WIRELESS NETWORKING

SPEEDLAN

TM 6000

OPERATOR'S MANUAL

Version 1.0

Last revised June, 2000

941-358-9283
941-355-0219 FAX
800-721-9283

www.speedlan.com
sales@speedlan.com

Division SPEEDCOM INTERNATIONAL
1748 Independence Blvd. C-5
Sarasota, FL 34234

PRODUCT LICENSE AGREEMENT

It is important for users of Wave Wireless hardware and software to take time to read this License Agreement associated with this software **PRIOR TO ITS USE**. The Customer or Reseller has paid a License fee to Wave Wireless for use of this software on one bridge or bridge/router. This License does not extend to any copyrights to the program nor does it license use of the program on more than one bridge or bridge/router nor to make copies of the program for distribution or resale. A product registration card is included with the product manual. Please complete the card within 10 days of receipt of the software/hardware and return it to Wave Wireless. Registration is required for warranty service, technical support and notification of product updates and revisions.

License Agreement: The Customer or Reseller is granted a non-exclusive License to use the licensed program on a single bridge or bridge/router subject to the terms and conditions as set forth in this agreement. The Customer or Reseller may not copy, modify or transfer the reference manual or other documentation or any copy thereof except as expressly provided in this agreement.

The Copyright and all intellectual/industrial rights of this program and associated material remain the property of Wave Wireless. **THE CUSTOMER OR RESELLER MAY NOT USE, COPY, SUBLICENSE, ASSIGN OR TRANSFER THE LICENSED MATERIALS OR ANY COPIES THEREOF IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS LICENSE AGREEMENT**. The Customer or Reseller shall not reverse assemble or reverse compile the Licensed product or any copy thereof in whole or in part.

RETURN POLICIES AND WARRANTIES

Initial One Year Warranty Term:
Each Wave Wireless product is warranted against defects in material and workmanship for a period of one year from date of shipment. During the warranty period Wave Wireless will, at its option, repair or replace products that prove to be defective.

If equipment fails, the Customer or Reseller shall notify Wave Wireless and request a Return Material Authorization (RMA) number. For warranty service or repair, this product must be returned to Wave Wireless. **All returns to Wave Wireless MUST have a valid RMA number written clearly on the outside of the box or the shipment will be refused. The buyer shall pay all return shipping** charges during the one-**year warranty.** ***All outbound shipments will be made via ground shipment by Wave Wireless or via air courier with the customer's account number with the exception of Extended/"Spare in the Air" Warranty holders.***

Extended Warranty Policies (Includes *"Spare in the Air"*)
At any time during the first year following an equipment purchase, an Extended Warranty Policy may be purchased for 10% of the original list price. Terms of the Extended Warranty include "Spare in the Air" privileges to allow the use of parts or a spare unit temporarily.

***"Spare in the Air"* Loaner Unit or Parts Replacement Policies**
For an additional 10% of list price, the customer may purchase a "Spare in the Air" policy. This policy gives the customer the right to a loaner replacement unit shipped within 24 hours of acceptance of the RMA by Wave. All outbound shipments will be made via overnight air courier (during the first year).

***"Spare in the Air"* Policy Steps for Warranty or Extended Warranty Loaner Service:**
1. Customer obtains RMA approval
2. Overnight shipment of spare unit or parts to customer within 24 hours of approved RMA. Customer swaps unit or part(s) with phone assistance, if required.
3. Customer returns part(s) to Wave Wireless. ***All returns to Wave Wireless MUST have a valid RMA number written clearly on the outside of the box or the shipment will be refused.***
4. After 14 days from the issuance of an RMA, an invoice for the list price of the unit or components will be issued for any equipment that has not been returned. This will be credited upon the return of the defective or replacement part or unit to Wave Wireless.

Extended Warranty Pricing Schedule
1st year: 10% of published equipment list price
2nd year: 15% of published equipment list price
3rd year: 15% of published equipment list price
*If all three years are purchased simultaneously, the cost will be 10% per year or 30% of list.

Years 2 & 3 can be purchased during the initial year of coverage if the equipment was under extended warranty during the first year or if a physical on-site equipment inspection is performed and equipment is evaluated in warrantable condition by Wave Wireless personnel at prevailing or site service call rates.

Onsite Services
Onsite services for troubleshooting and repair are billed at daily rate, plus expenses, unless otherwise agreed upon. Use of spectrum analyzers or other test equipment may raise the daily rate.

Rental Unit Loaner
Customer may rent a unit at an agreed upon daily rate, plus shipping expenses, in lieu of purchasing a spare or "Spare in the Air" policy. Rental days are counted from date shipped until the date the unit is received in return by Wave Wireless.

Refurbishing Fees
Any product returned that requires refurbishing, is damaged due to inadequate or improper packaging protection, or that has not been returned with original packing materials may be subject to a refurbishing fee.

Bench Test and Repair Time
A unit is returned as defective and through bench testing is determined that the unit is not defective, Wave Wireless, at its discretion, may charge bench test time at a rate of $85 U.S. per hour for testing and troubleshooting. Out of warranty repairs will be performed at a rate of $85 U.S. per hour plus parts. All shipping charges will be the responsibility of the customer.

Return for Credit

All returns to Wave Wireless MUST have a valid RMA number written clearly on the outside of the box or the shipment will be refused. **No returns for credit after 30 days will be approved.** Products must be returned undamaged and in original packaging or they will be subject to a minimum 20% restocking/refurbishing fee. Return freight charges must be prepaid. At the option of Wave Wireless, products may be returned for repair or replaced provided the goods have not been modified or repair attempted by someone other than Wave Wireless.

Limitation of Warranty

The foregoing warranty shall not apply to defects resulting from improper or inadequate maintenance by the buyer, buyer supplied interfacing, unauthorized modification or misuse, operation outside of the environmental specifications for the product, or improper site preparation or maintenance. ***Systems must be protected from electrical brownouts and surges by a quality UPS such as an APC Smart brand or Tripp Lite Omni or similar, or warranty shall be null and void***. Warranties do not apply to any product that has been (i) altered, except expressly approved by Wave Wireless in accordance with its instructions, (ii) damaged by improper electrical power or environment, abuse, misuse, accident, or negligence. Repairs in the case of damage from "acts of God" are covered on a time and materials basis. The warranty shall not apply if Wave Wireless prebuilt U.S. FCC approved antenna assemblies have been altered and installed by any persons other than professional wireless installers.

THE FOREGOING WARRANTIES ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

No statement, including, without limitation, representations regarding capacity, suitability for use or performance of products, whether made by Wave Wireless employees or otherwise, shall be deemed to be a warranty by Wave Wireless for any purpose or give rise to any liability for Wave Wireless unless expressly contained in writing. Resellers will have complete responsibility and liability for performance of its agreements with its customers and Resellers shall indemnify and hold Wave Wireless harmless from and against all liability arising out of such agreements.

Wave Wireless warrants that the firmware for use with the unit will execute its programming instructions when properly installed on the unit. Wave Wireless does not warrant that the operation of the unit or firmware will be uninterrupted or error-free. Wave Wireless shall not be obligated to remedy any software defect that cannot be repeated.

Wave Wireless is not responsible for equipment non-performance due to outside radio interference caused by any source.

Exclusive Remedies

The remedies provided herein are the buyer's sole and exclusive remedies. Wave Wireless shall not be liable for any direct, indirect, special, incidental or consequential damages, whether based on contract, tort or any legal theory.

OTHER IMPORTANT STATEMENTS AND WARNINGS

Copyright/Liability

SPEEDCOM International, dba Wave Wireless Networking 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. *SPEEDCOM* International, dba Wave Wireless Networking 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.

Trademarks

Wave Wireless Networking's name and all trademarks in this document are property of SPEEDCOM International Corporation, except for Microsoft® Corporation Windows 95®, Windows 98®, and Windows NT®.

FCC STATEMENT (FOR USA ONLY)
FEDERAL COMMUNICATIONS COMMISSION

Radio Frequency Interference Statement for Spread Spectrum Devices

Warning: This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Electronic Emission Notices

All the spread spectrum devices sold in this catalog comply with Part 15 of the FCC rules.
Operation is subject to the following two conditions:

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

If this equipment causes interference to radio reception (which can be determined by unplugging the power cord from the equipment) try these measures: (1) Re-orient the receiving antenna, (2) Relocate the equipment with respect to the receiver, (3) Plug the equipment and receiver into different branch circuits, or (4) Consult your dealer or an experienced technician for additional suggestions.

DANGER!!!

Rooftop or tower antenna installations are extremely dangerous and incorrect installation may result in injury, damage, or death. Rooftop and tower installations must be performed by professional antenna installers only.

Table of Contents

INTRODUCTION

Features and Benefits

Transparent Ethernet Bridging with Advanced Filtering for Security and Network Reliability
SPEEDLAN TM supports what is known as Transparent Ethernet Bridging with no Spanning Tree or Source Routing support. Since the brouter contained in the SPEEDLAN TM is intended to 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 to the Transparent Ethernet Bridging, the SPEEDLAN TM can drop (i.e., not forward) packets based upon the encapsulated higher layer data within the packet. It is this option that gives SPEEDLAN TM the ability to perform advanced firewall filtering and can add a significant measure of security and network reliablility to a network, surpassing that provided by modern multiprotocol routers.

IP Routing with Advanced Filtering for Security
The SPEEDLAN TM supports IP Routing in addition to bridging. It can be used to add routing capability when an IP router may be a more appropriate choice.

Features Chart

Hardware Supported
10/100BASE-T Ethernet Card
SPEEDLAN Wireless Radio

Bridging Features
Transparent Bridging
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

SNMP Features
IP “ping” Support
IP SNMP Support (MIB II, Ethernet, Inteface, SNMP, and Bridge MIB)
IP SNMP WaveLAN
IP SNMP Trap Support
SNMP Access Lists

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

USING CONFIGURATOR

Windows 95/98/NT 4.0 SPEEDLAN TM Configurator

Installing the Windows SPEEDLAN TM Configurator

1. Shut down all programs and applications.
2. **Note:** The SPEEDLAN TM Configurator uses digital libraries, 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.
3. Insert the CD into your floppy drive (i.e., Drive E, F, etc.).
4. If the **setup.exe** program does not install 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**.
5. Follow the installation prompts.
6. After the installation is complete, restart your computer.
   Note: Visit the web site for the newest SPEEDLAN TM Configurator.

File Menu

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

Configuring a Remote SPEEDLAN TM

To configure a remote (network attached) brouter, you can use the Open Remote Config and Save functions. You must have a remote SPEEDLAN TM configuration opened with the Configuration Utility before any configuration functions may be 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 then reprogrammed with the new configuration. After you save the configuration, you must wait the required 15-second period to allow the Flash ROM to be fully programmed and let the bridge reboot with the new configuration. **Turning off the SPEEDLAN TM or otherwise interrupting the reprogramming of the Flash ROM will 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 help avoid loss of communication between units.

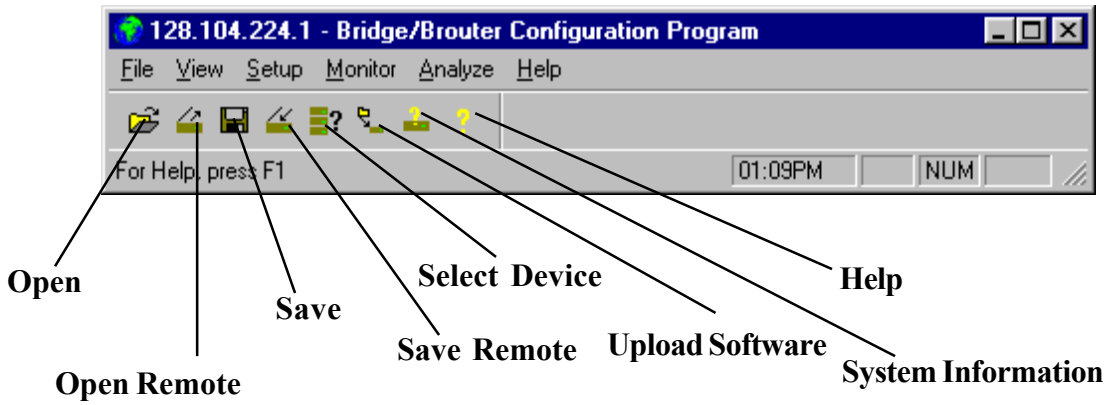
Configuring a Saved Configuration File

To configure a saved CNF file (configuration file), open it from the file menu using the open function. You then configure the file just as if you were configuring a remote SPEEDLAN TM. 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 TM; 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 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 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



Below the menus you see a row of seven icons. Each icon depicts a function that can also be accessed from the menus.

The File Menu

Open Config File - This function is used to open a configuration file from disk.
Open Remote Config - This opens the configuration file directly from a remote device.
Save Config - Saves the configuration you are working on to the place where you opened it.
Save Config File as - 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 function is 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 - Use this function to reboot a brouter from a remote location.
Exit - Closes the SPEEDLAN TM Configuration program.

CONFIGURING SPEEDLAN TM

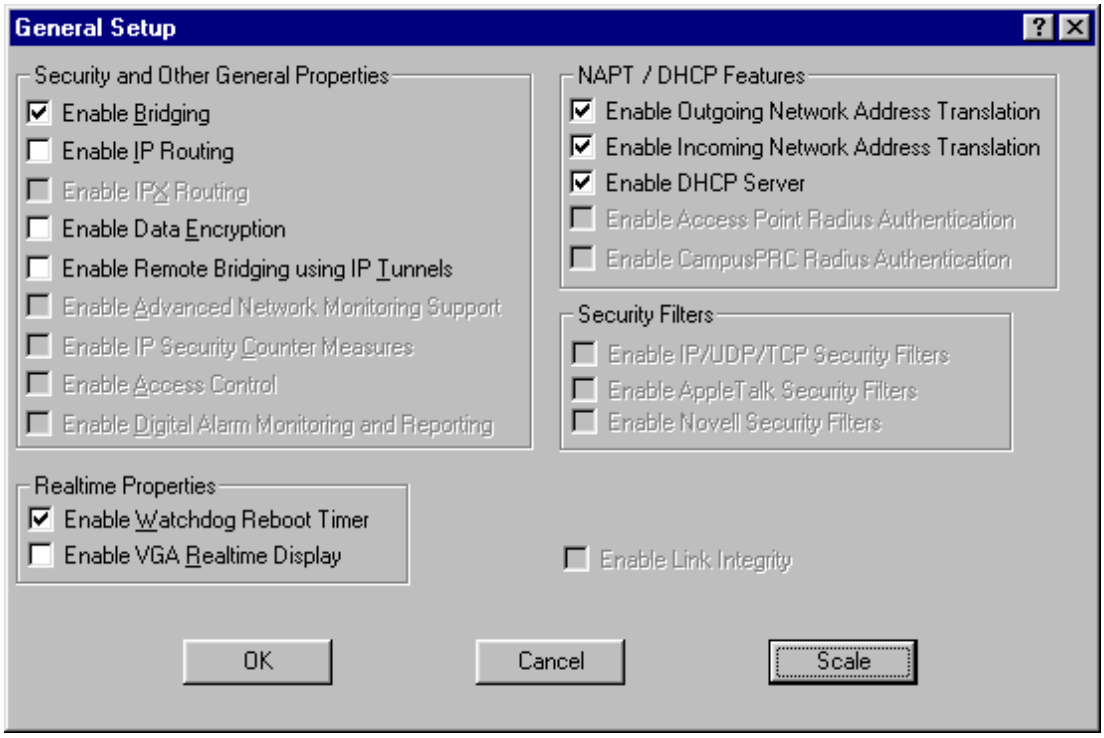
General Setup Menu

The third menu from the left is the Setup Menu. In this menu are the screens you will use to configure your brouters. Below are descriptions of the menu items and the settings found on their respective screens.

General Setup

Enable Bridging - The transparent bridging function will be enabled when this is item is checked. If you want the brouter to perform the bridging function,you must enable this. When bridging is enabled, the Bridge Setup Screen will be accessible. Bridging should be enabled for nearly all applications of the brouter. Default is on. (This function should never be disabled.)

Enable IP Routing - The transparent routing function will be enabled when this is item is checked. IP Routing will work properly only if the routes are set up in the IP Route Menu. **If the routes are not set up properly before you save the configuration, the bridge will become inoperable.** 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 XE units. If you did not purchase it when you originally bought the SPEEDLAN TM units, it can be purchased later as a software upgrade.

Data encryption is disabled by default. 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. To do this, return to the drop down menu presented when you clik on Setup. Now you will see a Data Encryption Setup item added to the menu list. Select Data Encryption Setup. Select 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 on all XE units you wish to have communicate together. Failure to set them to the same value will prevent any communications from taking place. (e.g. for multipoint to work properly, the base station AND all of the satellite units must use the same Encryption Key setting.

Enable Remote Bridging using IP Tunnels - SPEEDLAN TM supports 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 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 informatoin, see *Setting UP NAT*, *page 6*1.

Enable Incoming Network Address Translation - This option enables a company to unmap public network IP address into private network IP addresses. For more information, see *Setting UP NAT* on *page 61*

Enable DHCP Server - This option enables the DHCP client and the interface that is selected. For more information, see *Setting UP the IP Addresses*, *page 58.*

Enable Access Point Radius Authentication - This option is not available at this time

Enable CampusPRC Radius Authentication - This option is not available at this time.

Enable Link Integrity - 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.

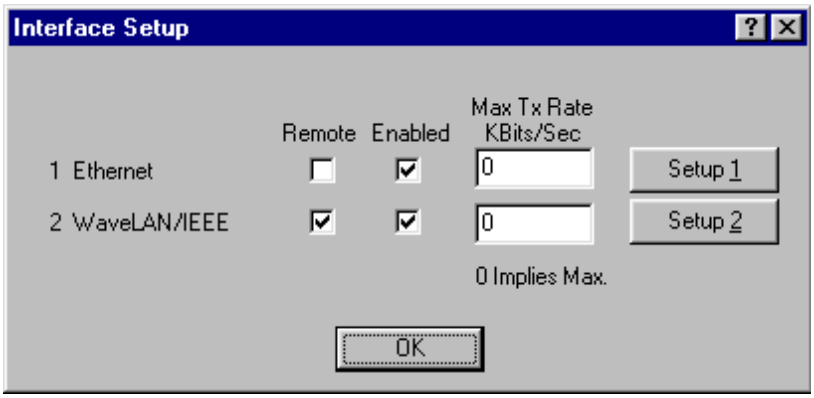
Enable Watchdog Reboot Timer - This feature instructs the bridge to reboot in the event that the bridge fails to receive any incoming packets, from any port, for a period of 10 minutes. The brouter will assume an error has occured and will reboot. If, after the brouter reboots, it does not receive an incoming hello signal, the bridge 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.

Enable VGA Realtime Display - This feature allows a client to install a video card and a monitor and view the statistics directly from the unit, instead of Configurator, laptop, PC, etc.

Note: Click Scale to view the LED Forwarding Scale.

Interface & Advanced Interface Setup

The interfaces that are installed in your brouter will be represented on this screen. The Remote check box is used to designate which interfaces will be considered local and remote. The local interface is consider to be the interface that connects directly to the local LAN with respect to the unit. 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.

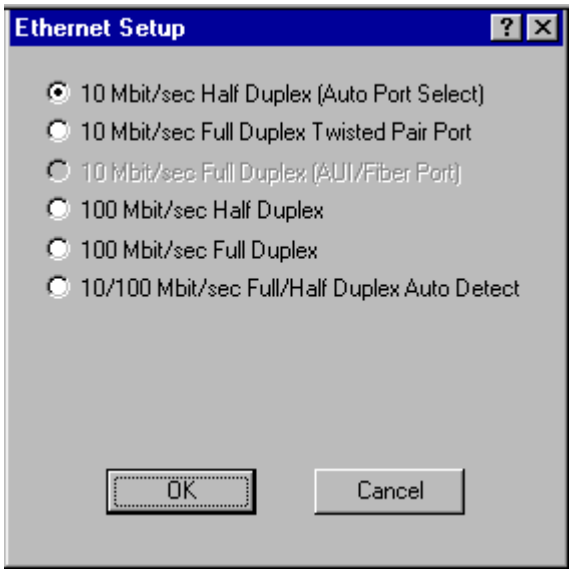


The Advanced Interface Setup has a few more advanced settings, but essentially they are the same set up screen. Note that the Max Tx rate is available on both the Interface Setup and Advanced Interface Setup. Max Tx Rate is useful to ISPs that want to regulate the maximum bandwidth provided to each customer. These settings should not be changed without the assistance of a Wave Wireless Networking Technical Support Engineer. Backup and Perm are not used with the XE series products. These fields must remain empty.

The Setup Buttons

Setup 1 - Ethernet Setup

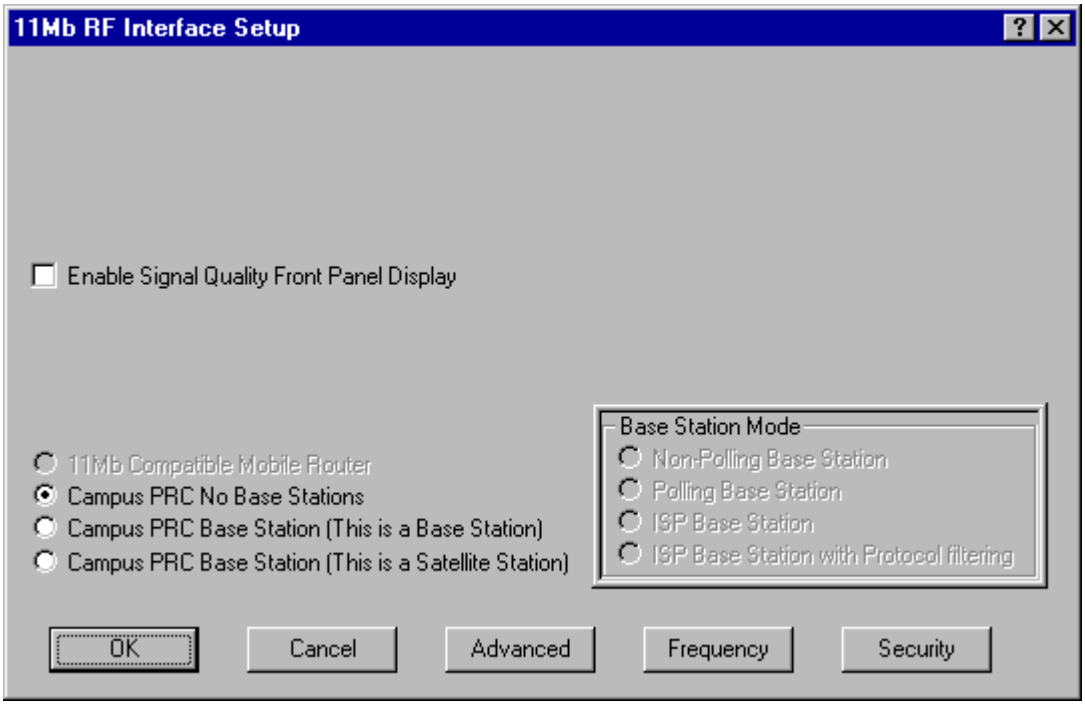
SPEEDLAN products come standard with a 10/100 Base-T interface to connect to your wired network. Although the interface is capable of operating at both 10 Mbps and 100 Mbps, it is not autosensing or autoswitching. The default setting is for 10 Mbps half-duplex operation. If you which to connect your SPEEDLAN unit to a 100 Mbps port, the Ethernet interface can be manually switched to 100 Mbps in this portion of the setup.



The card 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 Full Duplex using the options on this setup screen.

Pressing the Setup buttons (1 and 2) on the Interface & Advanced Interface Setup screen will open the Setup screen for the interface selected.

Setup 2 - 11 Mb RF Interface Setup - On this screen are 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 and how they effect the performance of the SPEEDLAN interfaces.



Transport Methods

The industry compatible method of transmitting and receiving data over wireless networks 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 refered to as CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Wireless networks are CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The reason collisions can not be detected is wireless cannot receive and transmit at the same time, hence SPEEDLAN TM is not able to listen for the collisions. In practice a properly operating SPEEDLAN 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, thus saving bandwidth by eliminating the extra overhead.

Campus Cell PRC Mode (No base stations) - This method of transportation requires that all brouters be able to detect each other. If any of the stations are unable to see each other then a Base Station must be assigned that can repeat traffic from one brouter to another. This method 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 SPEEDLAN network

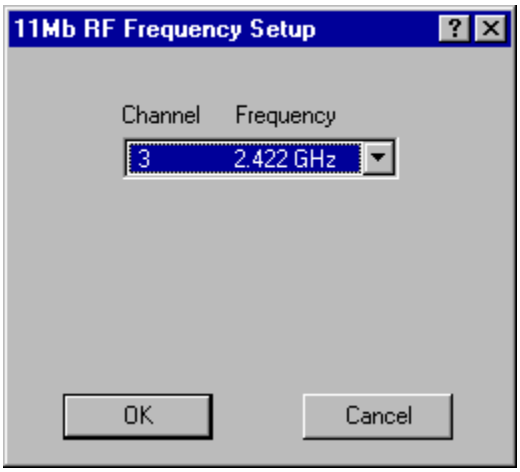
Campus PRC Mode (This is a Non-Polling Base Station) - This setting should be used if this is the only base station in the SPEEDLAN TM wireless network cell. With the previously mentioned 'Campus Cell PRC Mode (No Base Stations)' setting there is a requirement that all wireless stations be able to transmit to and receive from ALL other stations in the wireless network. This is not always possible due to particular topology and terrain. SPEEDLAN TM has a special mode where one of the wireless stations can be configured as a *Base Station* and all other wireless nodes setup as *Satellite Stations*. In this configuration the only requirement is that each satellite station be able to communicate directly with the base station. The base station is responsible for repeating packets that need travel between the satellite stations. The Non-Polling Base Station does not allocate bandwidth to each statellite. This is preferable when the total number of satellites in the wireless cell is less then somewhere between 5 to 10 stations.

The performance of this approach is greatly improved if the base station is connected to the most heavily loaded network or network server. This is due to the fact that data flowing from one satellite to another satellite station must be repeated (retransmitted) by the base station, thus more of the wireless bandwidth is used. Data packets flowing from a satellite station to the base station are transmitted directly to the base station without the need to be repeated.

Campus PRC Mode (This is a Polling Base Station) - This setting should be used if this is the one and only base station in the wireless network cell. When the number of satellites become greater then approximately 5 to 10 stations the Non-Polling Base Station sometimes is not as able to keep up with the wireless traffic that needs to be forwarded. The Polling Base Station alleviates this problem by continuously communicating with all of the satellite stations in its cell, and is responsible for dynamically assigning how much time is to be alotted to each satellite in the next transmission of data packets from that satellite. This is done after every transmission

and greatly improves the performance of a base station wireless network cell when the total number of satellite stations is greater then 5 to 10 stations. As the number of stations increases, the usage of the wireless network cell increases and efficiency is proportionately improved.

Campus PRC (This is a Satellite Station) - This is the configuration required for stations that are to be installed into a wireless network cell that utilizes a base station. Except for the base station, all the stations in this type of wireless network cell should be configured as Satellite Stations. The satellite configuration tells the brouter to forward all data that needs to pass through the wireless network to the base station. In addition, the satellite stations are configured to listen to the base station for instructions if they are forthcoming.

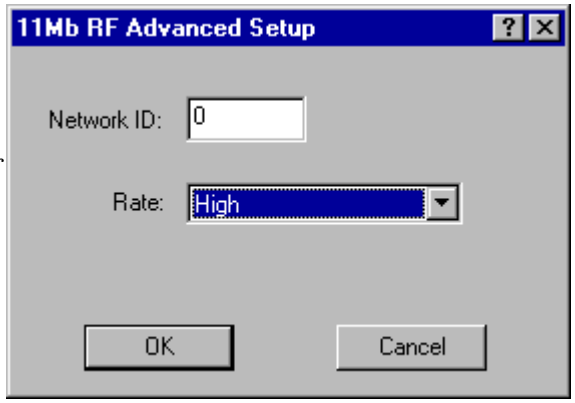


Frequency Button - The Frequency button can be found in the lower right hand corner of the individual interfaces setup screens. Clicking this button will open a new screen that allows you to change the operating frequency of the interface. All of the brouters expected to communicate with this device should be configured with the same frequency.

Advanced 11 Mb RF Interface Setup

Network ID - The Network ID is a security setting that allows the SPEEDLAN TM unit to reject packets from other wireless bridges in the area. Although the bridging or routing table would reject the packet once it was processed, the Network ID allows the bridge to reject the packet with much less processing. This improves the performance of the SPEEDLAN TM units in installations where many wireless bridges 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.

Warning: This setting must be set to the same value on all SPEEDLAN TM units you wish to have communicate together. Failure to set them to the same value will prevent any communications from taking place. (e.g. for multipoint to work properly, the base station AND all of the satellite units must use the same Network ID setting)



Rate – This setting refers to the RF data rate. The SPEEDLAN TM 11 Mbps radio has 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.

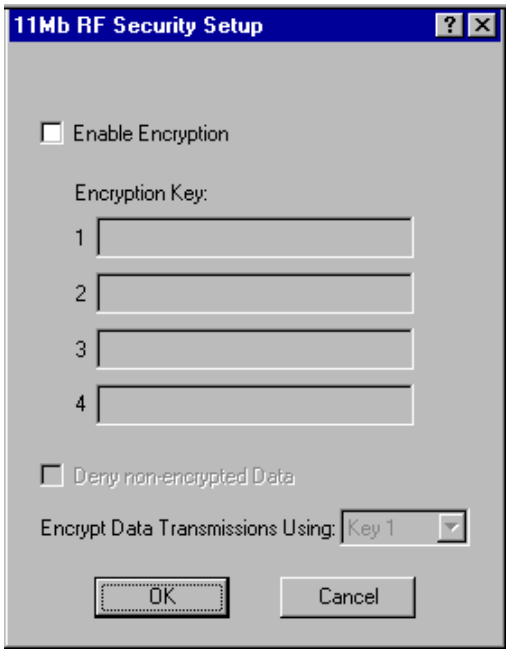
Standard – This setting limits the card to providing 2 Mbps of bandwidth. The receiver sensitivity of the radio with this setting is –89 dBm. You must use this setting if you want your XE unit to communicate with an older SPEEDLAN unit that uses a 2 Mbps radio.

Low - This setting limits the card to 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 on all XE units you wish to have communicate together. Failure to set them to the same value will prevent any communications from taking place.

11 Mb RF Security Setup – 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:

- 5 alphanumeric characters in the range of "a-z", "A-Z", and "0-9"
- A 10 digit hexadecimal value using the range "A-F" and "0-9". If you choose to use the hexadecimal method, use the prefix "0x" (zero, x) in defining the key

Examples:

- Alphanumeric: **a5F2z**
- Hexadecimal: **0xA95F2BR39K**

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**"

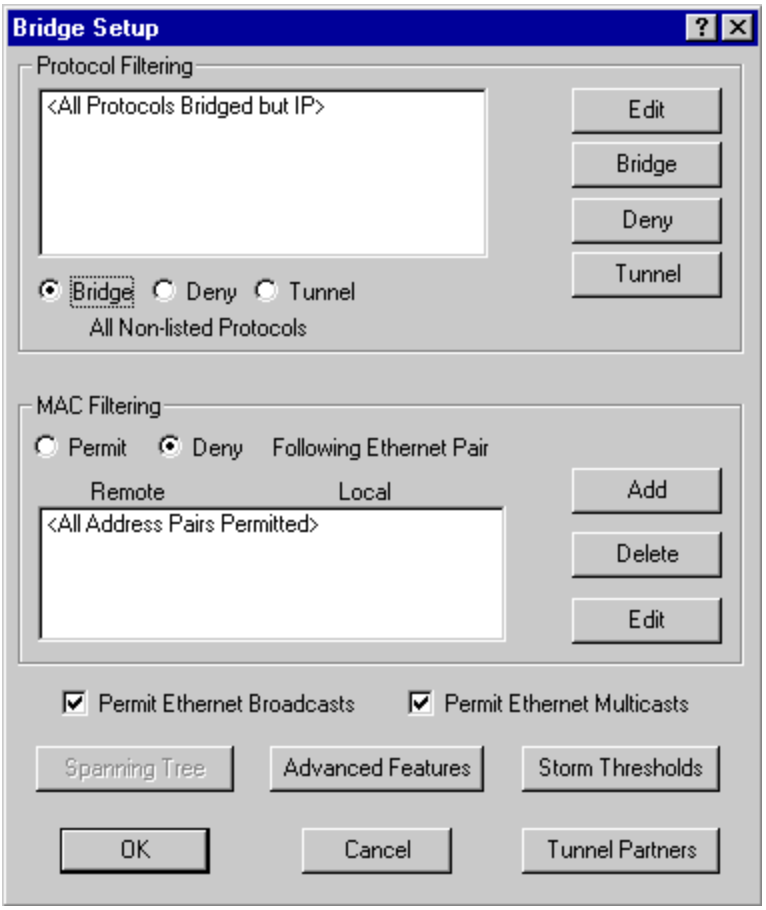
Warning: This setting must be set to the same value on all XE units you wish to have communicate together. Failure to set them to the same value will prevent any communications from taking place. (e.g. for multipoint to work properly, the base station AND all of the satellite units must use the same Encryption Key setting.

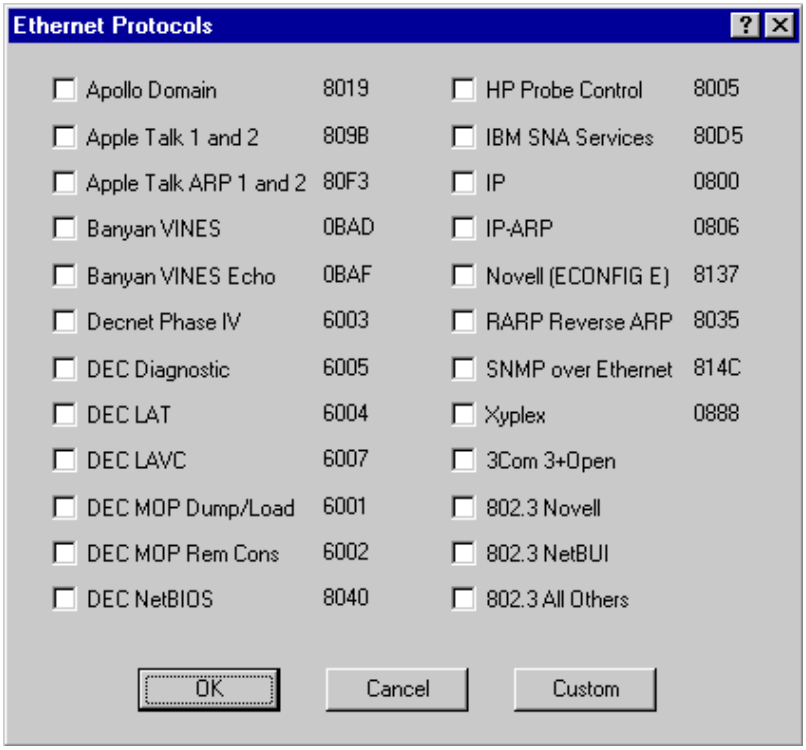
There is also an option to **Deny non encrypted Data**. This feature is disabled by default and is designed primarily for multipoint SPEEDLAN installations where it may not be necessary to run using data encryption at all locations. If you enable this option, any data received by this SPEEDLAN TM unit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

BRIDGING SETUP

The SPEEDLAN TM is an IEEE 802.3 MAC- layer bridge. The bridge can be configured to bridge or pass any 802.3 frame type protocols, including Novell IPX, TCP/IP, AppleTalk, etc. The SPEEDLAN TM 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.

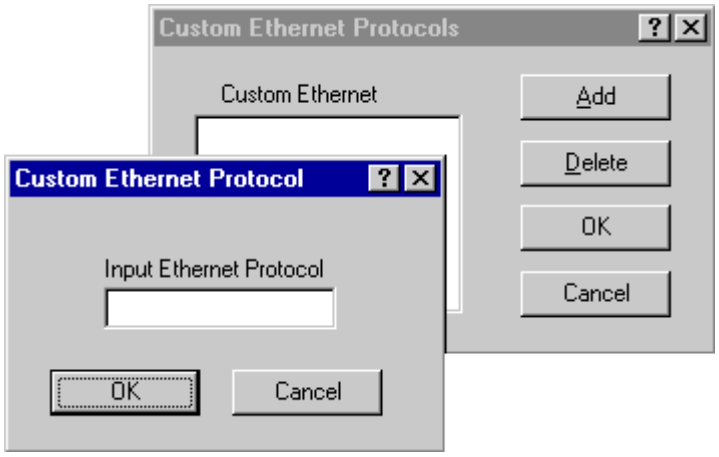
Protocol Filtering - By default, the SPEEDLAN is configured to pass all network protocols. When you press the Edit button, you will be presented with a list of protocols which you can select for filtering. After selecting the protocols, highlight them on this screen and press the Bridge or Deny buttons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



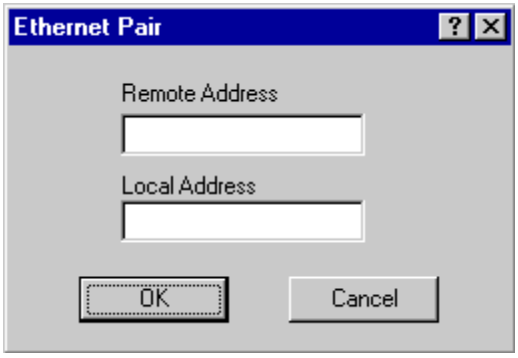


Ethernet Protocols - Some common Ethernet protocols and their associated ID numbers have been placed in this table. Simply select one from this list if you wish to set a filter for it.

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

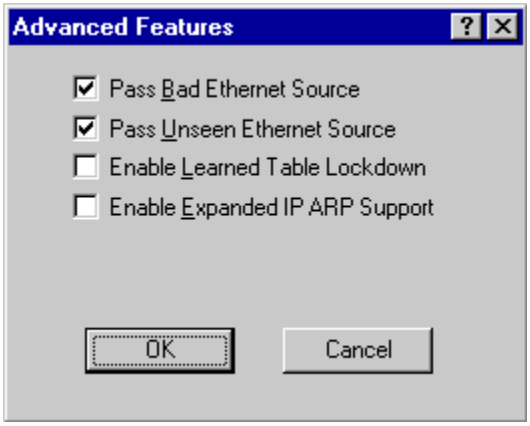


MAC Filtering - By default, the SPEEDLAN TM is configured to pass all traffic between all MAC-Address pairs. To add an address pair into the filter, click on the Add button in the MAC Filtering box. You will be prompted to enter the Remote Address, which will be the MAC Address that resides on the remote side of the brouter, and the Local Address, which will be the MAC Address that resides on the local side of your network. The side of the bridge you configured determines the remote side and local side (in the Interface Setup screen).



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 shutting off multicasts on the SPEEDLAN TM. Shutting off multicast packets will reduce the traffic being sent across your wireless network link. This will also reduce the number of interrupts that each computer connected to your network experiences.

Advanced Features - Clicking the *Advanced* button brings up this screen. Below are descriptions of the settings and how they will effect your network.



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.

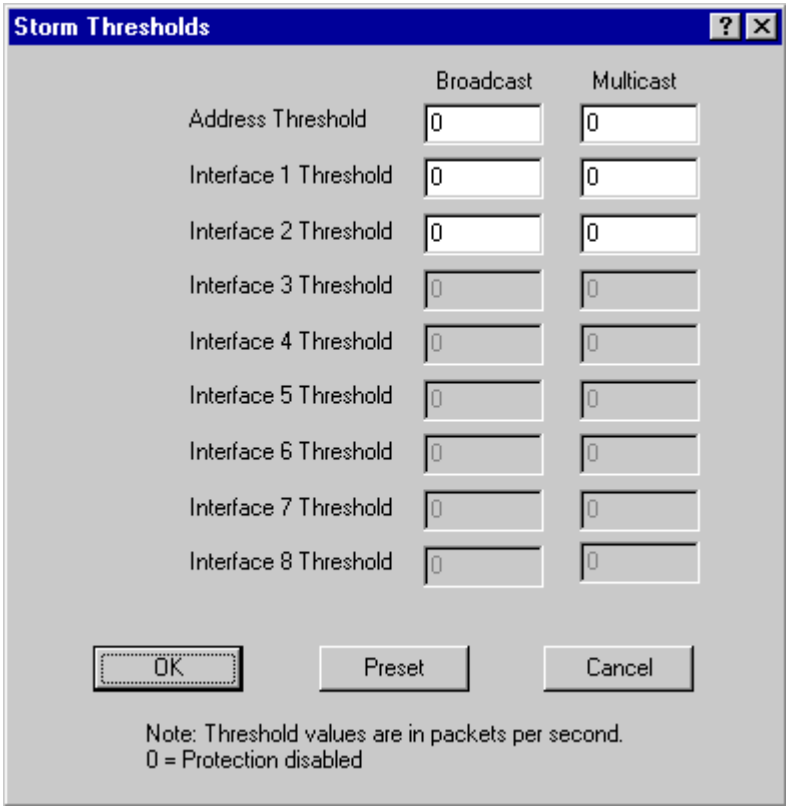
Pass Unseen Ethernet Source - Standard Ethernet bridges will always forward packets with destination addresses that have not been learned (i.e., have not previously been seen as a source address of a packet). This characteristic is needed for the proper operation of an Ethernet bridge. The downside to this, as our studies have shown, is that the failure mode of many Ethernet interface cards is to 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. It should be set to deny only by a qualified network engineer after careful testing and consideration. The default value for this setting is checked.

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 correctly functioning network 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 spoofing 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 TM 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 TM takes 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 TM 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.

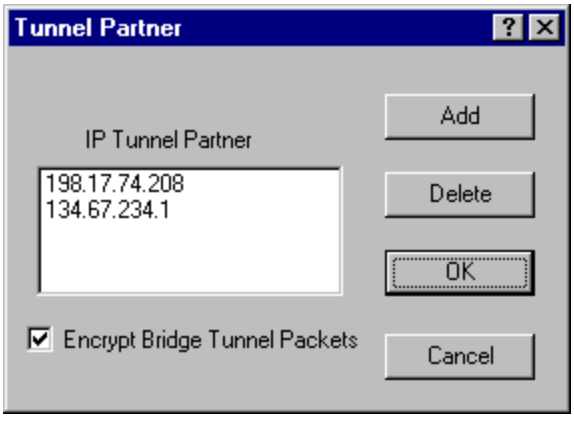
Storm Thresholds - One of the unique and very useful features of the SPEEDLAN TM is its ability to keep broadcast and multicast storms from spreading throughout a network. Network storms are common and can cause bridges, routers, workstations, servers, and PCs to slow down or crash. Storms occur if network equipment is configured incorrectly, if network software is not functioning properly, or poorly designed programs such as network games are used. These settings are disabled by default.



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.

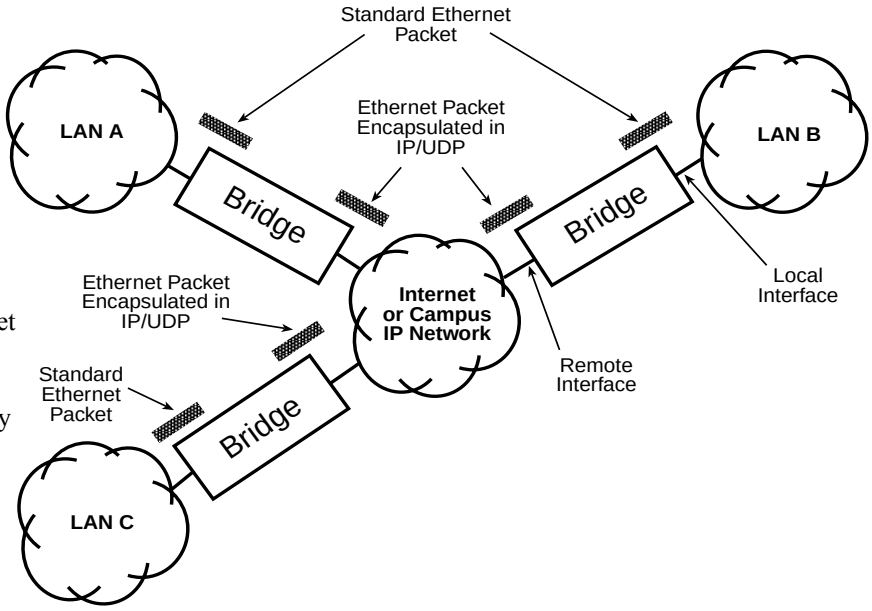
Preset Button - This button sets the broadcast and multicast storm thresholds to the recommended values. These values have been determined to offer good protection without interfering with the operation of the typical network. These values may need to be tuned for your particular network.



Tunnel Partners - Tunneling is a method of encapsulating Ethernet packets received from the local interface in an IP/UDP packet and sending them to one or more tunnel partners. Tunneling can be used to set up virtual Ethernet networks. In the General Setup menu, if the *Remote Bridging using IP Tunnels* is enabled, Tunnel Partners can be set up. This menu 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.

Encrypt Bridge Tunnel Packets - If purchased, brouters (from Wave Wireless) may contain a special software-encryption algorithm that is distinct from the optional SPEEDLAN encryption chip on the brouters. If Data Encryption is enabled on the General Setup menu 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.

Generic Ethernet Tunneling
(Through an IP Network)



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.

Setting Up the IP Addresses (IP Host Setup)

Use DHCP to set up the server and client IP addressing for the network. Use NAT to set up the translation for incoming and outgoing network IP addresses.

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 56* .

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
Understanding this methodology is difficult, even for customers. Therefore, let's explain this in easier terms. 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 2^{24} 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 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?
This term 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.

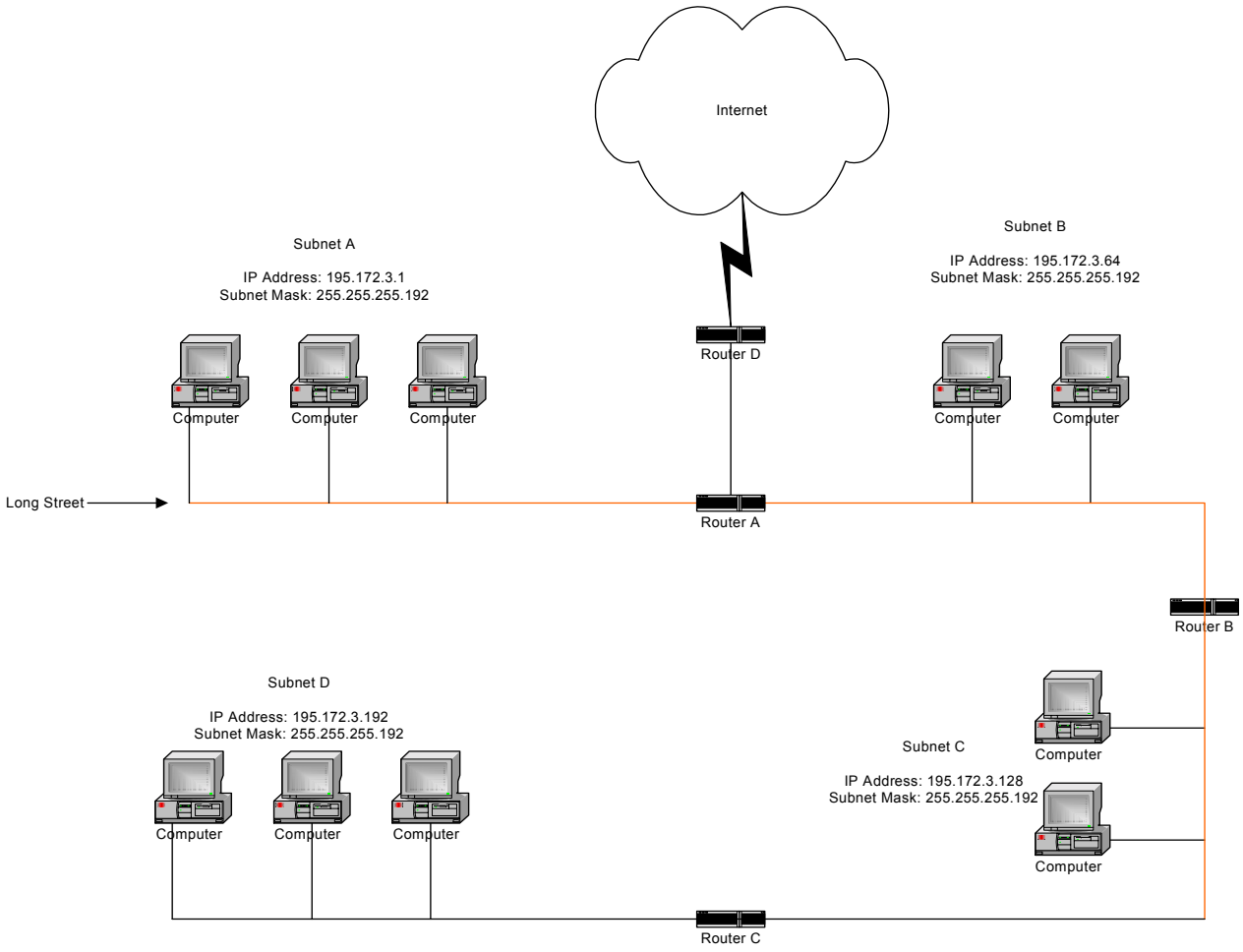
What is a Subnet Mask?
This term allows you to mask section(s) (depending on the class specified) of the octets in the network address. Each octet used in the subnet mask is assigned to a data link. The leftover octet(s) are assigned to the remaining nodes.

For more information on subnetting, see the example below and figure on the next page.

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 (also know as brouters), etc.).

Figure 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 one of the benefits of static or dynamic addressing.

How does a network administrator assign an IP address?

IP addresses are supplied by the network administrator (you), 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.

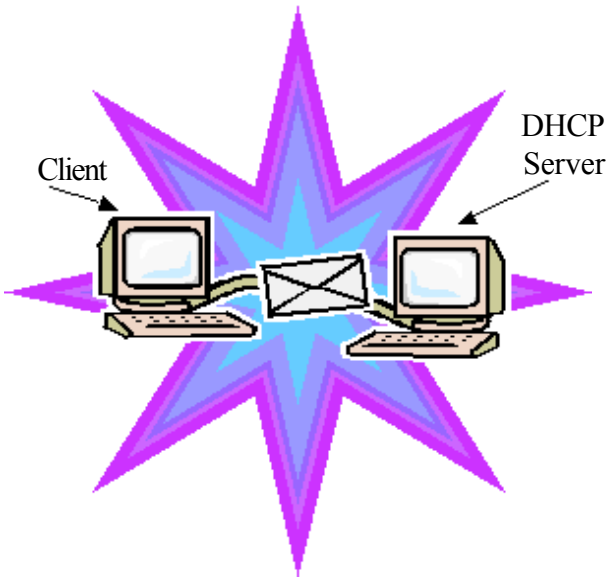
What is DHCP?

Dynamic Host Configuration Protocol (DHCP) allows network administrators (you) to assign static or 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 help resolve security, costly IP addressing services, and compatibility problems. DHCP is an alternative to BOOTP, which reduces the agony of assigning IP addresses and also provides advanced configuration options.

> **Note:** The figure on the next page may help you understand how a DHCP address is generally assigned.

Figure of DHCP Addressing



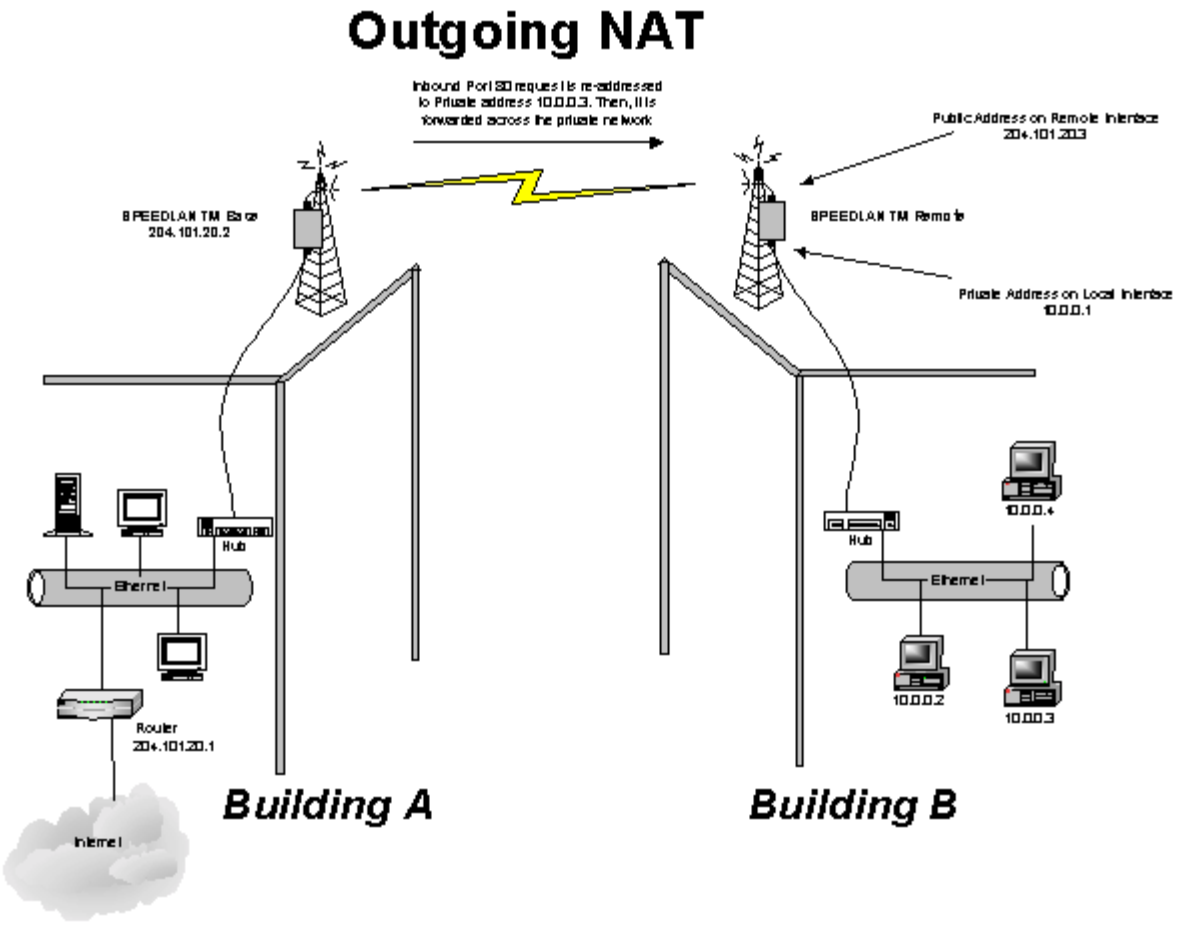
1. The client asks DHCP server for IP address and configuration if needed.
2. The DHCP server assigns an available IP address to client.
3. The client takes IP address from DHCP server and requests for any configuration needed.
4. DHCP server confirms IP address and configuration.

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.

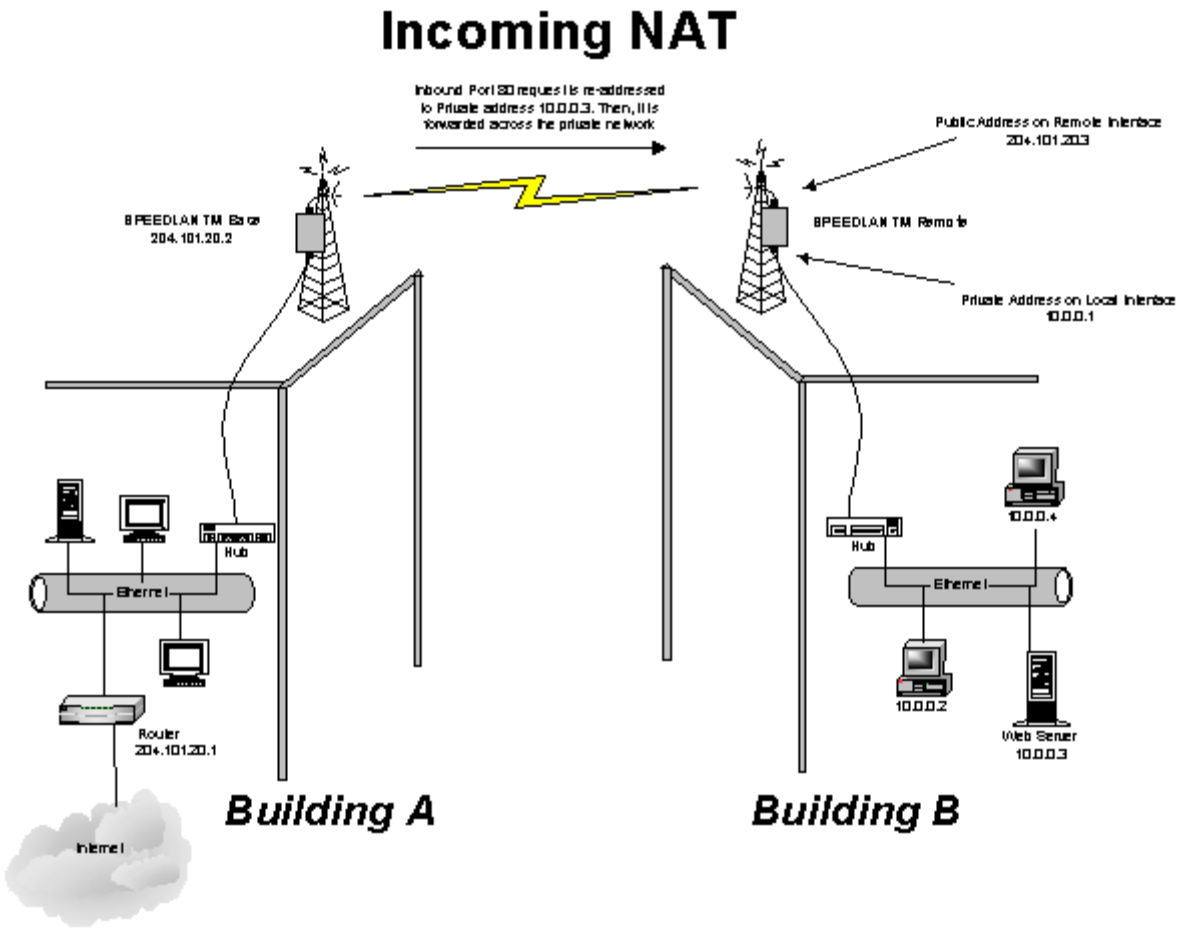
Network Address Translation (NAT) occurs when there is a translation among an Internet Protocol (IP address) used within one network (designated as inside network) to a different IP addresses within another network (designated as outside network). Network Address Translators (NATs) allow companies to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

Outgoing NAT



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

Incoming NAT



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 on a server is IP Address 10.0.0.3, you can create a pair that will specify that all requests received 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

In this section you will first assign a static IP address or enable the DHCP client. Second, choose the appropriate interface for the DHCP client. Third, enable the DHCP Server on the SPEEDLAN TM.

> **Note:** Confirm the IP address of your SPEEDLAN TM units by performing the following tasks. Open the SPEEDLAN TM 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:

1. **Physically assign a static IP address (Static IP)**

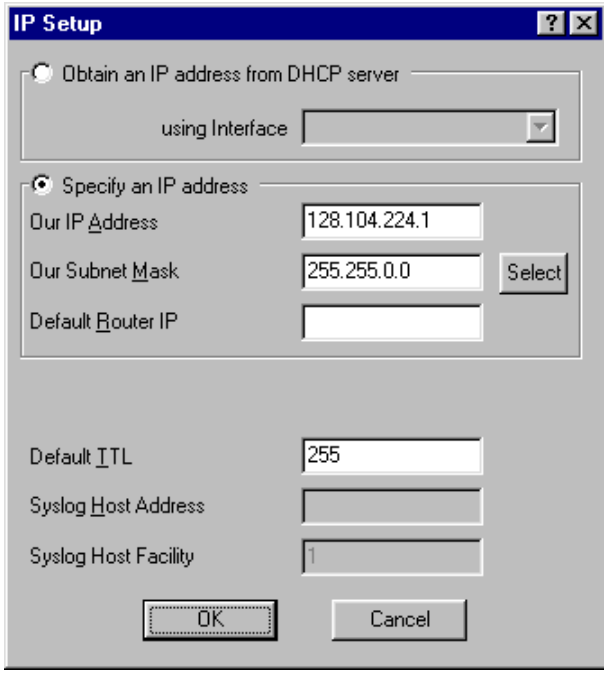
2. **Enable DHCP client and choose appropriate interface (Dynamic).**

   Note: After following Option #2 above, proceed to *Enabling the DHCP Server on the SPEEDLAN, page 59*.

Physically Assigning a Static IP Address

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

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



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 the computer on the Internet (i.e., 128.104.224.2).
   - **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 the figure called Subnetting a Network in the section called *Part I - A Quick Overview of IP Addressing, page 48*. Once the packet has traveled to the appropriate network, it goes through a masking process. A subnet mask is composed of zeros (0s) and (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 the method packets the 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**.

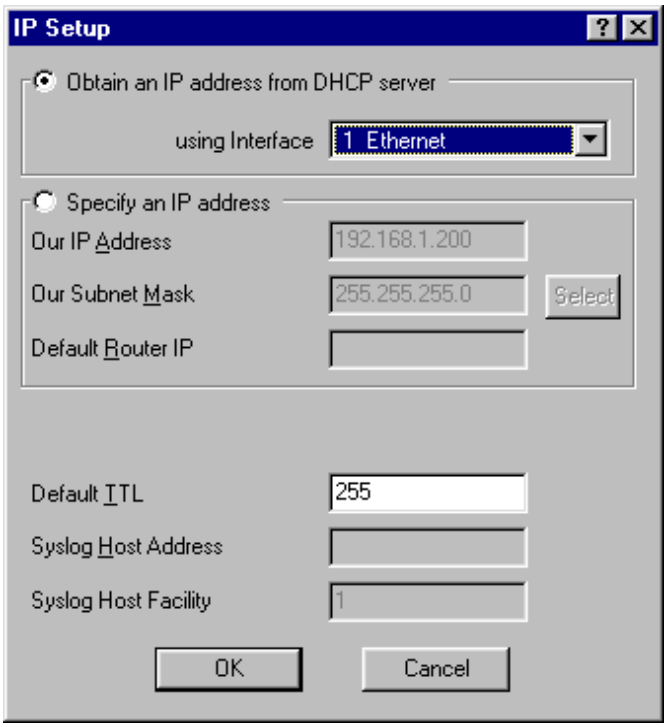
5. A message box appears informing you that the information will be saved to the brouter (i.e., 128.104.22.4). Click **Yes**.

6. The Configurator confirms that the configuration has been saved. Click **OK**. Restart the computer.
   Note: You are finished with this section. If you want to set up NAT, see *Part III - Setting Up NAT, page 61*.

Enabling the DHCP Client and Choosing the Appropriate Interface

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.



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

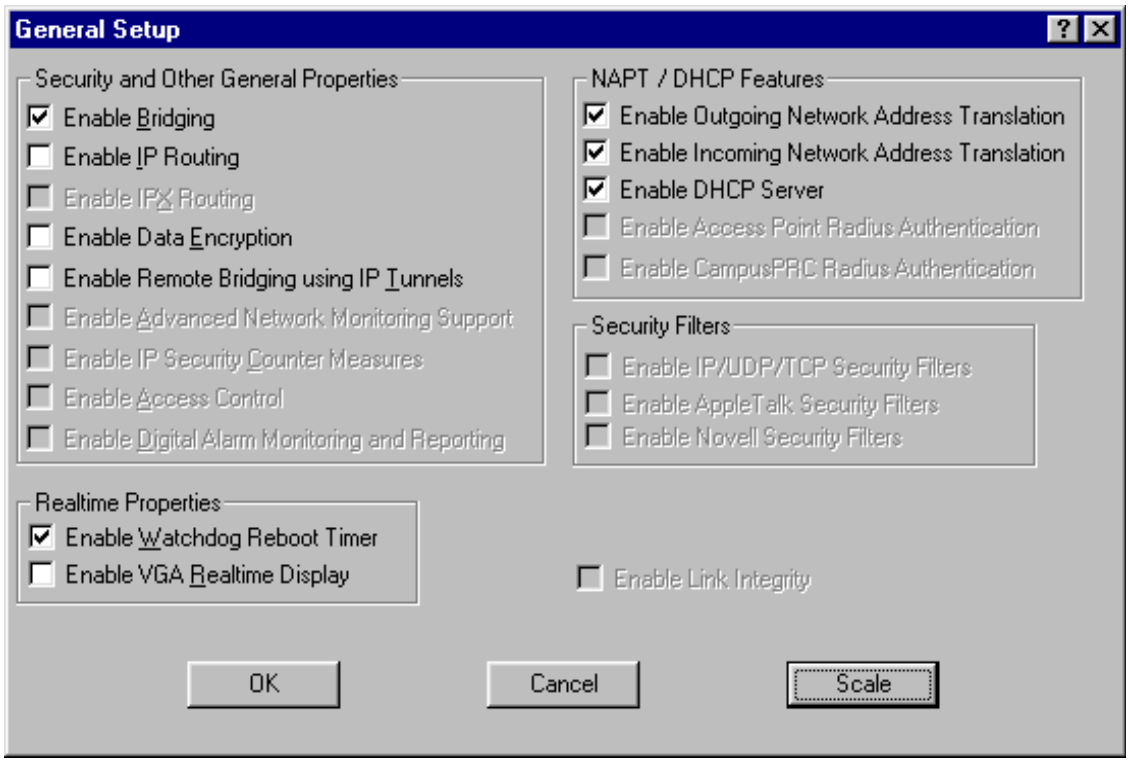
3. Next, select the interface for Ethernet or wireless network from the Using Interface drop-down list. Make sure that you select the interface that the DHCP server is located on.

   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 unless you are very familiar with IP functionality and how the Time to Live parameter will affect the method packets the treated by your network, as well as the network to which you are bridged (or routed).

Enabling the DHCP Server on the SPEEDLAN TM

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

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



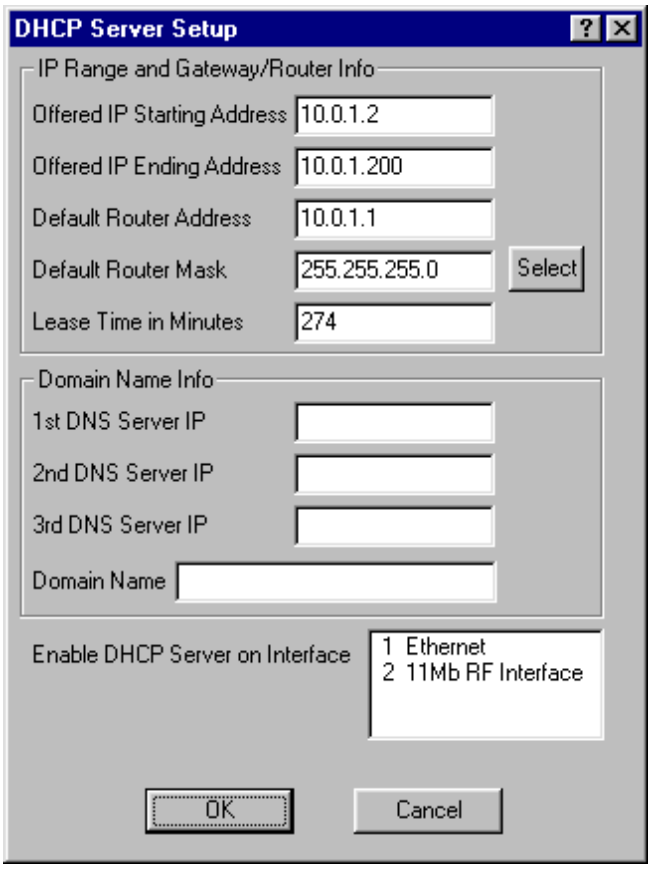
2. Select the **Enable DHCP Server** check box; this will enable you to set up the DHCP Server.

   Note: The only active NAT / DHCP check boxes in the NAPT / DHCP Features section (in the dialog box above) are the following:

   - **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 *Part III - Setting Up NAT*, *page 61*.
   - **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 *Part III - Setting Up NAT, page 61*.

3. From the **Setup** menu, choose **DHCP Server Setup**. The DHCP Server Setup dialog box appears (as shown on the next page).

4. Enter the IP range and gateway/router information:
   - **Offered IP Starting Address** – This is the start of the block of allowed IP addresses. For example, the "offered" IP address between a block of 20 to 40 is 20.
   - **Offered IP Ending Address** – This is the end of the block of allowed IP addresses. For example, the "ending" IP address between a block of 20 and 40 is 40.
   - **Default Router Address** – This is the IP address of the default router that allows clients to move outgoing packets to a single router on the same subnet.
   - **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 be reassigned to another computer.



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

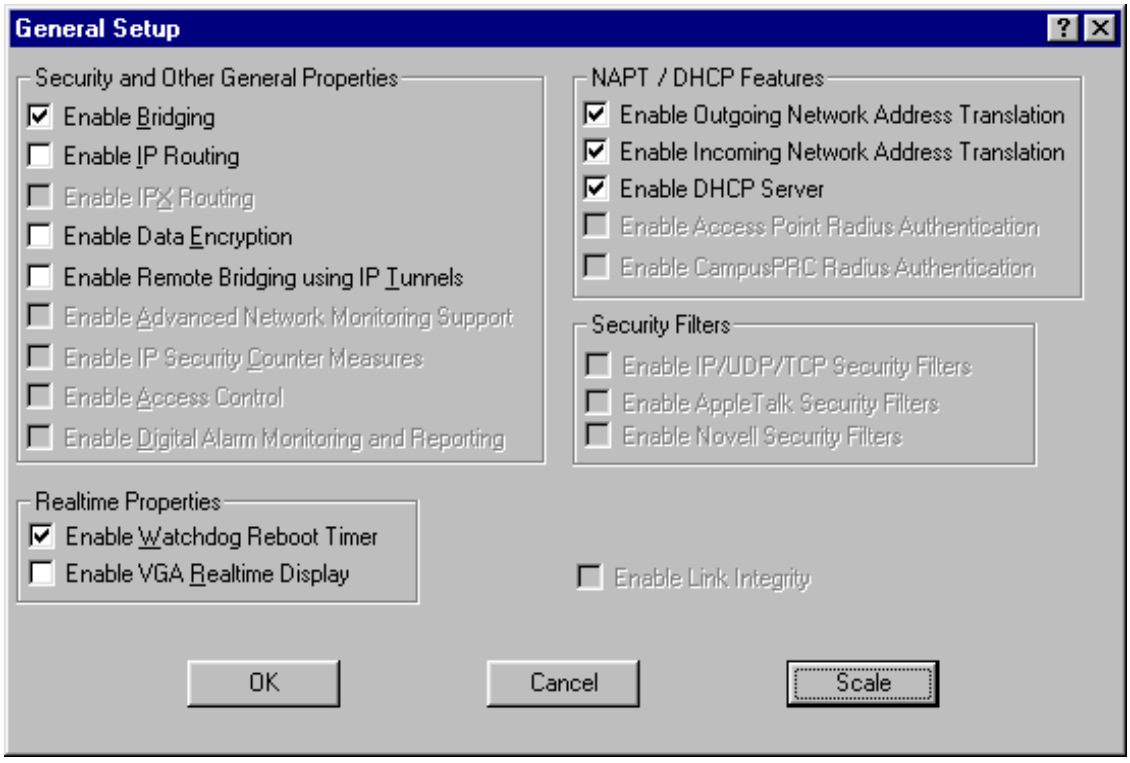
5. Enter the domain name information:
   - **1st DNS Server IP** – This setting will specify the client's 1st DNS Server.
   - **2nd DNS Server IP** – This setting will specify the client's secondary DNS server.
   - **3rd DNS Server IP** – If needed, this setting will specify the client's third DNS 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 that you want to Enable DHCP on (i.e., Ethernet or wireless interface).
7. Click **OK**.
8. After you have finished entering the appropriate information, click **OK**.
9. Now save the changes to the bridge or router. 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**. Restart the computer.

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 *pages 54 and 55*.

To setup outgoing NAT, do the following:

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

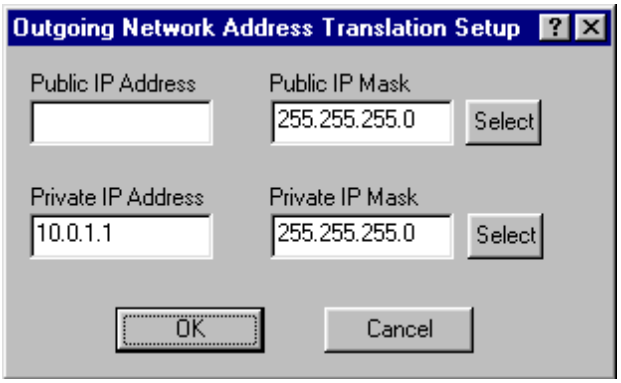


2. Select the **Enable Outcoming Network Address Translation** check box. Click **OK**.

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

4. The Outgoing Address Translation Setup dialog box appears (as shown on the next page).

Note: NAT is a useful tool that will be enabled the majority of the time on the client or satellite side of the SPEEDLAN ISP or SPEEDLAN MP. It is rarely enabled on the base unit. 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 pulbic 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.



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 (computer) 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 unit.
   - **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**.

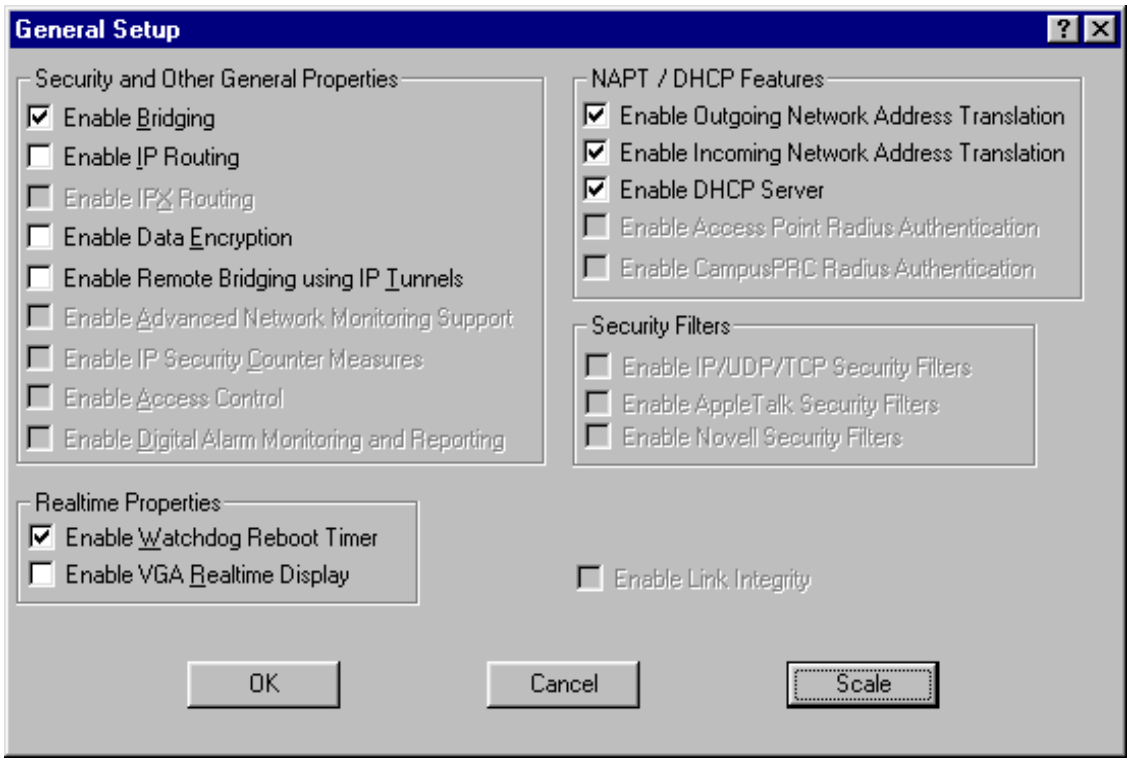
8. Now save the changes to the bridge or router. From the **File** menu, choose **Save Config**.

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

10. The Configurator confirms that the configuration has been saved. Click **OK**. Restart the computer.

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

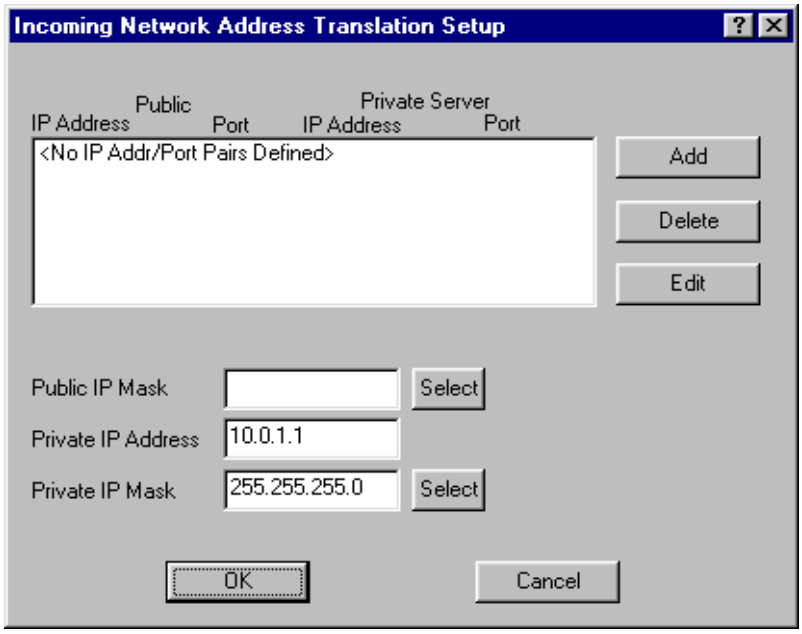
1. From the **Setup** menu, choose **General Setup**. The General Setup dialog box appears.



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 (as shown on the next page).



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**.