classes

The first octet defines the "class" of the address, which is the only method to tell the size of the network (how big) and where the internet address belongs. There are three main classes:

- Class A: 35.**0.0.0**
- Class B: 128.5.**0.0**
- Class C: 192.33.33.**0**

-non-bolded text = Part of network address

-bolded text = Part of local address (node section)

This definition is not random; it is based on the fact that routers, by reading just the first three bits of the address field, designate which network class it belongs to. This selection simplifies the way routers handle the messages (packets) and speed up the forwarding process.

In fact, IP defines five classes:

- **Class A** addresses use 8 bits (1 octet) for the network portion and 24 bits (3 octets) for the node (or host) section of the address. This provides up to 128 networks with 16.7 million nodes for each network.
  - First byte is assigned as network address
  - Remaining bytes used for node addresses
  - Format: network, node, node, node
  - In IP address 49.22.102.70, "49" is network address and "22.102.70" is the node address—all machines on this network have the "49" network address assigned to them
  - Maximum of 224 or 16,777,216 nodes

- **Class B** addresses use 16 bits (two octets) for the network portion and 16 bits for the node (or host) section of the address. This provides up to 16, 384 networks with 64,534 nodes for each network.
  - First two bytes are assigned as network address
  - Remaining bytes used for node addresses
  - Format: network, network, node, node
  - In IP address 130.57.30.56, "130.57" is the network address, and "30.56" is the node address
  - Maximum of 216 or a total of 65,534 nodes

- **Class C** addresses use 24 bits (3 octets) for the network portion and 8 bits (two octets) for the node (or host) section of the address. This provides 16.7 million networks with 256 nodes for each network.
  - First three bytes are assigned as network address
  - Remaining byte used for node address
  - Format: network, network, network, node
  - In IP address 198.21.74.102, "198.21.74" is the network address, and "102" is the node address
  - Maximum of 28 or 254 node addresses

- Class D
    - Range is 224.0.0.0 to 239.255.255.255
    - Used for multicast packets (i.e., host sends out router discovery packets to learn all of the routers on the network)

- Class E
    - Range is 240.0.0.0 to 255.255.255.255
    - Reserved for future use

Note: Class D & E **should NOT** be assigned to net assignment of IP addresses. In addition, the first octet, 127, is reserved. In each network definition, the first node number (i.e., "0") is used to define the network, as well as the last number (i.e., "255"). The last number is known as the broadcast address.

Public IP addresses can be obtained from the following address:

Network Solutions
InterNIC Registration Services
505 Huntmar Park Drive
Herndon, VA 22070
hostmaster@internic.net

Note: Non-public addresses can include a network address assigned from the network administrator or from the IP provider. Also, there is one network in each class that is defined for private use, allowing the creation of internal networks. These addresses are Class A: 10.0.0.0, Class B: 172.10.0.0, and Class C: 192.168.0.0.

Subnetting a Network

The increasing number of hosts and networks make impractical address blocks that are not smaller than 245. In order keep the IP address small, so routers can manage them without changing the whole protocol, a smaller network definition is created. This is called a subnet. Subnets are intended to:

- Reduce network traffic
- Optimize performance
- Simplify management
- Create more effective and efficient addresses for large geographic distances

Default Subnet masks

- Class A: **255**.0.0.0
- Class B: **255.255**.0.0
- Class C: **255.255.255**.0

Note: Subnet mask is bolded.

What is a Subnet?

Subnetting allows you to create multiple networks within one Class A, B, or C network. Each data link (octet) contains its own unique identifier also known as the subnet. Also, each node on the same data link must belong on the same subnet as well.

What is a Subnet Mask?

A subnet mask allows you to mask section(s) (depending on the class specified) of the octets in the network address. Each octet used in the subnet mask is assigned to a data link. The leftover octet(s) are assigned to the remaining nodes.

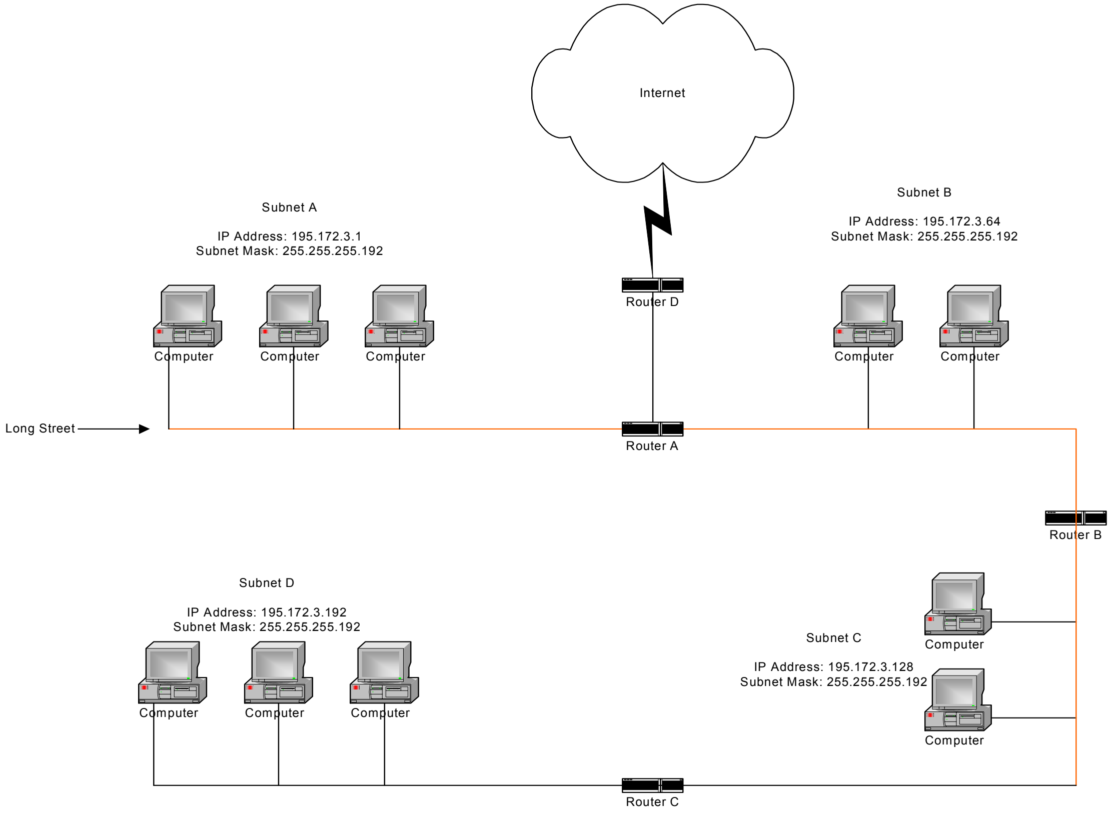
For more information on subnetting, see the example below and *Diagram of Subnetting a Network, page 7-7*.

Example of Subnetting:

For example, a Class C network (255.255.255.0) contains three masked octets (255.255.255). The last octet (0) is leftover for remaining nodes (i.e., computers).

If Router D is reading IP Addresses 195.172.3.1 (let's call this IP Address 1) and 195.172.3.64 (let's call this IP Address 2) on this Class C network, it would send IP Address 1 to Subnet A and IP Address 2 to Subnet B. The remaining nodes in each subnet (A through D) on this network can contain up to 254 pieces of network equipment (computers, printers, fax machines, bridges or routers, etc.).

Diagram of Subnetting a Network



Still confused?

An easier method to explain this concept is to use the classic "mailing" analogy used in IP addressing. Consider that this network, called Long Street, is four blocks long. There are 254 houses on Long Street, and each block contains 64 houses. Houses 1 to 63 reside on Block A. Houses 64 to 127 reside on Block B. Houses 128 to 191 reside on Block C. Houses 192 to 254 reside on Block D. Think of each block as a subnet. This means that Blocks A, B, C, and D are all part of Long Street, which is also known as the network in this example. The mailman would organize the letters (or IP addresses for network equipment) by creating four piles (one for each block, or subnet). As soon as the mailman picks up pile A in his hand, he knows which block to turn on. This same reasoning applies to piles B, C, and D as well. Router D knows exactly which subnet to transfer (or turn) the packets to by reading its IP and subnet mask address. Note that each subnet on this network is 255.255.255.192. Why is 192 the last octet in the subnet mask and not 64? The last octet, 192, is the mask that allows 64 "houses" to know that the mailman (or router) is coming in advance. The "houses" will know it's mailman "Jim" by looking at the IP number.

Note: If the network is managed by a Simple Network Management Protocol for local or Internet access, each brouter must contain a unique IP Address. This is a benefit of static or dynamic addressing.

How does a network administrator assign an IP address?

IP addresses are supplied by the network administrator, the ISP, or hosting company.

The two types of IP addressing—manual (static) and automatic (dynamic) addressing—are described below.

- Manual (static) Addressing
  Each device connected to the Internet must have its own unique IP address. Also, if a computer is being used as a server, you will assign it a permanent IP address. This enables other computers to connect to it. Static addressing is also beneficial to users that need to maintain a "constant" connection to the Internet. This will enable users to easily access the IP address.
- Automatic (dynamic) Addressing
  A DHCP (Dynamic Host Configuration Protocol) server assigns the IP address to each computer as the computer connects to the network. If a computer moves to a new network (i.e., great for temporary employees or mobile users), it must be assigned a new IP address for that network. DHCP can be used to manage these assignments automatically. DHCP is described in further detail below.

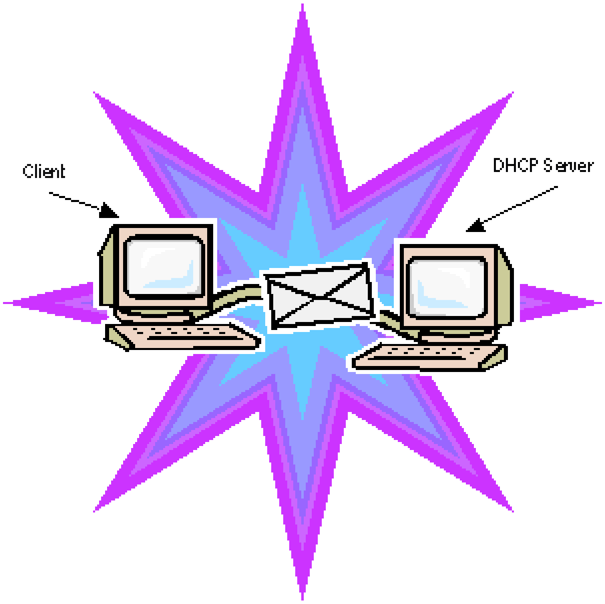
What is DHCP?

Dynamic Host Configuration Protocol (DHCP) allows network administrators to assign dynamic IP addresses for the period of time needed to connect to the Internet. Think of DHCP as leasing an apartment. A prospective tenant may not need to live in an apartment for two years, maybe just a year. Therefore, the tenant will only sign a one-year lease agreement. For example, each time a computer is set up to connect to the Internet, the network administrator uses DHCP to automatically assign the computer a unique IP address. That computer will give up its IP address when it is no longer needed (when the lease has ended) allowing new a computer (or a new tenant) on the same network to use it. This benefits educational and corporate settings where users often log on to different computers. In this case more IP addresses outnumber computers because you can quickly reconfigure the network if needed from a centralized location.

Servers that utilize DHCP resolve security issues, costly IP addressing services, and compatibility problems. DHCP is an alternative to BOOTP, which reduces the agony of assigning static IP addresses and also provides advanced configuration options.

Note: The figure on the next page may help you understand how DHCP assigns an IP address.

Figure of DHCP Addressing



1 The client asks DHCP server for IP address and configuration if needed.

2 The DHCP server assigns an available IP address to client.

3 The client takes IP address from DHCP server and requests any additional configuration needed.

4 DHCP server confirms IP address and configuration.

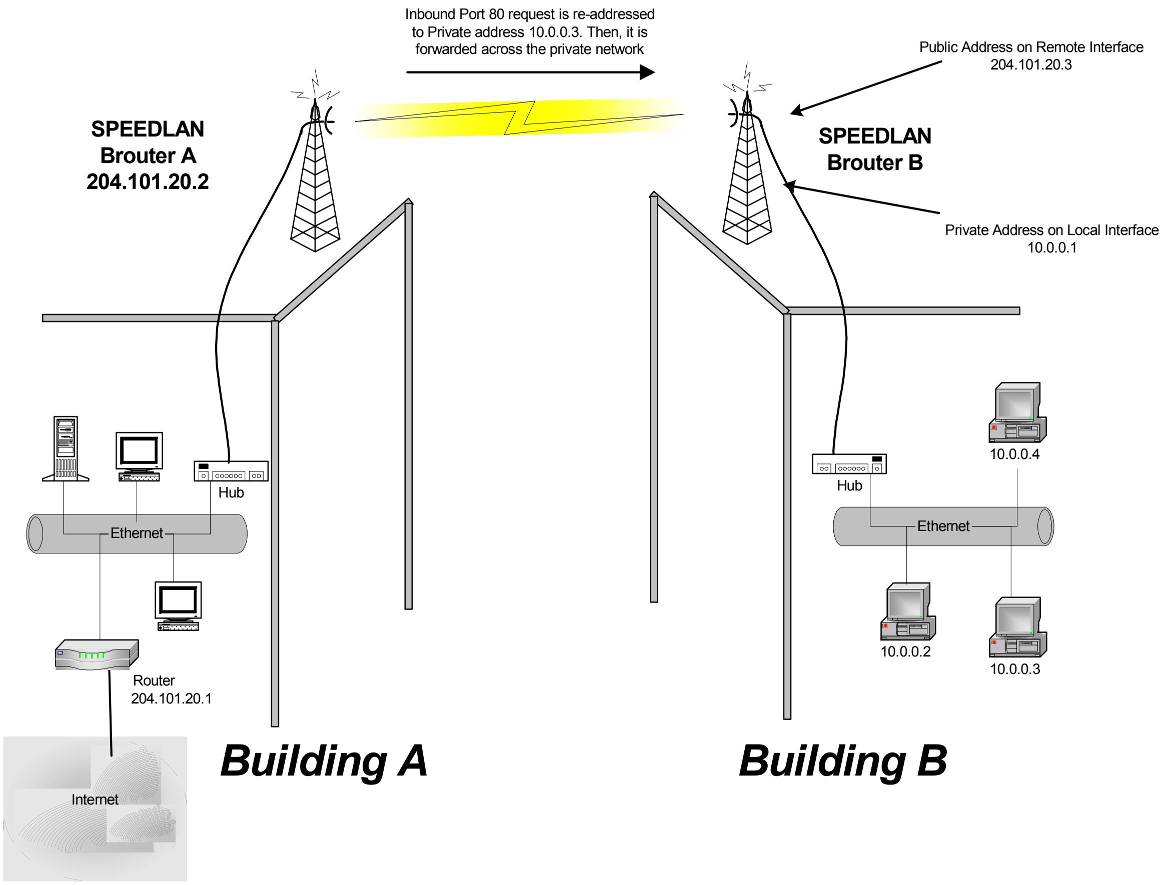
What is NAT?

Network Address Translation (NAT) is the conversion of an Internet Protocol address (IP address) used within one network to a different IP address within another network. One network is designated the inside network and the other is the outside network.

Network Address Translation (NAT) occurs when there is a translation among an Internet Protocol (IP address) used within one network (designated as inside network) to a different IP addresses within another network (designated as outside network). Network Address Translators (NATs) allow companies to decrease the number of global IP addresses. This enables companies to communicate with other devices on the Internet using a single IP address (or more than one IP address).

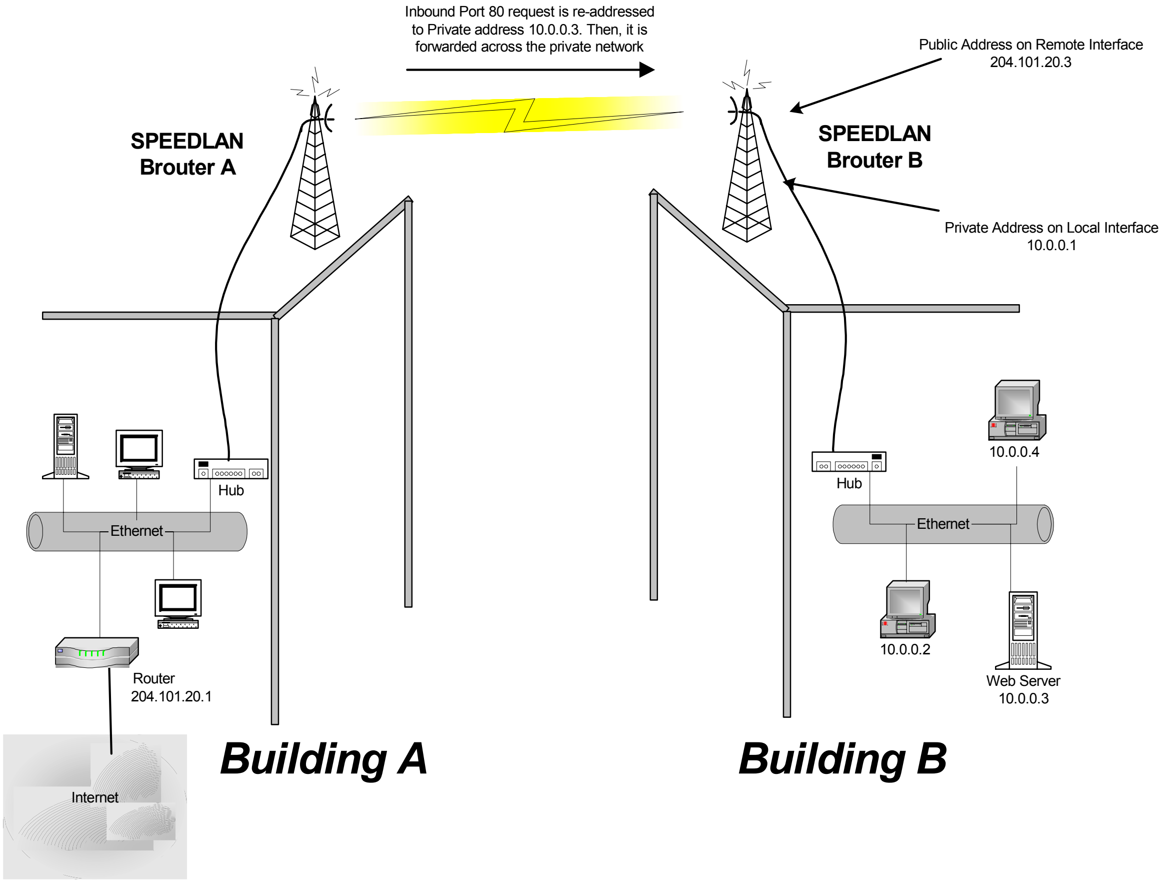
For example, a company can provide its clients with one IP address, allowing access to the company's firewall only. This IP address is not a "real" address on the company's internal network, but it is successfully translated to the correct IP location through NAT (i.e., NAT router). Therefore, the company controls access through firewalls and provides multiple IP addresses to outside customers without excessive limited resources, or "global" Internet IP protocols.

Diagram of Outgoing NAT


Inbound Port 80 request is re-addressed to Private address 10.0.0.3. Then, it is forwarded across the private network
Public Address on Remote Interface 204.101.20.3
SPEEDLAN Brouter A 204.101.20.2
SPEEDLAN Brouter B
Private Address on Local Interface 10.0.0.1
Hub
Ethernet
Router 204.101.20.1
Internet
Building A
Building B
Hub
Ethernet
10.0.0.4
10.0.0.2
10.0.0.3

As the packet is transmitted from the private network (in Building B) across the public network (Building A and the Internet), the packet will be re-addressed as 204.101.20.3, also known as the public address. When the packet returns to SPEEDLAN B, the packet will be re-addressed to the IP address of the private network by using the MAC address contained in the header to identify the destination.

Diagram of Incoming NAT


Inbound Port 80 request is re-addressed to Private address 10.0.0.3. Then, it is forwarded across the private network
Public Address on Remote Interface 204.101.20.3
SPEEDLAN Brouter A
SPEEDLAN Brouter B
Private Address on Local Interface 10.0.0.1
10.0.0.4
Hub
Hub
Ethernet
Ethernet
Router 204.101.20.1
10.0.0.2
Web Server 10.0.0.3
Internet
Building A
Building B

Incoming NAT allows you to specify ports on the private network that you would like to be available on the public network. For example, if a web server is being hosted on a public network in Building B (IP Address 10.0.0.3), you can create a pair that will specify that all requests on the public IP address, Port 80, be forwarded to IP Address 10.0.0.3 on the private IP address, Port 80.

Part II - Setting Up the IP Address

The following section discusses DHCP client (and interface), DHCP Server, Static IP addresses, and Outgoing and Incoming NAT.

Note: Before you begin, confirm that you have properly read the configuration from the SPEEDLAN brouter you want to configure. Then, perform the following tasks: Open the SPEEDLAN Configurator. From the **File** menu, choose **Open Remote Config**.... Then, click **Scan**. The Scan dialog box appears. Select the appropriate brouter and click **OK**. Click **OK** again. A message box appears confirming that the "Configuration has been read from the Bridge" (i.e., 128.104.224.1). Click **OK**.

To set up the IP address, do ONE of the following:

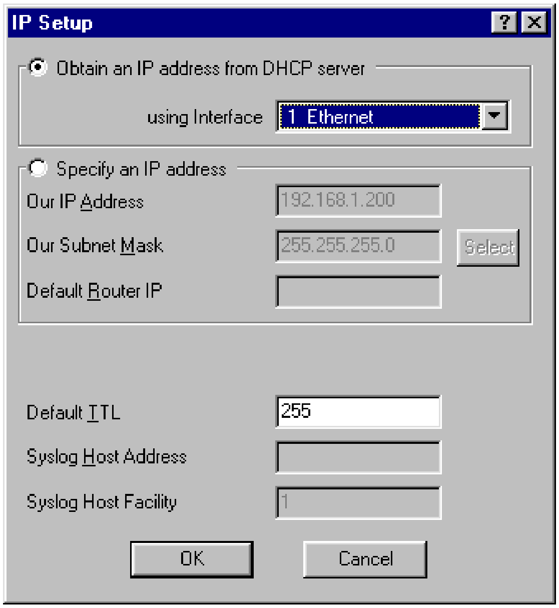
- Enable DHCP client for dynamic addressing. For more information, see *Enabling the DHCP Client and Choosing the Appropriate Interface, page 7-14*, **OR**
- Assign a static IP address. For more information, see *Assigning a Static IP Address, page 7-18*.

Enabling the DHCP Client and Choosing the Appropriate Interface

Note: Before you begin, confirm that you have properly read the configuration from the SPEEDLAN brouter you want to configure. Then, perform the following tasks: Open the SPEEDLAN Configurator. From the **File** menu, choose **Open Remote Config**.... Then, click **Scan**. The Scan dialog box appears. Select the appropriate brouter and click **OK**. Click **OK** again. A message box appears confirming that the "Configuration has been read from the Bridge" (i.e., 128.104.224.1). Click **OK**.

To enable the DHCP client and choose the appropriate interface, do the following:

1 From the **Setup** menu, choose **IP Setup**. The IP Setup dialog box appears.



IP Setup

● Obtain an IP address from DHCP server

using Interface: 1 Ethernet

○ Specify an IP address

Our IP Address: 192.168.1.200

Our Subnet Mask: 255.255.255.0

Default Router IP:

Default TTL: 255

Syslog Host Address:

Syslog Host Facility: 1

2 Select the **Obtain an IP address from DHCP Server** option.

3 Next, select the interface for Ethernet or wireless network from the **Using Interface** drop-down list. Make sure that you select the interface where the DHCP server is located.

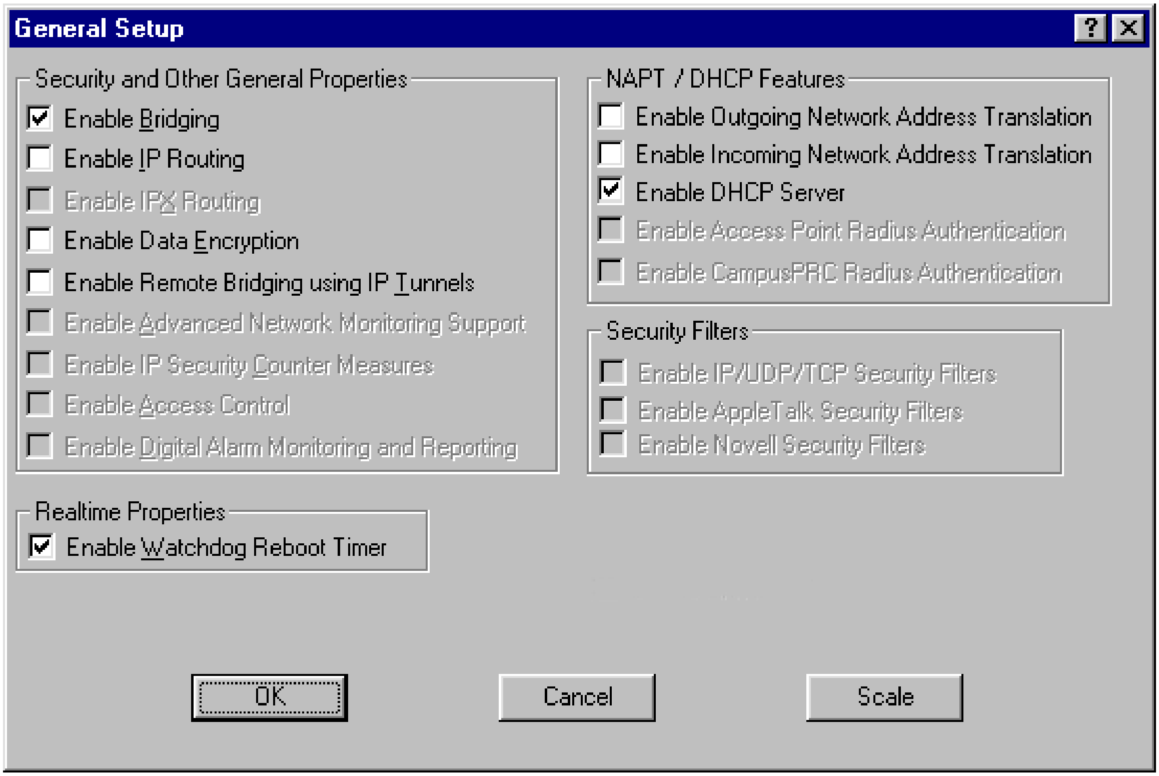
Note: The information for Default TTL should already be entered. The IP host on the Internet sends out each packet with a default "Time to Live" parameter. If you want to override the factory default of 64 attempts, you can specify your new default here. **This parameter should not be changed less you are very familiar with IP functionality and how the Time to Live parameter will affect how packets are treated by your network, as well as the network to which you are bridged (or routed).**

Enabling the DHCP Server on the SPEEDLAN

Note: Before you begin, confirm that you have properly read the configuration from the SPEEDLAN brouter you want to configure. Then, perform the following tasks: Open the SPEEDLAN Configurator. From the **File** menu, choose **Open Remote Config**.... Then, click **Scan**. The Scan dialog box appears. Select the appropriate brouter and click **OK**. Click **OK** again. A message box appears confirming that the "Configuration has been read from the Bridge" (i.e., 128.104.224.1). Click **OK**.

To enable the DHCP Server on the SPEEDLAN, do the following:

1 From the **Setup** menu, choose **General Setup**. The General Setup dialog box appears.



General Setup

Security and Other General Properties

☑ Enable Bridging
□ Enable IP Routing
□ Enable IPX Routing
□ Enable Data Encryption
□ Enable Remote Bridging using IP Tunnels
□ Enable Advanced Network Monitoring Support
□ Enable IP Security Counter Measures
□ Enable Access Control
□ Enable Digital Alarm Monitoring and Reporting

NAPT / DHCP Features

□ Enable Outgoing Network Address Translation
□ Enable Incoming Network Address Translation
☑ Enable DHCP Server
□ Enable Access Point Radius Authentication
□ Enable CampusPRC Radius Authentication

Security Filters

□ Enable IP/UDP/TCP Security Filters
□ Enable AppleTalk Security Filters
□ Enable Novell Security Filters

Realtime Properties

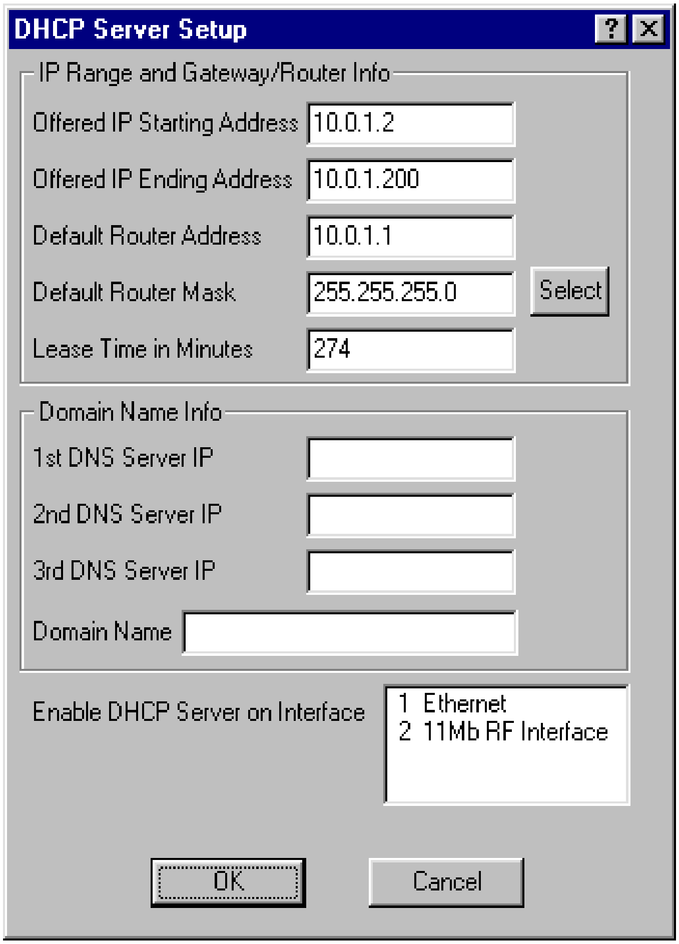
☑ Enable Watchdog Reboot Timer

2 Select the **Enable DHCP Server** check box; this will enable you to set up the DHCP Server.

Note: You do not need to enable NAT (Outgoing and Incoming) in order to use SPEEDLAN's DHCP Server. Please read the sections of this manual describing those options carefully before enabling either NAT feature.

- **Enable Outgoing Network Address Translation**
  This feature enables a company to map the private networks IP addresses into one or more global public network IP addresses. This means that outsiders will only view the single (or more if designated) IP network address assigned for global viewing on the Internet. For more information, see *Outgoing NAT, page 7-20*.
- **Enable Incoming Network Address Translation**
  This feature enables a company to unmap public network IP address into private network IP addresses. For more information, see *Incoming NAT, page 7-22*.

3 From the **Setup** menu, choose **DHCP Server Setup**. The DHCP Server Setup dialog box appears.



DHCP Server Setup

IP Range and Gateway/Router Info

Offered IP Starting Address: 10.0.1.2

Offered IP Ending Address: 10.0.1.200

Default Router Address: 10.0.1.1

Default Router Mask: 255.255.255.0

Lease Time in Minutes: 274

Domain Name Info

1st DNS Server IP:

2nd DNS Server IP:

3rd DNS Server IP:

Domain Name:

Enable DHCP Server on Interface:
1 Ethernet
2 11Mb RF Interface

4 Enter the IP range and gateway/router information:

- **Offered IP Starting Address**
  This is the start of the block of allowed IP addresses.

- **Offered IP Ending Address**
  This is the end of the block of allowed IP addresses.
- **Default Router Address**
  This is the subnet mask of the default router.
- **Default Router Mask**
  This is the router that initially accepts or transfers packet to the directly connected networks or static networks.
- **Lease Time in Minutes**
  This is the amount of minutes that the computer can use the assigned IP address. When the time is up, the IP address will revert to the pool of available addresses and can be reassigned to another computer. The maximum time is 300 minutes.

Note: Click **Select** to view the IP Mask List. Select the appropriate IP Mask and click **OK**.

5 Enter the domain name information:

- **1st DNS Server IP**
  This setting will specify the client's first DNS Server.
- **2nd DNS Server IP**
  This setting will specify the client's secondary DNS server.
- **3rd DNS Server IP**
  If needed, this setting will specify the client's third DNS server.
- **Domain Name**
  This is the web domain name of the organization on the Internet such as "www.speedlan.com". It is not necessary to use the first portion of the domain name leaving the entry as "Speedlan.com".

6 Select the interface on which you want to Enable DHCP (i.e., Ethernet or wireless interface). Note: If the requests for an IP address will be received through the wired Ethernet interface, select **#1 Ethernet. If the requests will be received through RF interface from a remote PC, select #2 11 Mb RF Interface.**

7 Click **OK**.

8 After you have finished entering the appropriate information, click **OK**.

9 Now save the changes to the brouter. From the **File** menu, choose **Save Config**.

10 A message box appears informing you that the information will be saved to the bridge or router. Click **Yes**.

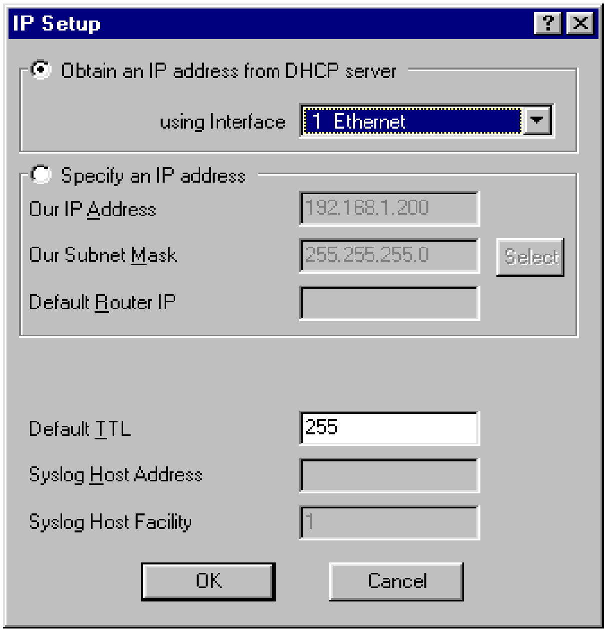
11 The Configurator confirms that the configuration has been saved. Click **OK**. The SPEEDLAN ISP shelfmount brouters will automatically reboot at this point.

Assigning a Static IP Address

Note: Before you begin, confirm that you have properly read the configuration from the SPEEDLAN brouter you want to configure. Then, perform the following tasks: Open the SPEEDLAN Configurator. From the **File** menu, choose **Open Remote Config**.... Then, click **Scan**. The Scan dialog box appears. Select the appropriate brouter and click **OK**. Click **OK** again. A message box appears confirming that the "Configuration has been read from the Bridge" (i.e., 128.104.224.1). Click **OK**.

To physically assign a static IP address, do the following:

1 From the **Setup** menu, choose **IP Setup**. The IP Setup dialog box appears.



IP Setup

● Obtain an IP address from DHCP server

using Interface: 1 Ethernet

○ Specify an IP address

Our IP Address: 192.168.1.200

Our Subnet Mask: 255.255.255.0

Default Router IP:

Default TTL: 255

Syslog Host Address:

Syslog Host Facility: 1

2 Select the **Specify an IP address** option. Enter the following information:

- **Our IP Address**
  The unique number assigned by the network administrator, ISP or host provider. This tells network the location (IP address) of this device on the Internet (i.e., 128.104.224.1).
- **Our Subnet Mask**
  This term allows network administrators to mask section(s) (depending on the class specified) of the octets in the network address. Each octet used in the subnet mask is assigned to a data link. The leftover octet(s) are assigned to the remaining nodes.

Note: For more information, see *Subnetting a Network, page 7-5*. Once the packet has traveled to the appropriate network, it goes through a masking process. A subnet mask is composed of zeros (0s) and ones (1s). This tells the router which addresses to look under and which ones not to look under. Therefore, subnet masking allows the router to transfer the packet traffic more quickly than a network without a subnet. Again, this address is obtained from the network administrator, IP host, or host provider.

- **Default Router IP**
  If you have an established network, use the IP address for the router already set up for that network. If you do not have an established network, leave this entry blank.
- **Default TTL**
  This information should already be entered. The IP host on the Internet will send out each packet with a default "Time to Live" parameter. If you want to override the factory default of 64 attempts, you can specify your new default here. This parameter should not be changed unless you are very familiar with IP functionality and how the Time to Live parameter will affect how packets are treated by your network, as well as the network to which you are bridged (or routed).

Note: Click **Select** to view the IP Mask List. Select the appropriate IP Mask and click **OK**.

3 After you have finished entering the appropriate information, click **OK**.

4 Now save the changes to the brouter. From the **File** menu, choose **Save Config**.

5 A message box appears informing you that the information will be saved to the brouter (i.e., 128.104.22.4). Click **Yes**.

6 The Configurator confirms that the configuration has been saved. Click **OK**. The computer will reboot at this point.

Note: If you want to set up NAT, see *Part III - Setting Up NAT, page 7-20*.

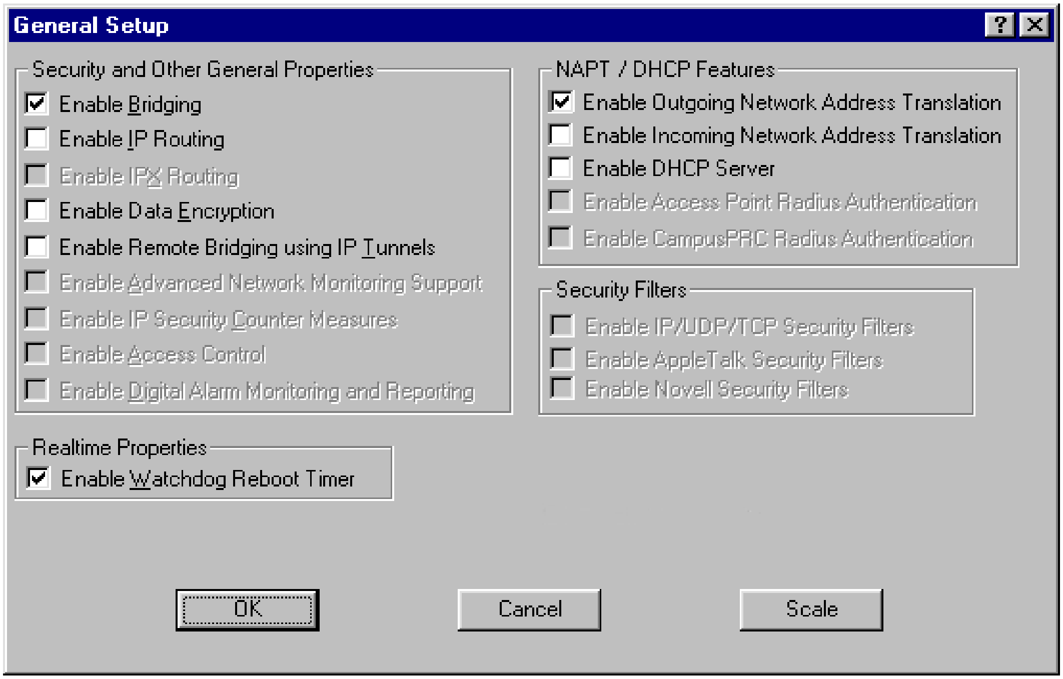
Part III - Setting Up NAT

This section explains how to setup outgoing and incoming Network Address Translation (NAT). For more information on outgoing and incoming NAT, see *Diagram of Outgoing NAT, page 7-11* and *Diagram of Incoming NAT, page 7-12*.

Outgoing NAT

To setup outgoing NAT, do the following:

1 From the **Setup** menu, choose **General Setup**. The General Setup dialog box appears.



General Setup

Security and Other General Properties

☑ Enable Bridging
□ Enable IP Routing
□ Enable IPX Routing
□ Enable Data Encryption
□ Enable Remote Bridging using IP Tunnels
□ Enable Advanced Network Monitoring Support
□ Enable IP Security Counter Measures
□ Enable Access Control
□ Enable Digital Alarm Monitoring and Reporting

NAPT / DHCP Features

☑ Enable Outgoing Network Address Translation
□ Enable Incoming Network Address Translation
□ Enable DHCP Server
□ Enable Access Point Radius Authentication
□ Enable CampusPRC Radius Authentication

Security Filters

□ Enable IP/UDP/TCP Security Filters
□ Enable AppleTalk Security Filters
□ Enable Novell Security Filters

Realtime Properties

☑ Enable Watchdog Reboot Timer

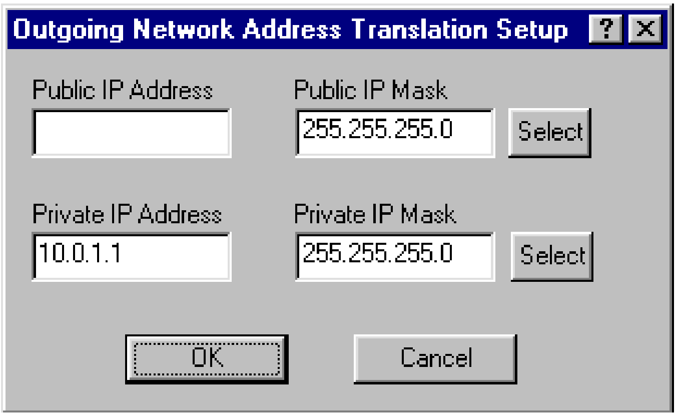
2 Select the **Enable Outgoing Network Address Translation** check box. Click **OK**.

3 From the **Setup** menu, choose **Outgoing Network Address Translation Setup**.

4 The Outgoing Address Translation Setup dialog box appears.

Note: NAT is a useful tool that will be enabled the majority of the time on the remote side of the wireless connection. It is rarely enabled on the base station. NAT is also useful to have private networks connected to public networks (i.e., the Internet) without needed a public IP address for every node. By using only one public IP address, NAT controls who in the private network made a request to an address in the public network.
This translates the IP addresses from one side to another, hiding the private network

from the public. This means that the public will view only one public and valid IP address.



Public IP Address

Public IP Mask 255.255.255.0

Private IP Address 10.0.1.1

Private IP Mask 255.255.255.0

5 Enter the appropriate outgoing information:

- **Public IP Address**
  This is the IP address for the outside network. If you have more than one public address, you can assign it to node on a private network (One-to-One NAT). Therefore, all requests for a particular IP address from the outside or public network will be translated to the appropriate private IP address. This may be necessary if you have a server or workstation (host) that needs to be connected to a remote network.
- **Private IP Address**
  This is the IP address for the inside or private network only, which hides behind the Public IP address.
- **Public IP Mask**
  This address assigns the Subnet mask to the Public (Ethernet) portion of the SPEEDLAN brouter.
- **Private IP Mask**
  This address assigns the Subnet mask to the private network interface.

Note: Click **Select** to view the IP Mask List. Select the appropriate IP Mask and click **OK**.

6 Click **OK**.

7 After you have finished entering the appropriate information, click **OK**.

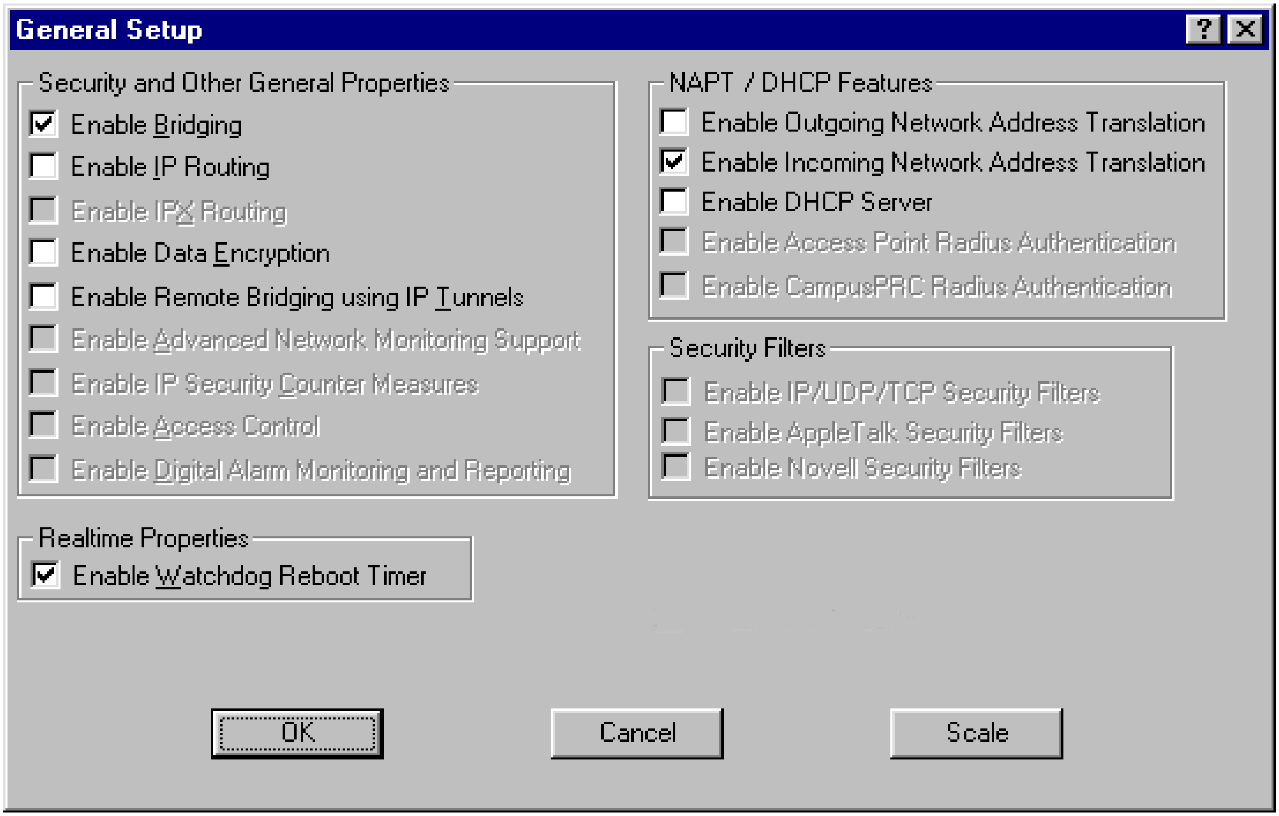
8 Now save the changes to the bridge or router. From the **File** menu, choose **Save Config**.

9 A message box appears informing you that the information will be saved to the bridge or router. Click **Yes**. The Configurator confirms that the configuration has been saved. Click **OK**. The SPEEDLAN ISP shelfmount brouters will automatically reboot at this point.

Incoming NAT

To set up incoming IP network address for NAT, do the following:

1 From the **Setup** menu, choose **General Setup**. The General Setup dialog box appears.



General Setup

Security and Other General Properties
☑ Enable Bridging
□ Enable IP Routing
□ Enable IPX Routing
□ Enable Data Encryption
□ Enable Remote Bridging using IP Tunnels
□ Enable Advanced Network Monitoring Support
□ Enable IP Security Counter Measures
□ Enable Access Control
□ Enable Digital Alarm Monitoring and Reporting

NAPT / DHCP Features
□ Enable Outgoing Network Address Translation
☑ Enable Incoming Network Address Translation
□ Enable DHCP Server
□ Enable Access Point Radius Authentication
□ Enable CampusPRC Radius Authentication

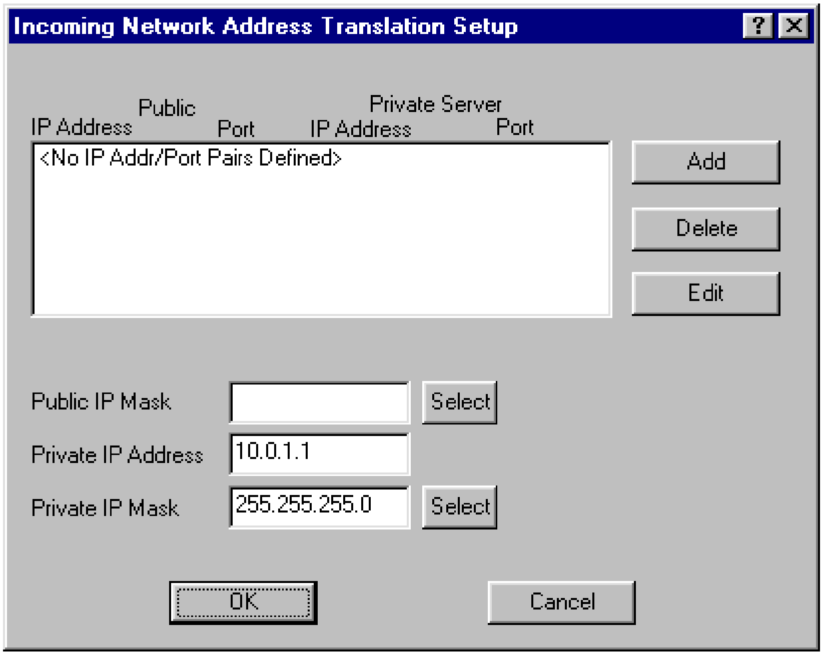
Security Filters
□ Enable IP/UDP/TCP Security Filters
□ Enable AppleTalk Security Filters
□ Enable Novell Security Filters

Realtime Properties
☑ Enable Watchdog Reboot Timer

2 Select the **Enable Incoming Network Address Translation** check box. Click **OK**.

3 From the **Setup** menu, choose **Incoming Network Address Translation Setup**.

4 The Incoming Address Translation Setup dialog box appears.



<No IP Addr/Port Pairs Defined>

Public IP Mask:

Private IP Address: 10.0.1.1

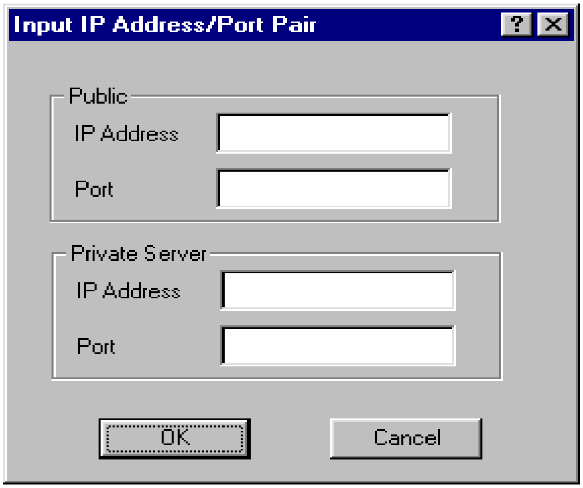
Private IP Mask: 255.255.255.0

5 Enter the appropriate incoming information:

- **Public IP Address**
  This is the IP address for the outside network. If you have more than one public address, you can assign it to a node on the private network (One-to-One NAT). Therefore, all requests for a particular IP address from the outside or public network will be translated to the appropriate private IP address. This may be necessary if you have a server or workstation (or computer) that needs to be connected to a remote network.
- **Private IP Address**
  This is the IP address for the inside network only, which hides behind the public IP address.
- **Private IP Mask**
  This address assigns the Subnet mask to the private network interface.

Note: Click **Select** to view the IP Mask List. Select the appropriate IP Mask and click **OK**.

6 Click **Add** to enter another IP address/port pair. The Input IP Address/Port Pair dialog box appears.



7 Then enter the following information as appropriate. Then, click **OK** to close this dialog box.

- **Public IP Address**
  This is the IP address for the outside network. All requests for a particular IP address from the outside or public network will be translated to the appropriate private IP address.
- **Public Port**
  This item will allow you to assign a particular port that you would like to have one of the private IP addresses to be able to respond to. Here are a few of the more common ports used:

  FTP - 20 & 21
  SMTP – 25
  DNS – 53
  HTTP – 80
  NNTP - 119
- **Private Server IP Address**
  This is the IP address of the server or workstation (or computer) where you want to get the “received message” for this port assignment.
- **Private Server Port**
  This is the port of where you want to have the server receive the messages.

8 Click **Delete** to permanently remove the IP address/port pair selected. Click **Edit** to modify the IP address/port pair selected. Click **OK**. You will return to the Incoming Network Address Translation Setup dialog box.

9 After you have finished entering the appropriate information, click **OK**.

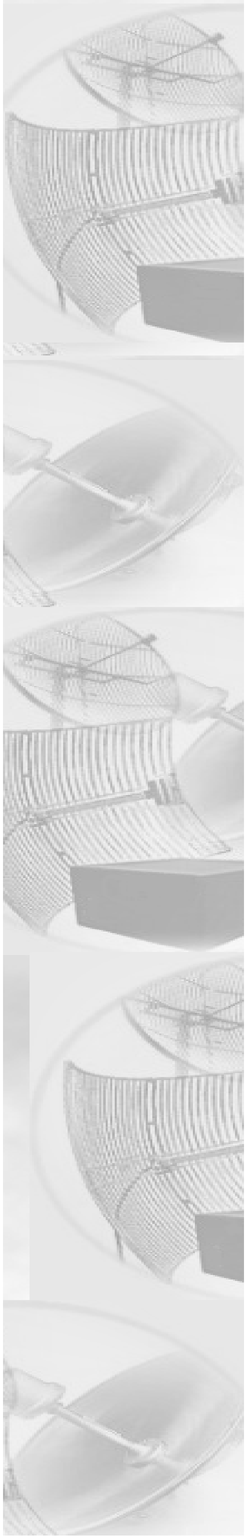
10 Now save the changes to the bridge or router. From the **File** menu, choose **Save Config**.

11 A message box appears informing you that the information will be saved to the bridge or router. Click **Yes**.

12 The Configurator confirms that the configuration has been saved. Click **OK**. The SPEEDLAN ISP shelfmount brouters will automatically reboot at this point.

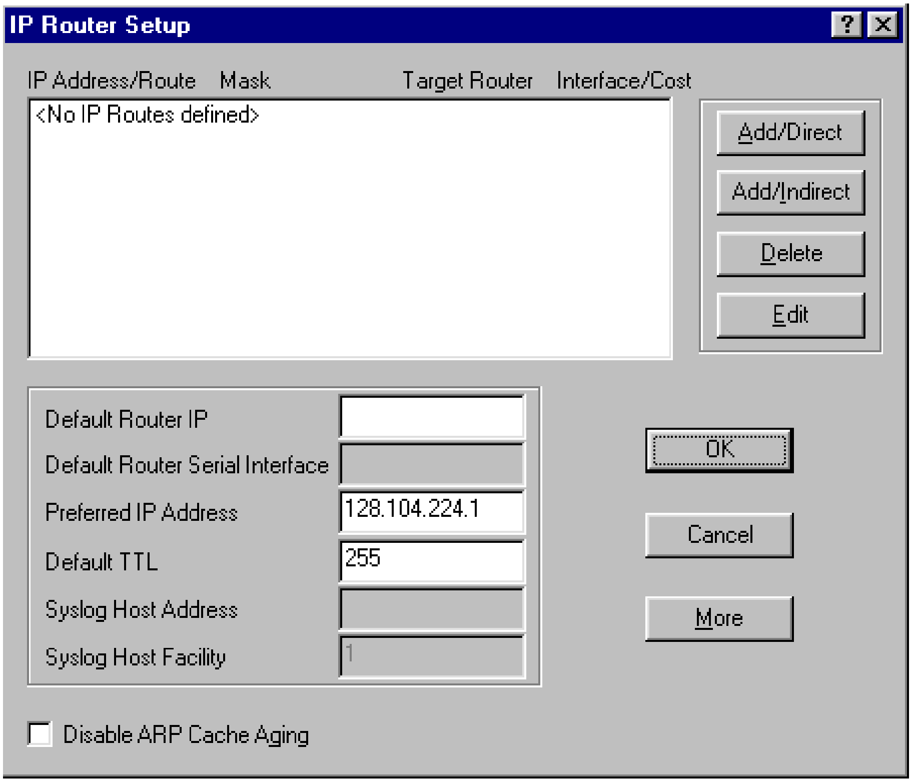
Notes:

Chapter 8
IP-Router Setup



IP Routing Setup

IP Routing in the General Setup dialog box must be enabled for this dialog box to appear. Then, choose **IP Routing Setup** from the **Setup** menu on the SPEEDLAN Configurator. This dialog box must be completed before saving any configuration in which IP Routing has been enabled. **Saving the configuration with incomplete entries in the route table will render the SPEEDLAN inoperable.** Enter the appropriate information as described below:



<No IP Routes defined>

Default Router IP
Default Router Serial Interface
Preferred IP Address 128.104.224.1
Default TTL 255
Syslog Host Address
Syslog Host Facility 1

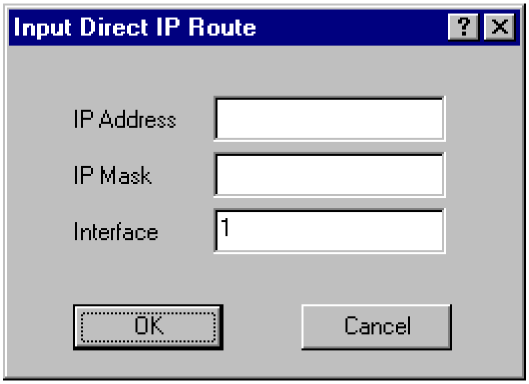
☐ Disable ARP Cache Aging

- **Default Router (IP Address)**
  This entry should be set to the IP address of the default router that the SPEEDLAN is to use when it does not know where to route a particular IP packet.
- **Default Router Interface**
  This entry should be set to the interface to which the default router is connected.
- **Preferred IP Address**
  From time to time routers will transmit unsolicited IP packets such as SNMP Traps, Syslog, RIP, or IP ARP packets. Most routers randomly use one of the IP addresses from one of the router's interfaces as the source IP address for these packets. On the brouter you can specify the source IP address that you prefer to use for these packets.

- Default TTL
  IP hosts on the Internet send out packets with a default "Time To Live" parameter. If you want to override the factory default of 64 attempts, specify your new default value here.
- Disable ARP-Cache Aging
  Use this option if you want to keep a permanent record of the IP to Ethernet addresses table for each computer directly connected to an interface on the brouter. This feature is helpful when used in conjunction with a corporate-wide SNMP monitoring tool to create a database of all Ethernet-to-IP address combinations on your network. A standard IP router and the bridge will age their ARP cache entries. It will time out and delete the ARP entries after a certain specified period (usually 10 minutes). The brouter has the option of not aging (deleting) any ARP cache entries. This will not normally cause any IP network problems, but this could result in a large ARP cache table. Since the typical brouter can hold over 10,000 ARP entries, this is not normally a problem.

Add/Direct Button

Click this button to specify the direct routes for each of the interfaces on the brouter. Direct routes are those that are directly connected to the interfaces. As an example, if Interface 1 is to have subnet 128.146.6.0 connected to it and an IP address of 128.146.6.1 with a subnet mask of 255.255.255.0, an entry in this dialog box should be set up as: IP Address = 128.146.6.1; IP Mask = FFFFFF00; and Interface = 1.



Input Direct IP Route

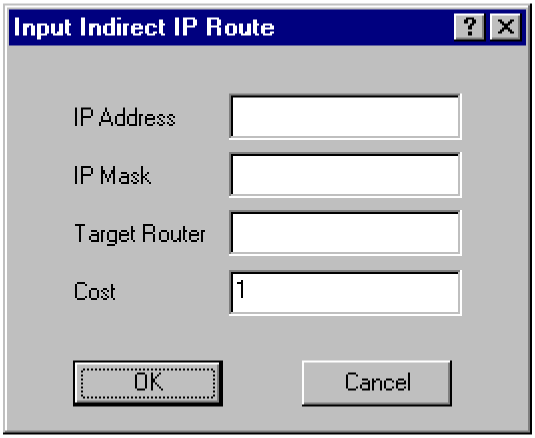
IP Address

IP Mask

Interface 1

Add/Indirect Button

Click this button to specify the indirect routes for this brouter. These routes are sometimes referred to as static routes. You can use indirect routes to define the way to get to subnets that are attached to other routers in your network. As an example, if subnet 198.17.74.0 is attached to router 128.146.11.20, in order for this brouter to route packets to 198.17.74.1 you should specify an entry that is set up as: IP Address = 198.17.74.0; IP Mask = FFFFFF00; Next Hop = 128.146.11.20 with Cost = 1.



Input Indirect IP Route

IP Address

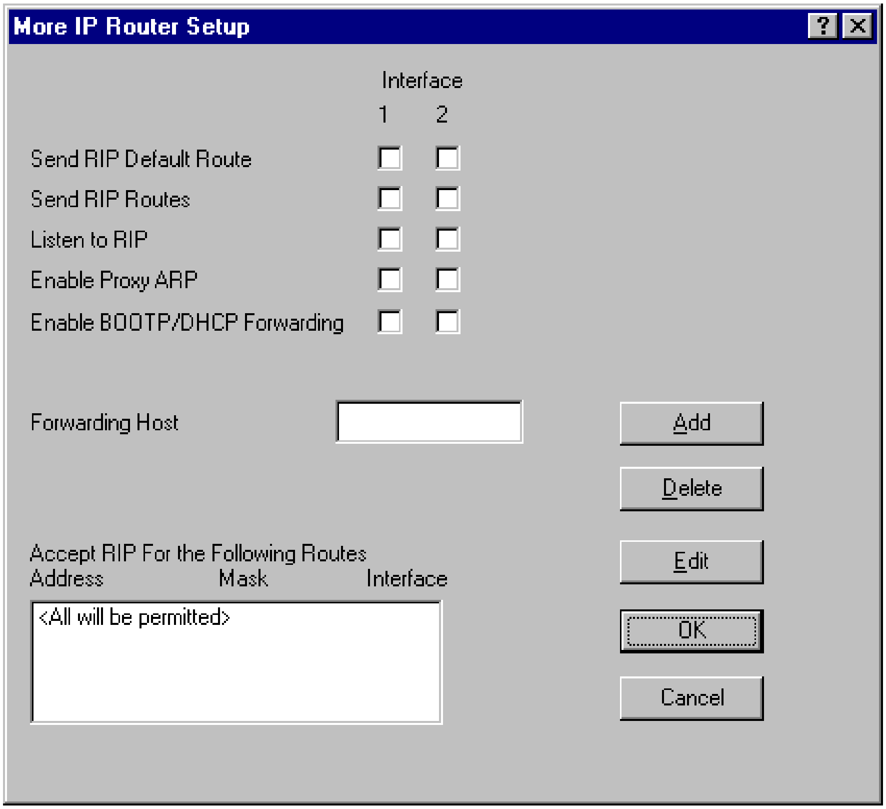
IP Mask

Target Router

Cost 1

More Button - RIP Routing

Click this button on the IP Router Setup dialog box to enable RIP. Wave Wireless brouters support what is known as RIP (Routing Information Protocol). RIP allows users to permit network equipment to communicate with each other to handle the routing plan of your network. Select the appropriate check boxes as described below:



More IP Router Setup

	Interface 1	Interface 2
Send RIP Default Route	□	□
Send RIP Routes	□	□
Listen to RIP	□	□
Enable Proxy ARP	□	□
Enable BOOTP/DHCP Forwarding	□	□

Forwarding Host

Accept RIP For the Following Routes

Address Mask Interface

<All will be permitted>

- **Send RIP Default Route**
  Enabling this feature instructs the brouter to inform the network (via RIP) that it is the default router for that network. **This feature should only be enabled if this brouter is the only default router on the local network.**
- **Send RIP Routes**
  Enabling this feature instructs the brouter to forward all route information gathered and stored by this brouter through the interface(s) selected. This is normally used in conjunction with Listen to RIP which instructs the brouter to gather RIP information from other RIP devices on your network.

- Listen to RIP

  This function enables the brouter to listen for and update its RIP information. The routes gathered in this manner come from other RIP-enabled routers on your network. This feature is normally used in conjunction with Send RIP Routes, which instructs the brouter to pass along all RIP information it has gathered to other RIP devices on your network.

- Enable Proxy ARP

  This feature allows the brouter to be used as the proxy host for users on the local network. This instructs the brouter to act as a "proxy" for the local destination host. This is used in circumstances that require connections not normally permitted for individual users on a network.

- Enable BOOTP/DHCP Forwarding

  This feature allows the brouter to pass BOOTP and DHCP requests across the wireless network.

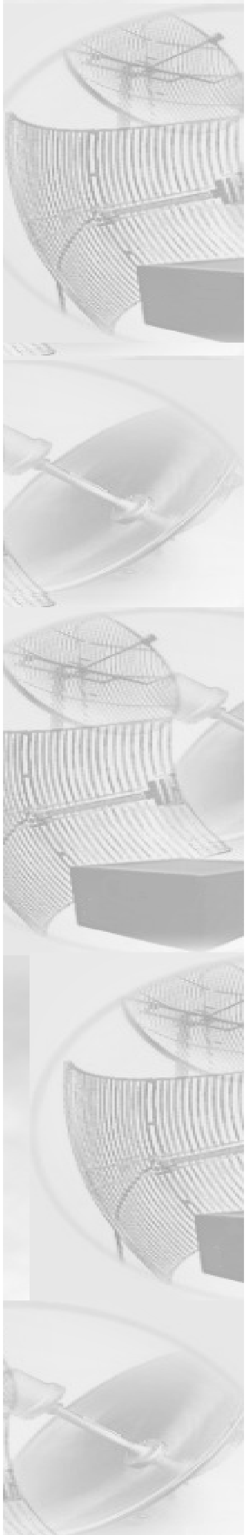
- Forwarding Host

  Defines the IP address of the device configured to act as the forwarding host for BOOTP and DHCP messages in a routed network.

- Accept RIP For the Following Routes

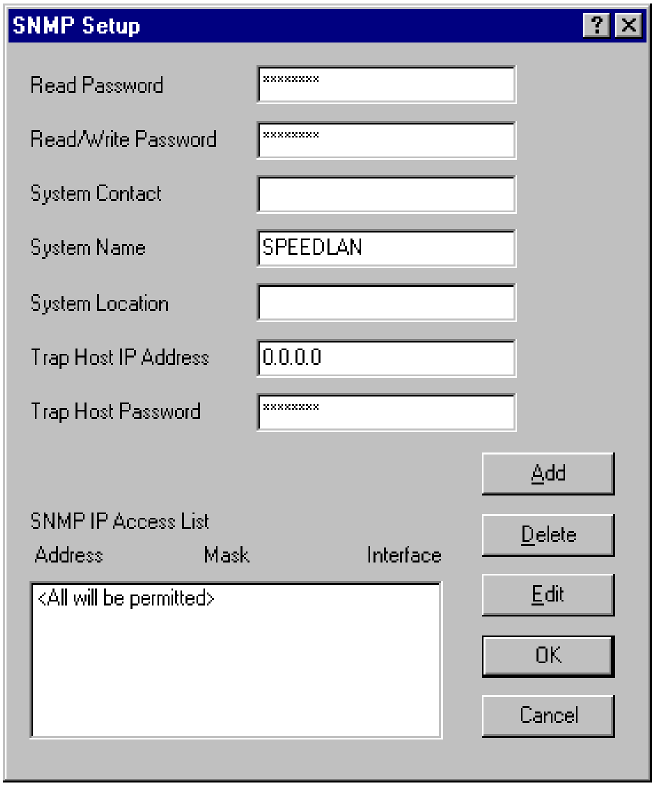
  Normally RIP instructs the brouter to forward all route information gathered to all RIP devices located on you network. Specifying devices in the RIP Access List allows you to limit which devices will be sent RIP. The devices specified in this list will be the only devices to receive RIP, while all other devices will be denied the RIP information stored on this brouter.

Chapter 9
SNMP Setup



SNMP Setup

Choose **SNMP Setup** from the **Setup** menu of the SPEEDLAN Configurator to set up SNMP.



Read Password ********

Read/Write Password ********

System Contact

System Name SPEEDLAN

System Location

Trap Host IP Address 0.0.0.0

Trap Host Password ********

SNMP IP Access List

Address	Mask	Interface
<All will be permitted>		

- Read Password
  This is the read-only password used for SNMP support. It is the SNMP password needed to read the Flash ROM Configuration and SNMP MIB variables. The factory-default value for this variable is the string "public".
- Read/Write Password
  This is the read/write password used for SNMP support. It is the SNMP password needed to write the Flash ROM configuration and SNMP MIB variables into the brouter. The string should be set to a value that is known only by you. The factory-default value for this variable is the string "public" and should be changed to a string known only to you.
- System Contact
  This field should contain the identification of the contact person for this SNMP-managed node, together with information on how to contact this person.
- System Name
  This field should contain the administratively assigned name for this managed node. By

convention, this is the node's fully qualified Internet Domain name (e.g., "bridge20.speedlan.com").

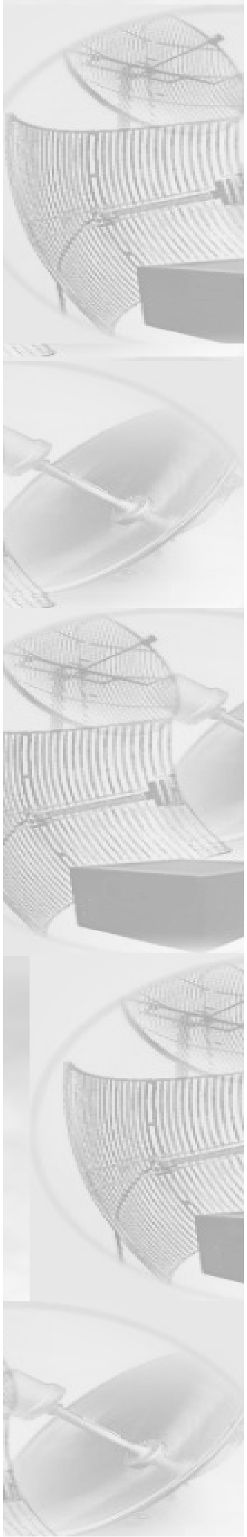
- **System Location**
  This field should contain the physical location of this node. (e.g., "telephone closet, 3rd floor").
- **Trap Host IP Address**
  This is the IP address of a network-connected host that is set up to receive SNMP Trap messages from this brouter. If you do not have an SNMP Trap Host, set this to 0.0.0.0.
- **Trap Host Password**
  This is the SNMP read/write password (community name) of the host that is set up to receive SNMP Trap messages. This field is ignored if the Trap Host IP Address described above is 0.0.0.0.
- **SNMP IP Access List**
  You can optionally set up a list of networks, subnets, and hosts that are authorized to access the brouter via SNMP.

TIP

To modify the SNMP Access List, click **Add**, **Delete**, or **Edit**.

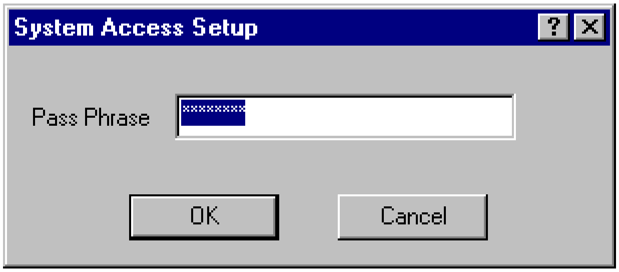
Note:

Chapter 10
System Access Setup



System Access Setup

Choose **System Access Setup** from the **Setup** menu of the SPEEDLAN Configurator to enter a password for the System Access Pass Phrase. This will enable you to create a connection between the equipment or wireless brouters. The default for the Pass Phrase is "**public**".



Pass Phrase ********

All wireless units connected to the brouter are restricted to systems based on the System Access Pass Phrase. Any wireless brouter that does not have the correct System Access Pass Phrase will not be to establish a wireless data connection.

Chapter 11
SNMP Monitoring