# SPEEDLAN 9000 Series

*Installation and Operation User Guide Version 1.0*

*Last Revised: March 2002*

A SPEEDCOM WIRELESS CORPORATION

Copyright/Liability

Copyright ©2002. Wave Wireless Networking. All rights reserved. SPEEDLAN and SPEEDCOM are registered trademarks of Wave Wireless Networking. SPEEDView, Wave Wireless Networking and the Wave Wireless Networking logo are trademarks of Wave Wireless Networking. All other trademarks mentioned in this document are the property of their respective owners.

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.

For more information, contact Wave Wireless Networking at:
Wave Wireless Networking
7020 Professional Parkway East
Sarasota, FL 34240
www.wavewireless.com

Technical Support
941-907-2300 (phone)
941-355-0219 (fax)

**Chapter 1 - Introduction ..... 1-1**
Features and Benefits ..... 1-2
SPEEDLAN 9000 Series Features..... 1-2
ISP Functionality ..... 1-2
Configuration and Monitoring ..... 1-3
Wired LAN Interface..... 1-3
Wireless LAN Interface ..... 1-3
SPEEDView (A Network Management Tool) ..... 1-4
IP-Router Features ..... 1-4
Additional Functionality for SPEEDLAN 9000 RF cable loss is negligible ..... 1-4
Equipment Features..... 1-4
SPEEDLAN K2's Polling Protocol -- How it Works in Star Networks ..... 1-5
Point-to-Multipoint Functionality..... 1-5
Point-to-Point Functionality ..... 1-7
SPEEDLAN 9000 Mesh Protocol -- How It Works in Non-Line-of-Sight Networks..... 1-8
Routing Around Obstacles..... 1-10
SPEEDLAN's NLOS Pico Cell Architecture ..... 1-11
SPEEDLAN 9000 Mesh Protocol's Core Components ..... 1-11
Network Expansion: Connecting Buildings in a SPEEDLAN 9000 Network ..... 1-12

**Chapter 2 - Installing the SPEEDLAN 9101 & SPEEDLAN 9102 Hardware..... 2-1**
Rooftop and Tower Installations Warning ..... 2-2
Hardware Overview ..... 2-2
Drawings of Outdoor, Remote-Mounted Components..... 2-2
Indoor Junction Box ..... 2-2
The SPEEDLAN 9101 (with an Attached Standard Omni) ..... 2-3
Bottom View of SPEEDLAN 9101 ..... 2-3
System Description..... 2-4
Package Contents..... 2-4
Installation Steps for the SPEEDLAN 9101 ..... 2-5
Installation Diagram of the SPEEDLAN 9101..... 2-6
The SPEEDLAN 9102 (with an External Antenna)..... 2-8
Bottom View of SPEEDLAN 9102 ..... 2-11
System Description..... 2-1
Package Contents..... 2-11
Installation Steps for the SPEEDLAN 9102..... 2-12
Installation Diagram of the SPEEDLAN 9102..... 2-17

**Chapter 3 - Using the SPEEDLAN 9000 Configurator ..... 3-1**
Initial Configuration of the SPEEDLAN 9000 .....3-2
Prerequisites .....3-2
Configuring the SPEEDLAN 9000..... 3-3
Wireless Interface IP Address Assignment ..... 3-4
Automating the Configuration of Multiple SPEEDLAN 9000s ..... 3-4
Completing Configuration..... 3-4
Adding Additional SPEEDLAN 9000s to the Wired Network ..... 3-4

Overview of the SPEEDLAN 9000 Configurator Main Menu ..... 3-5
Logging on to the SPEEDLAN 9000 Configurator ..... 3-6
Logging On ..... 3-10
After Logging On ..... 3-11
Interfaces ..... 3-11
Setup ..... 3-12
Interface Parameters ..... 3-13
System ..... 3-16
General ..... 3-16
Performance ..... 3-17
Password ..... 3-18
Routing ..... 3-18
Def Gateway ..... 3-18
Route Table ..... 3-19
Static Route ..... 3-19
Wireless ..... 3-21
Configuration ..... 3-22
DHCP Server ..... 3-24
How DHCP Assigns an IP Address ..... 3-24
Basic Instructions for Setting Up DHCP on an Interface ..... 3-25
Elements Defined on the General and Known Client Pages ..... 3-27
Viewing Log Messages ..... 3-30
Enabled Interfaces ..... 3-30
DHCP Relay ..... 3-30
NAT ..... 3-31
Outgoing NAT ..... 3-32
Incoming NAT ..... 3-33
Diagnostics & Troubleshooting ..... 3-35
Interface Statistics ..... 3-35
ARP Table ..... 3-36
ICMP Statistics ..... 3-37
Connectivity ..... 3-39
System Control ..... 3-39
Administrative Access Pages ..... 3-40
User Configuration ..... 3-40
Replication ..... 3-42
Remote Control ..... 3-43
Factory Reset ..... 3-43

**Chapter 4 - Using SPEEDView ..... 4-1**

What is SPEEDView? ..... 4-2
System Requirements ..... 4-2
Installation Instructions ..... 4-2
Starting SPEEDView ..... 4-3
Star Network ..... 4-5
Mesh Network ..... 4-6
The Program Instructions ..... 4-6

The Main Tab .....4-7
The Main Tab Icons .....4-8
The Node, Link, Stats and View Menus (on the Main tab) .....4-10
Buttons (on the Main tab) .....4-11
Performing a Bandwidth Test .....4-13
Performing a Ping Test .....4-14
Accessing the Statistics Tabs on Bottom of Main Tab..... 4-15
Options Tab ..... 4-19
Admin Tab ..... 4-21

**Chapter 5 - Basics of IP Addressing ..... 5-1**
Basics of IP Addressing .....5-2
What is an IP address? .....5-2
Internet Address Classes .....5-2
Subnetting a Network .....5-4
How does a network administrator assign an IP address? .....5-7
What is DHCP? .....5-7
What is NAT? .....5-9
NAPT .....5-9
Diagram of Outgoing NAT .....5-10
Diagram of Incoming NAT .....5-11

**Glossary for Standard Data Communications**
**Software License Agreement**
**Wave Wireless Networking LIMITED WARRANTY STATEMENT**
**FCC Statement**

Notes:

# Chapter 1
# Introduction

# Features and Benefits

## SPEEDLAN 9000 Series Features

The SPEEDLAN 9000 series offers the network manager unsurpassed flexibility in meeting the challenges of designing, building and managing today's wireless broadband networks. Because the 9000 series routers support both mesh and star topologies, they provide the network manager powerful tools with which to build complex networks. This allows wireless broadband networks and services to be extended on a greater scale, and to more buildings than ever before. The 9000 series are all remote-mounted 11 Mb routers that are installed on the building's rooftop which help reduce signal loss.

In a mesh topology, the SPEEDLAN 9000 series routes around physical limitations, eliminating the line-of-sight (LOS) issue present in star topology-only networks. This self-healing mesh topology process enables each router to be heard on the network. By removing LOS issues caused by large buildings, hills, and other obstructions, service providers can reduce network deployment costs while maximizing their broadband wireless investment and reach new markets that could otherwise not be served. Each router in a mesh topology can communicate up to a 1/2 mile with its neighboring router, or greater depending on its antenna configuration.

In a star topology, the router can act as a polling central base station or as polling Customer Premise Equipment (CPE). CPE will only transmit when instructed by the base station. This process helps conserve bandwidth and reduce costs as well. Links in a star topology can reach distances up to 25 miles, depending on its antenna configuraton.

The SPEEDLAN 9000 series is an all-in-one solution allowing a multitude of network options for the service provider to offer a variety of network options: stand-alone, point-to-point, point-to-multipoint, self-healing mesh, or a combination of all. For information on the type of routers included in the SPEEDLAN 9000 series, see *Equipment Features, page 1-4*.

## ISP Functionality

The SPEEDLAN 9000 series is tailored to fit the needs of Internet Service Providers (ISPs) and Broadband Telecommunications Providers. ISPs currently providing service can increase customer density in an existing area or in a new area. ISPs looking to service MDU/MTU environments, universities, corporations and manufacturing campuses (etc.) needing inter-building connectivity can use the SPEEDLAN 9000 series to overcome line-of-sight (LOS) restrictions between buildings. Also,

ISPs can beat cost and time roadblocks that are normally associated with wired infrastructure networks.

The SPEEDLAN 9000 series presents an unparalleled level of performance and features, including Network Address Translation (NAT) and Dynamic Host Control Protocol (DHCP) server. NAT increases network security and allows the occupants of an entire building to share a single global IP address. DHCP server allows IP addresses be assigned dynamically at the remote building. Distributing these administrative functions to each remote building significantly reduces the "administrative overhead" traffic that must travel back to the service provider's headquarters.

## Configuration and Monitoring

- web-based management system
- IP addressing
- Set security parameters (read-only, administrative or full access)
- Set data rate and frequency
- Perform ISP-related functions
- Firewall protection
- Encryption
- Diagnostic features
- Link test
- Firmware upgrades
- SNMP supported in future

## Wired LAN Interface

- Compliance: IEEE 802.3 Ethernet
- Physical interface: 10Base-T, 10/100Base-Tx
- Supports: IP, TCP, UDP, ICMP, RIPv1, Ripv2, OSPF, SNMP, TFTP, IGMP, ARP, DHCP relay, DHCP server, DHCP client, NAT
- Network Addressing: MAC address of the Ethernet interface

## Wireless LAN Interface

- Single 11 Mb interface
- Uses star (via SPEEDLAN $K^2$ polling protocol) or mesh topologies (via Mesh protocol)
- Range: up to 25 miles (with amplifier)

### SPEEDView (A Network Management Tool)

- Provides an "at a glance" view of activity in each NLOS pico cell, as well as in a line-of-sight (star) network.
- Monitor and control management functions with this Windows-based management tool for local and remote units/routers from any location on the network, including mobile hand-held devices (e.g., iPAQs) for "on-site" monitoring.
- View and configure many parameters and services for unit/router by double-clicking any unit/router icon. This action will open the SPEEDLAN 9000 Configurator.

### 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 - not supported yet
- Strong encryption (AES) supported

### Additional Functionality for SPEEDLAN 9000 RF cable loss is negligible

- Units/routers can be mounted in more remote locations because Ethernet cable is connected to other units/routers
- 10/100 BASE-T Ethernet interface

## Equipment Features

The SPEEDLAN 9000 series offers all the equipment you need to meet your connectivity requirements:

Decide on the type of unit/router you will need.

- **SPEEDLAN 9101:** A unit/router used in a non-line-of-sight pico cell (using the Mesh protocol) is referred to as a SPEEDLAN 9101. This unit/router contains a standard, omni antenna which is directly attached on the top. You do not need an external antenna. In addition, the parameters are configured with the Mesh protocol in the SPEEDLAN 9000 Configurator.

  This type of self-healing mesh topology process helps you reach buildings that do not have a clear line-of-sight back to the base station without the possibility of interference from hidden transmitters. For more information on this topic, see *SPEEDLAN 9000 Mesh Protocol -- How It Works in Non-Line-of-Sight Networks, page 1-8*.

- **SPEEDLAN 9102**: Can be used with the $K^2$ polling protocol or the Mesh protocol:
  - $K^2$ polling protocol : A unit/router used in star networks such as a remote station (CPE), point-to-point or as a base station is referred to as a SPEEDLAN 9102. The parameters on this unit/router are configured via the $K^2$ polling protocol in the SPEEDLAN 9000 Configurator. This unit/router uses an external antenna, such as a grid, sectoral, etc. For more information on how the $K^2$ polling protocol works, see *SPEEDLAN $K^2$'s Polling Protocol --How It Works*. If you need to use an amplifier with the SPEEDLAN 9102, see *If Using An Amplifier with the SPEEDLAN 9102, page 2-16*.
  - Mesh protocol: Most users needing the mesh topology solution will use the SPEEDLAN 9101. However, there is the option of using an external antenna (e.g., high-gain omni antenna, sectoral or directional). If you choose this option, use the SPEEDLAN 9102, and it can act as a mesh topology solution.

**Note:** A SPEEDLAN 9102 is shipped as mesh, CPE star or base star. Mesh and CPE star are user ready. If you need to use the unit/router as a base star (or base station), you must contact Wave Wireless to order the "key" to activate this functionality.

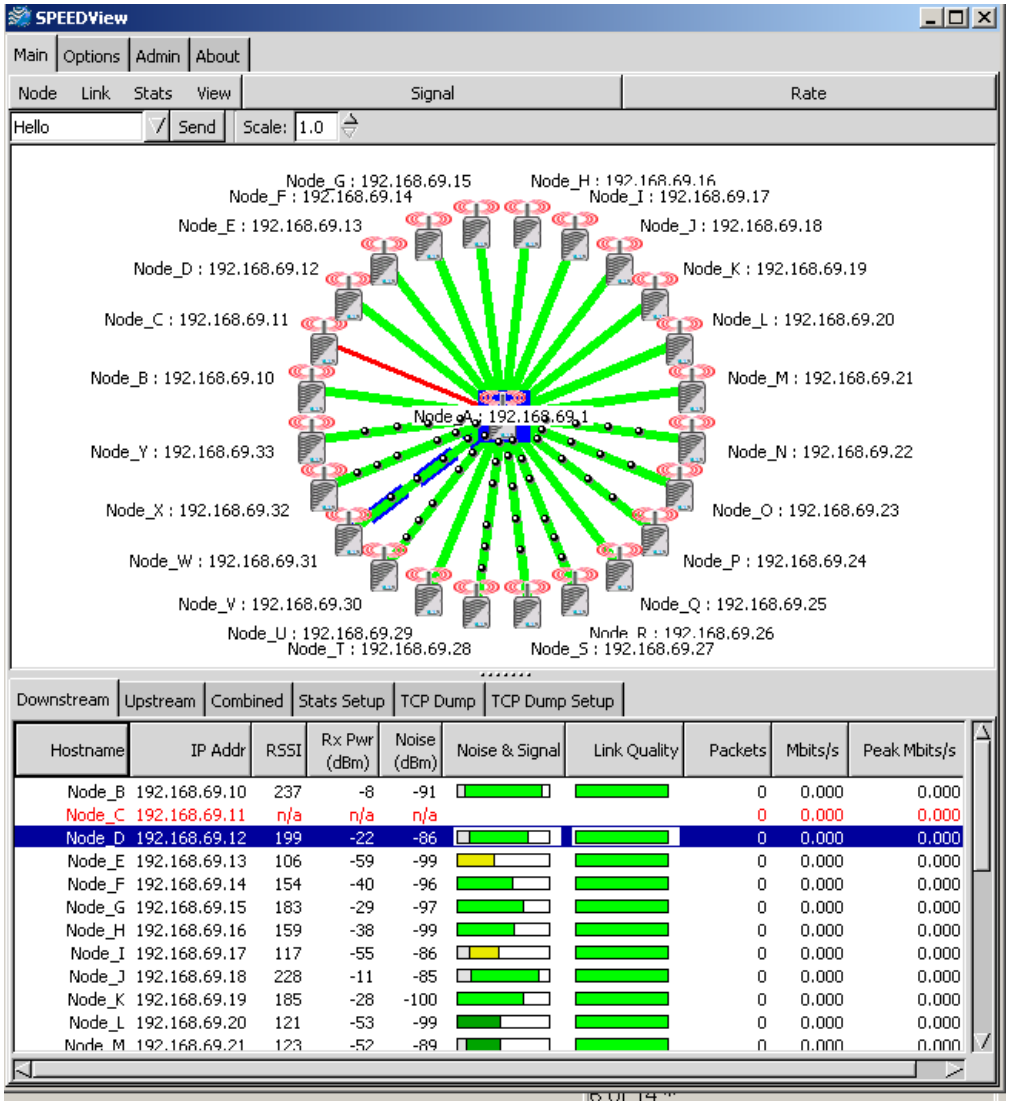
## SPEEDLAN $K^2$'s Polling Protocol -- How it Works in Star Networks

Here are the popular scenarios for star networks using the SPEEDLAN $K^2$ polling protocol: point-to-multipoint (CPE and base station) and point-to-point (one unit/router talking to another, and a base station if needed). If any of the SPEEDLAN 9102 units/routers are unable to see each other, a base station must be used to repeat traffic to next unit/router in line.

### Point-to-Multipoint Functionality

A point-to-multipoint network consists of a group of units/routers (Customer Premise Equipment, hereon abbreviated as CPE) and a base station. The network is based on a star topology (as shown in the following graphic), thus CPE must have clear LOS to the base station. The base station acts as the "traffic cop" within the network, making use of a polling protocol in order to control the flow of data between the CPE and the base station. The base station continuously polls the CPE, allowing CPE the opportunity to transmit some data via their wireless interface. This configuration solves the "hidden transmitter" problem since CPE will only transmit when instructed to do so by the base station.

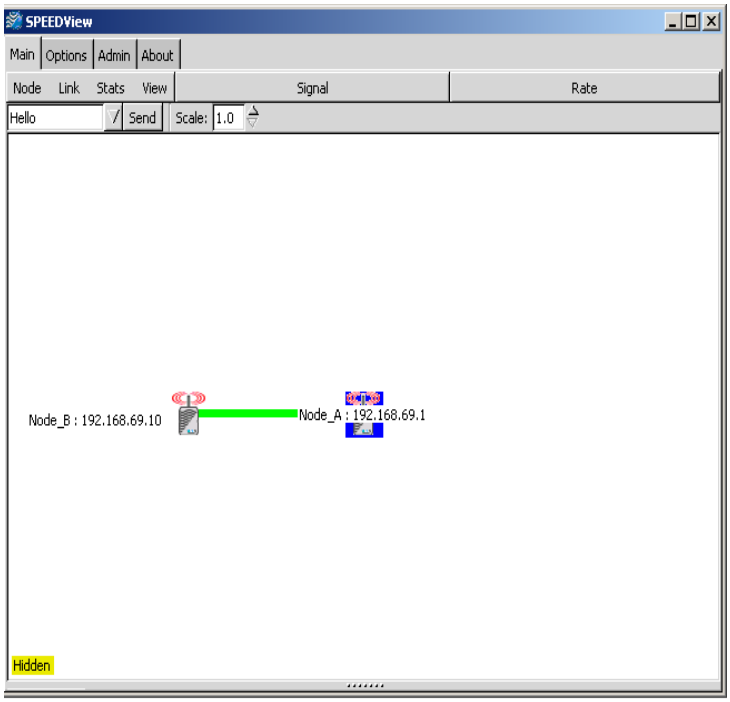
The amount of traffic the CPE is allowed to transmit within each poll interval changes dynamically based on configuration information and the network wide traffic mix at any specific point in time (as shown in the following graphic). CPE can be limited to a maximum amount of bandwidth in the upstream direction (from CPE to base). Similarly, the base can be configured to limit the amount of data transmitted in the downstream direction (from base to CPE) on CPE by CPE basis.




Using SPEEDView, the graphic above illustrates a point-to-multipoint network topology. The SPEEDLAN 9102 base station (unit/router in blue square in the middle) polls the CPE. The black "beads" are used to indicate how much bandwidth is being used at a given point in time. The higher

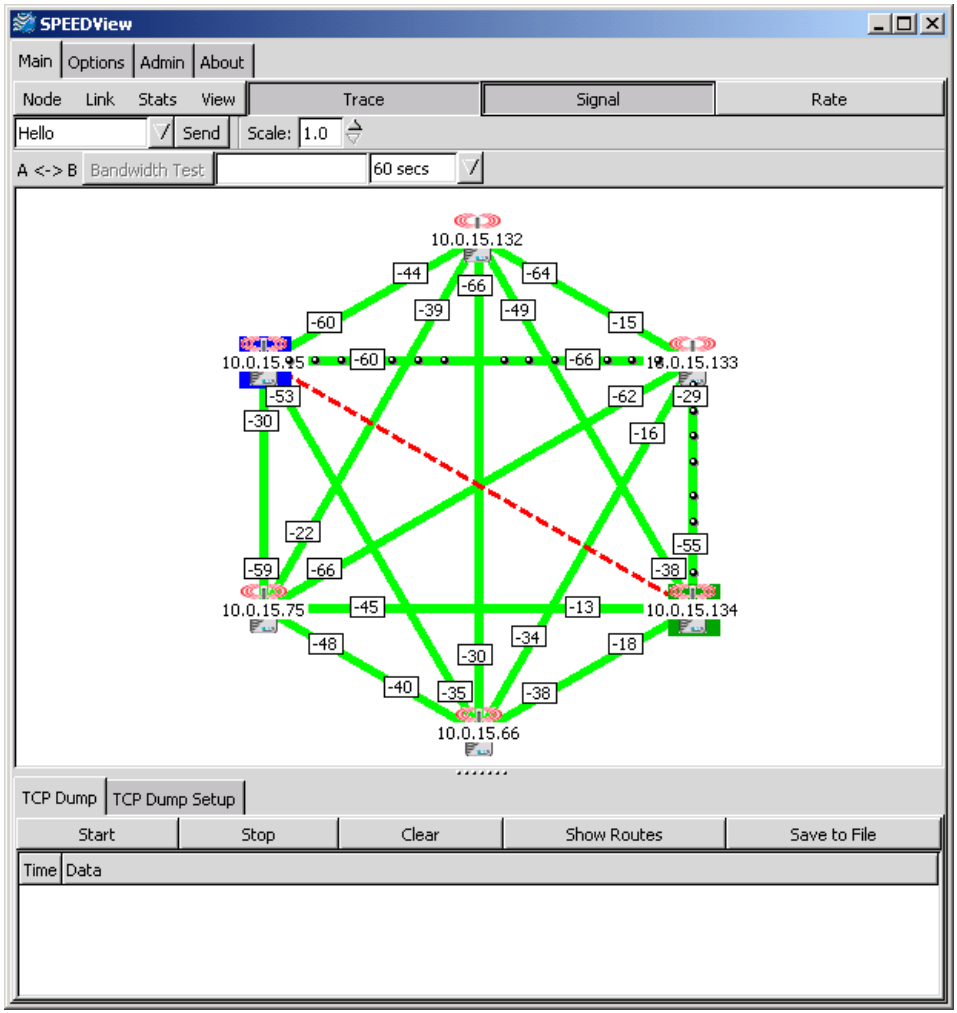
the number of beads shown on the link, means that there is more traffic being transmitted on the link (at that moment in time). The base station controls when and which CPE can transmit.

## Point-to-Point Functionality




The point-to-point network is the simplest form of the fixed wireless network: a single link between two wireless units/routers having line-of-site, as shown in the graphic above via SPEEDView. These links work well for dedicated connections but do not scale very well. If any of the units/routers are unable to see each other, a base station must be used to repeat traffic to next unit/router in line.

# SPEEDLAN 9000 Mesh Protocol -- How It Works in Non-Line-of-Sight Networks




Using SPEEDView the graphic above shows that every unit/router in the non-line-of-sight (NLOS) network can be heard. These products provide the unique ability to "self-heal the network" as a sector's topography or geography changes over time, and reach buildings blocked by obstructions within line-of-sight.

What is happening in the graphic above?

- You will notice negative numbers next to the units/routers, or referred to as nodes on the network diagram. These numbers represent the signal strength for the nodes (or units/routers) in the diagram.

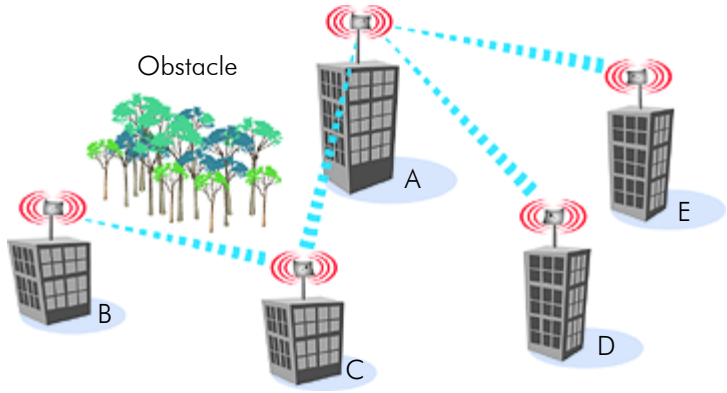
- You will note that the Trace button is selected, which traces the data flow between the selected pairs or links. This example displays a trace route (hint: look for black beads) between the selected nodes. You will see the links chosen by the routing algorithm in order to send data from the source node to the destination node.
- SPEEDView also displays the broken links, and you can also use the "Block" feature to test a "mock" link that is disconnected. The broken (or disconnected) link will appear as a red, dashed line. This link appears when there is no signal strength between nodes. This example displays a broken mock link between the node pair.
- SPEEDView also displays the data flow (upstream, downstream and combined total) for the selected nodes on the network in the lower window which is referred to as the Statistics window. SPEEDView can also be used to perform bandwidth, link and ping tests. For more information about SPEEDView, see the separate document titled, "SPEEDView Quick Start Guide."

### So, how do mesh topology solutions reach buildings obstructed from line-of-sight issues?

Based on the routing protocol called Topology Based Reverse Path Forwarding (TBPPF), SPEEDLAN's mesh technology provides each unit/router the unique ability to learn multiple network paths that traffic can follow. Using specialized routing algorithms, its network radios are updated without degrading bandwidth or efficiency, as with other full-topology protocols.

The rest of this section explains each unique component of a mesh topology solution: how it routes around obstacles, its NLOS pico cell architecture, Mesh protocol's core components, and how it expands or integrates with the network.

## Routing Around Obstacles




Explaining this scenario on the simplest level (using the Mesh protocol as shown in the graphic above), A can route a packet to B, despite the tree obstruction (block of trees) within the path. How does this procedure work?

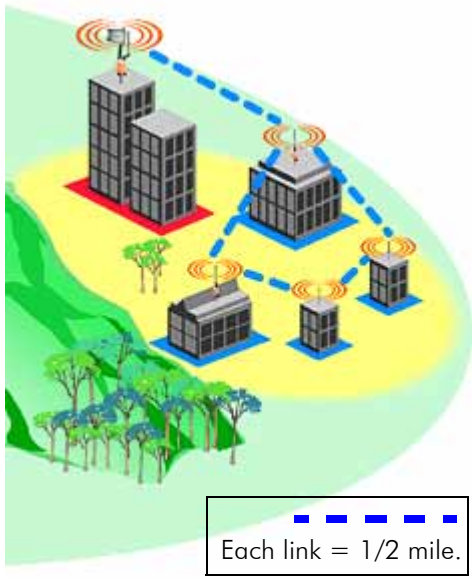
1. A can see that there is not a clear path to B.
2. C can see that there is a clear path to B. The most efficient path in this case is to hop from A to C to B.

**Note:** No manual programming is required because A automatically detects its neighboring unit/ router (in this case C, and B and detect a clear path to C). Therefore, the packet is successfully re-routed around the obstacle (between B and A).

This process creates a more scalable, flexible, and extended wireless network (as shown in *Network Expansion: Connecting Buildings in a SPEEDLAN 9000 Network, page 1-12*).

## SPEEDLAN's NLOS Pico Cell Architecture

Each SPEEDLAN 9101 or SPEEDLAN 9102 in a NLOS pico cell can communicate up to a 1/2 mile with its neighboring unit/router.




## SPEEDLAN 9000 Mesh Protocol's Core Components

SPEEDLAN 9000 Mesh protocol includes three central components:

### Neighbor Discovery

Neighbor discovery occurs when each unit/router sends a broadcast "hello" message to determine which units/routers are linked to the network. ("Hello" messages are much smaller than other protocol messages, which conserves bandwidth on the network.) These units/routers then send back a message to the originating source via the most efficient network path. These messages are formed containing only the basic information needed to educate the routers, as to which neighbor belongs to whom.

### Topology Updates

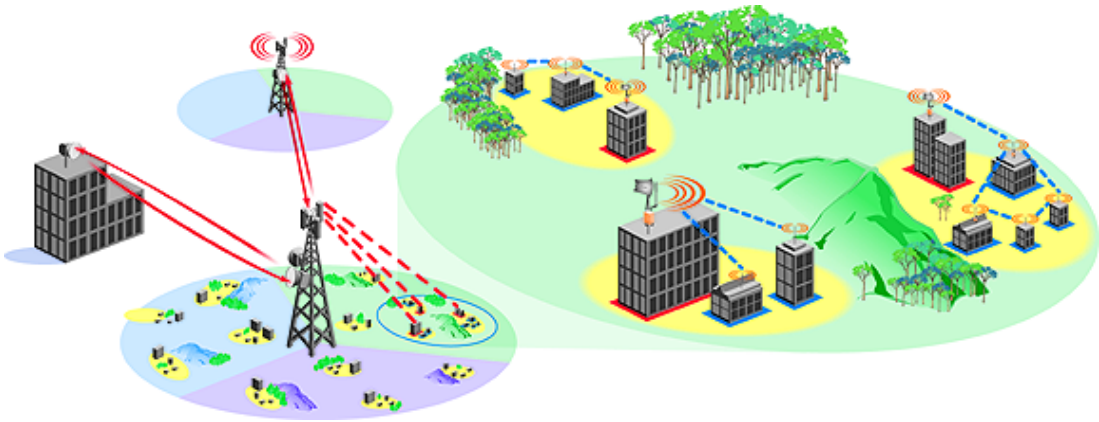
Initial neighbor discovery, caused by adding a new or removing an expired unit/router, precipitates a topology change to all other routers so that their routing tables can be updated. Once established on the network, "hello" messages are confined to changes in a router or its neighboring status. These messages will keep all routing tables current: keeping track of connections. This process helps to maintain an efficient network.

### Routing

Routing is simply the act of guiding a packet from one destination to another, whether on the same network or across multiple networks. A router keeps a table or a "route map" of its neighbors and the best path to other known networks. Many routers use a "hop" count to determine the number of hops that a packet travels. A "hop" can be defined as the trip that a data packet takes from one router (or intermediate point) to another on the network.

The SPEEDLAN 9000 outperforms other units/routers because the SPEEDLAN 9000 routing table broadcasts only the information that changed, such as when new routes are added or old routes are removed from the network. This information is sent to the units/router's immediate neighbors along the most efficient path to the end destination. This process helps conserve bandwidth. If an existing path is modified in some way, by the addition or deletion of a router, a SPEEDLAN 9000 using the Mesh protocol can monitor its routing table to decide if a secondary path should be taken. One could call this a "self-healing" network, which means it finds a secondary route through the network without manually reprogramming the units/routers.

## Network Expansion: Connecting Buildings in a SPEEDLAN 9000 Network



Use SPEEDLAN 9102 units/routers to connect clients within LOS via the $K^2$ protocol. Connect buildings obstructed by LOS issues with SPEEDLAN 9101 units/routers, or with SPEEDLAN 9102 units/routers in a NLOS pico cell. It is important to understand how different SPEEDLAN 9000 units/routers can be used together, such as follows:

### Designing a Broadband Wireless MAN

Using a mix of wireless technologies, SPEEDLAN makes it possible to design a wireless MAN capable of delivering high-speed Internet services to a variety of buildings. In the installation diagram above, the ISP has installed three polling base stations, two high-speed microwave links,

and several SPEEDLAN 9000 units/routers. Connecting base stations to a high-speed backhaul provides the necessary bandwidth for network expansion and eliminates bandwidth bottlenecks.

### Broadband Backbone Links

The two-high speed microwave links provide full-duplex 100Mb/s backbone links to other areas of the MAN. These 100Mb/s microwave backbone links provide the necessary bandwidth for network expansion and eliminate bandwidth bottlenecks. Service providers can save money because they will no longer have to depend on backhaul support from the telecommunications infrastructures.

The three polling base stations create a broadband wireless MAN, while operating independently from the telecommunications infrastructure. The three base stations have been installed on three non-overlapping 2.4 GHz channels, providing 11 Mb/s of connectivity to three sectors of the network (total of 100Mbps). This effectively gives the ISP a 33 Mb/s base station from which to increase the network penetration and user density. Each remote base station uses directional antennas to achieve maximum distance and to prevent interference from the other base stations. These sectorized base stations then connect to SPEEDLAN 9000s, which are located in NLOS pico cells throughout the sectors (represented as yellow, circular cells in the diagram above). As a provider's network grows, connections may be expanded incrementally to create entire wireless metropolitan area networks, up to 25 miles from the base station.

### Building a SPEEDLAN 9000 Network

The SPEEDLAN 9000 series can be spread throughout the MAN to make it possible to deliver high-speed Internet services to a wide variety of buildings: enterprises, schools, hospitals, to companies that relocate or need to expand their network. Previously, the ISP could not reach these buildings blocked by LOS limitations, such as hills and trees. The SPEEDLAN 9000 series contains the Mesh protocol to go around obstructed buildings. These specialized networks are referred to a NLOS pico-cells. (In the previous diagram, these NLOS pico cells are represented as yellow, circular cells.)

### NLOS Pico Cells

Each unit/router in a NLOS pico cell is capable of routing data to its destination. Traffic can be routed around buildings, trees, and other obstructions because this NLOS unit/router simply locates the next closest unit/router within LOS.

Notes:

# Chapter 2
# Installing the SPEEDLAN 9101 & SPEEDLAN 9102 Hardware

## Rooftop and Tower Installations Warning

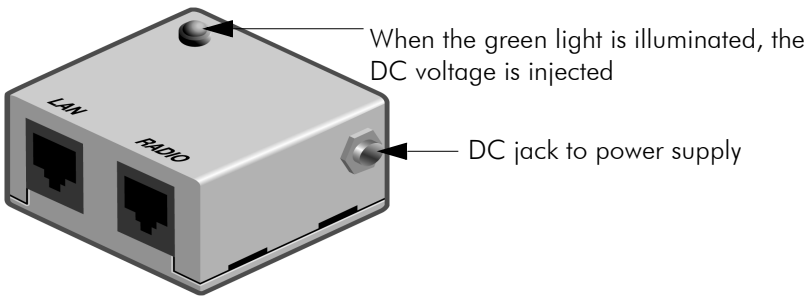
Rooftop, tower and mounted equipment (routers) installations are extremely dangerous and incorrect installation can result in death, injury, or property damage.

## Hardware Overview

The SPEEDLAN 9000 series contains the following units/routers: SPEEDLAN 9101 and the SPEEDLAN 9102. For more information, see *Equipment Features, page 1-4*. All SPEEDLAN 9000 series equipment (SPEEDLAN 9101 and SPEEDLAN 9102), use the outdoor, remote-mounted chassis and are installed on the rooftop (on pole or mast). The following are components for both the SPEEDLAN 9101 and SPEEDLAN 9102:

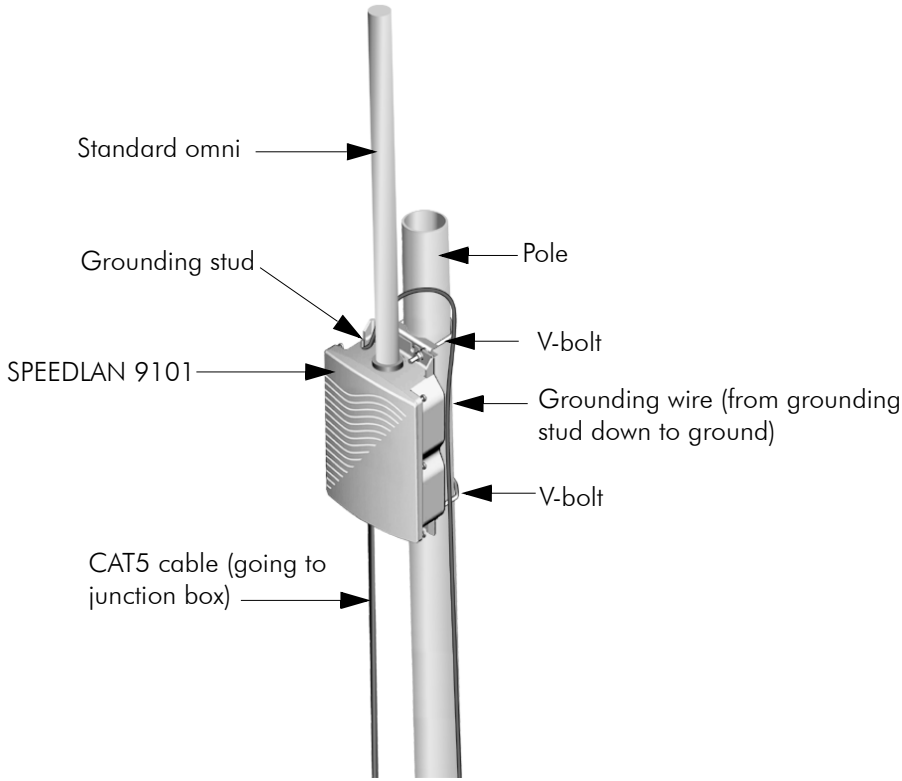
## Drawings of Outdoor, Remote-Mounted Components

### Indoor Junction Box

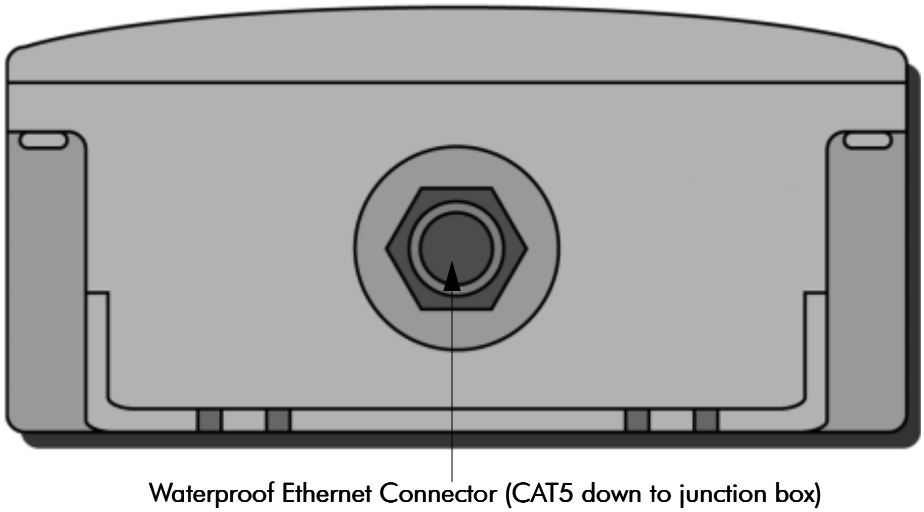



The indoor junction box is used with the SPEEDLAN 9101 and SPEEDLAN 9102.

# The SPEEDLAN 9101 (with an Attached Standard Omni)




## Bottom View of SPEEDLAN 9101



## System Description

These are high-speed, long range wireless LAN outdoor, remote-mounted units/routers that provide connectivity to units/routers operating in a NLOS pico cell.

## Package Contents

- SPEEDLAN 9101
- Product registration card
- CD containing: Product manual, SPEEDView management Software and SPEEDView Quick Start Guide
- Indoor junction box
- Standard, omni antenna is attached to the router
- V-bolts

The following items are included with the installation kit, which can be purchased separately:

- Cable ties (5)
- Waterproof putty tape (1)
- Specialized CAT5 cable
- Electrical tape (1)

Customer Sourced / Other

- Open/closed or socket wrench to tighten the nuts on the V-bolts (5/16") (customer sourced only)
- Grounding rod clamps (can be purchased separately)
- Wall mounts (can be purchased separately)

**Note:** You do not need a lightning arrestor with the SPEEDLAN 9101 because it is already included inside the outdoor, remote-mounted chassis.

## Installation Steps for the SPEEDLAN 9101

To install your SPEEDLAN 9101, follow the steps below:

### Step 1: Mounting the SPEEDLAN 9101

This unit/router will have an omni attached via an RF cable assembly. No additional steps are needed for this step. Go to Step 2.

### Step 2: Mounting the SPEEDLAN 9101 on the Pole

Select one of the two options below:

- **Pole Mount:** On a pole mount, position the router 5 to 10 feet below the antenna. Then, attach the router to the mounting pole using the two V-bolted clamps, one on top of the router and the other on the bottom of the router. Make sure you tighten the screws on the back of the pole mount.
- **Wall or Concrete Mount:** On a side building mount, position the router 5 to 10 feet below the antenna. Then, attach the router to the wall or concrete using the concrete or wood mounting screws. Make sure the router is secured.

### Step 3: Running the Cabling

1. Run CAT5 cable (from bottom of router) down to junction box located inside the building.
2. Secure grounding wire by running this wire to a suitable "earth" ground and fasten it securely in place. See the installation diagram following these directions.
3. Connect the Junction Box to the Power Supply by connecting the power cord of AC-DC Vdc adapter to 110 or 220 Vac power outlet (the input voltage of this universal adapter can vary from 100 to 240 Vac). Connect the DC output of the adapter to DC jack on the indoor junction box.
4. Connect the wireless SPEEDLAN 9101 to the customer's Ethernet LAN or PC by connecting the RJ-45 plug on a standard Ethernet CAT5 cable to the white RJ-45 port connector on indoor junction box. Connect the other end of the Ethernet CAT5 cable to your Ethernet hub, switch or unit/router.

**Note:** The lightning arrestor and RF cable assembly is enclosed inside the router.

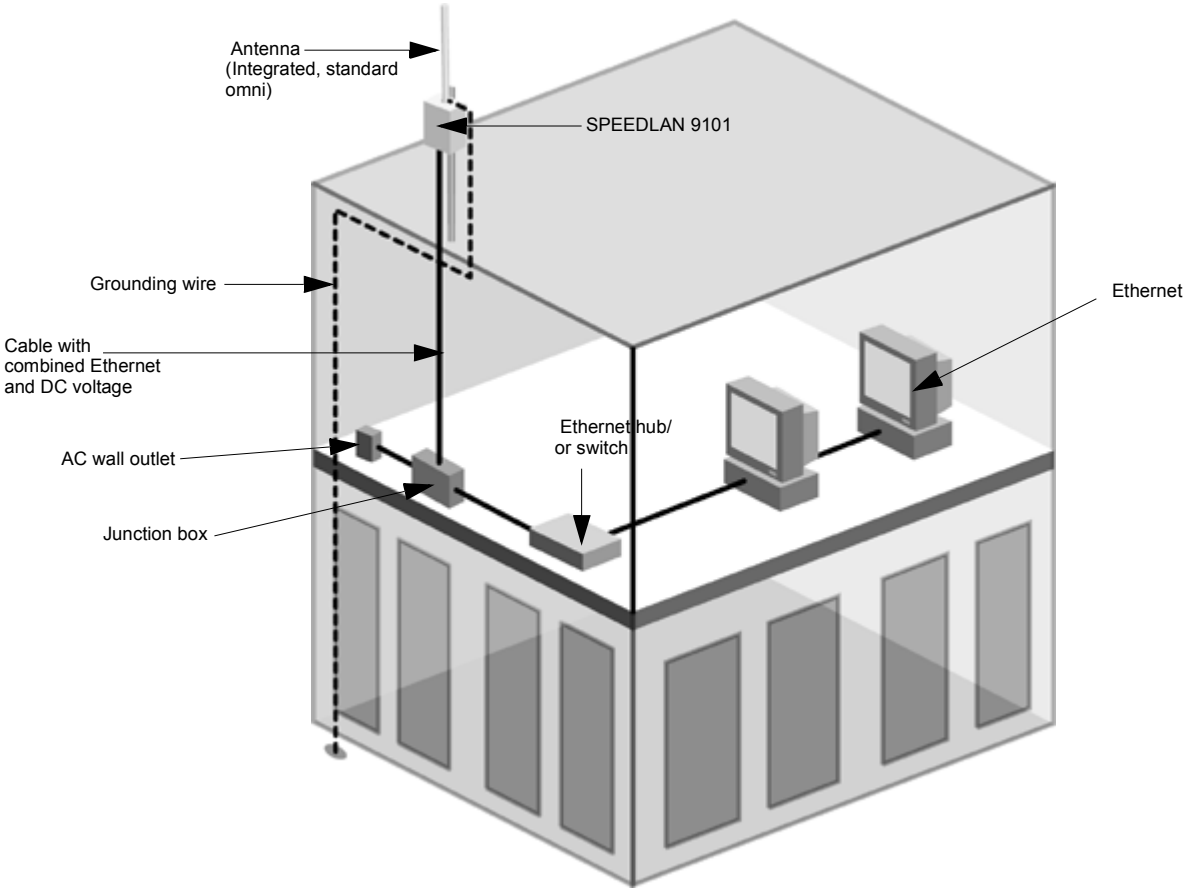
### Important Note: Waterproofing the Connectors!

Make sure you waterproof all the connectors, as follows: Apply two layers of electrical tape to the connector, and leave approximately 3 inches of cable exposed on either side of the connector. An alternative is to begin at the lowest point, so the tape overlaps from bottom to top creating a shingled effect. (This creates an effective barrier against runoff.) Apply this "shingle effect" to each

layer of the sealing process. Then, apply one layer of insulation putty over the top of the electrical tape, and leave at least one inch of the cable jacket to ensure a good seal. Do not stretch the putty, as this causes thinning and reduces the effectiveness of a good seal. Finally, apply five layers of electrical tape over the insulation putty and extend at least one (1) inch past the putty. This is the most important step in a creating a watertight seal. Make sure that there are no wrinkles in the tape, and the final wrap must be completed from bottom to top.

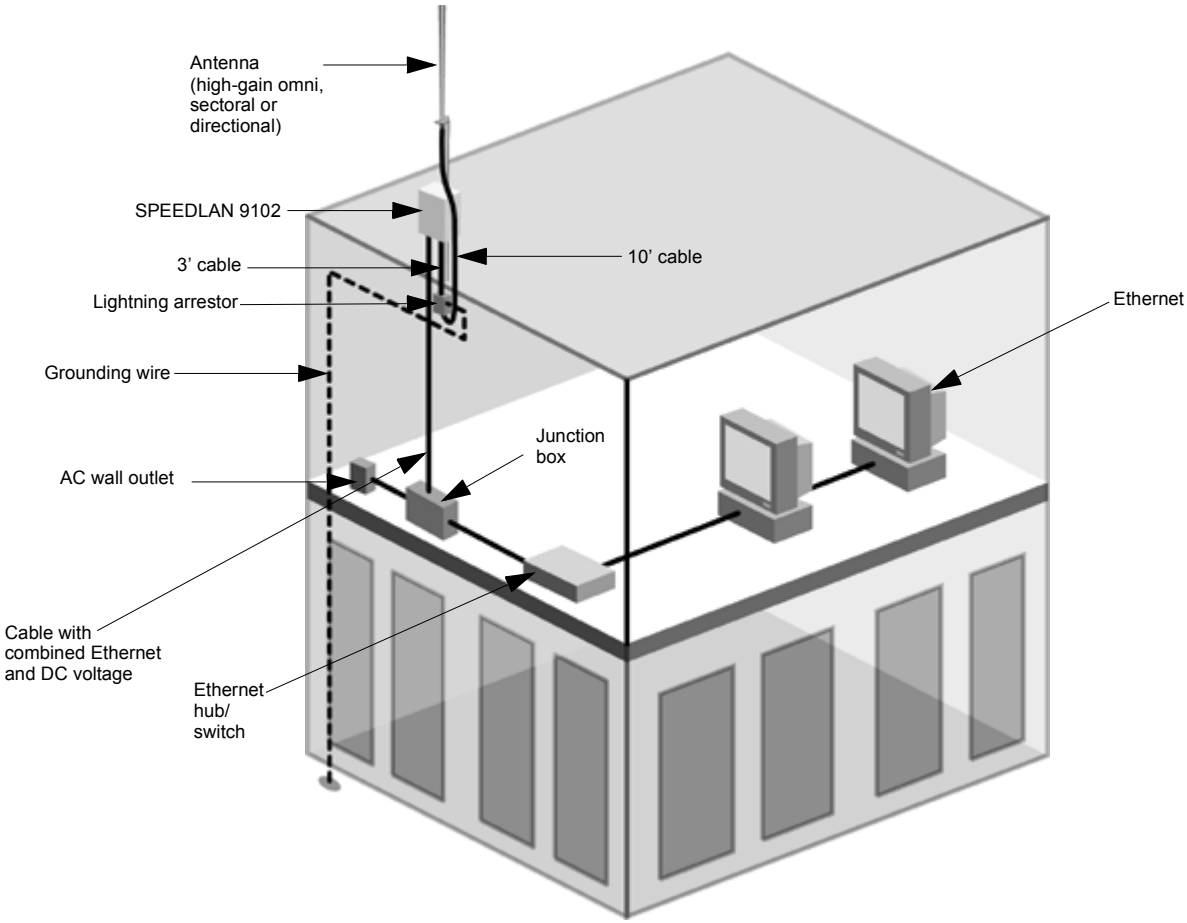
## Installation Diagram of the SPEEDLAN 9101

The diagram below displays where the main components are located for the SPEEDLAN 9101 with an integrated, standard omni (that is, an omni attached to the unit/router).



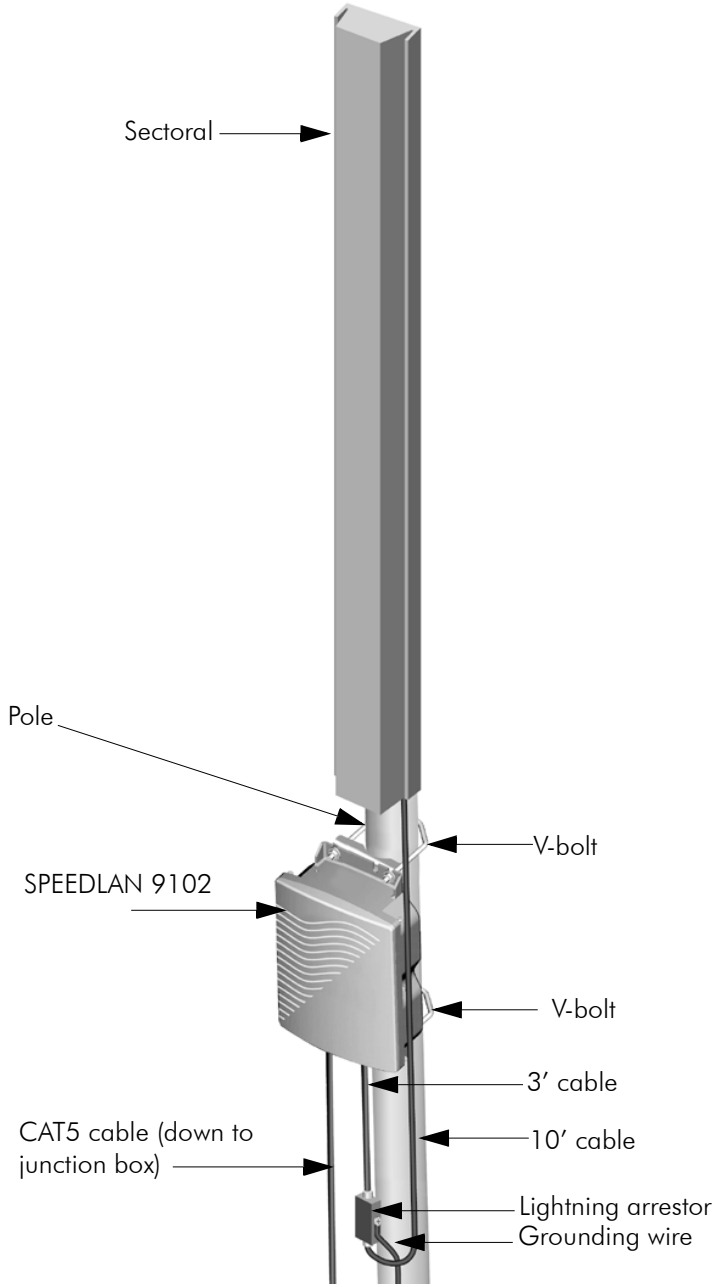
**Note:** Most users needing the mesh topology solution will use the SPEEDLAN 9101. However, there is the option of using an external antenna (e.g., high-gain omni antenna, or sectoral or directional). If you choose this option, follow the installation directions for the SPEEDLAN 9102, and it can act as a mesh topology solution. Contact Wave Wireless for more information. Below is an example of this solution:

**SPEEDLAN 9102 with High-Gain Omni (or Sectoral, or Directional)**

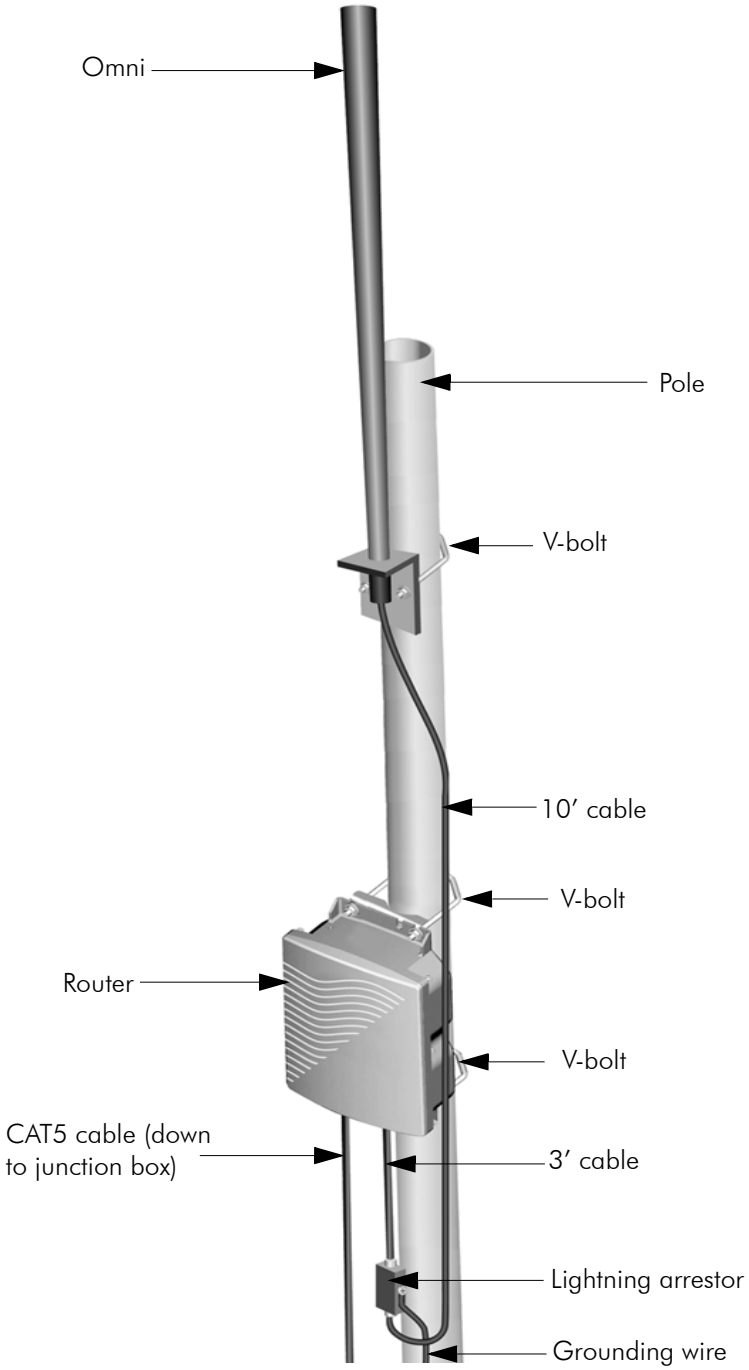


# The SPEEDLAN 9102 (with an External Antenna)

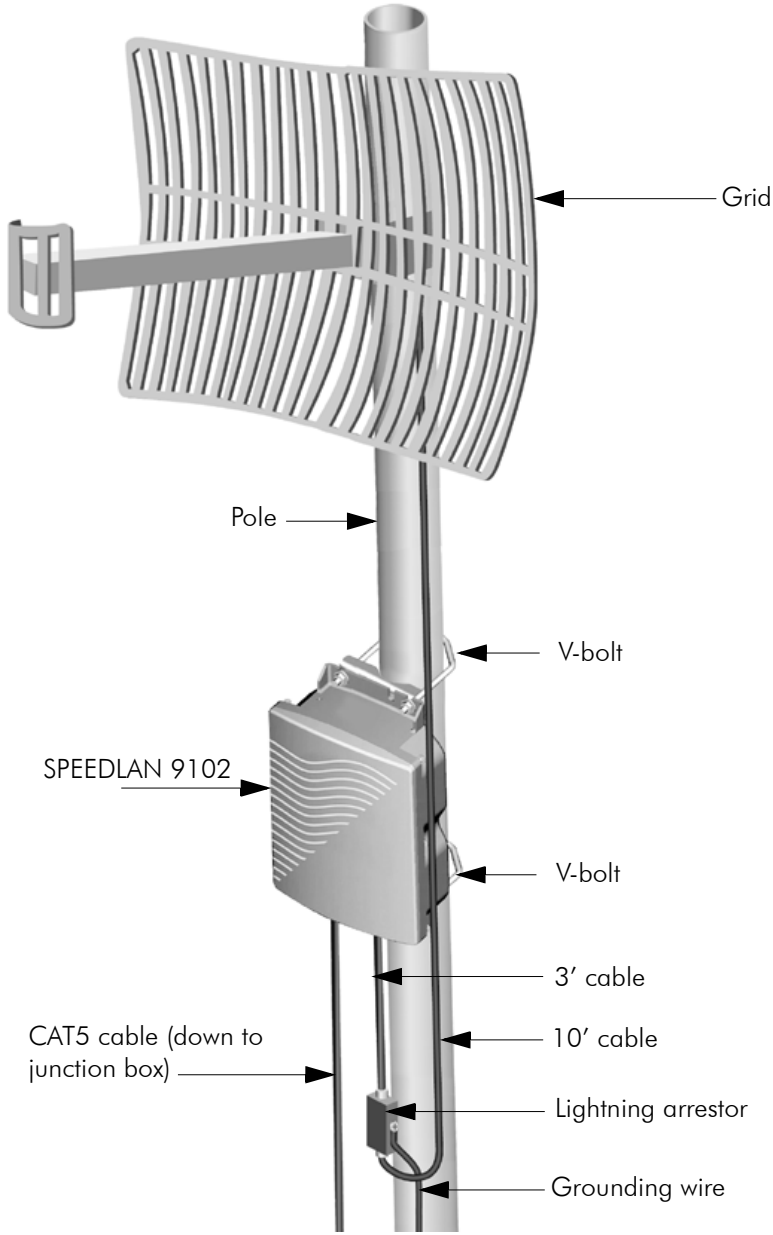
### As a Base Station with Sectoral



### As a Base Station with High-Gain Omni

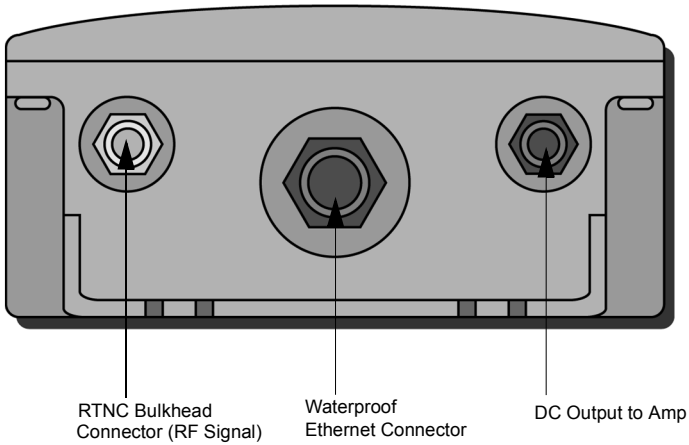


### As CPE/Point-to-Point with Grid (or Directional Antenna)




For best results when installing SPEEDLAN 9102 as CPE (or for point-to-point), use a horizontal grid antenna and make sure the polarities match. 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.

## Bottom View of SPEEDLAN 9102




## System Description

The SPEEDLAN 9102 units/routers are high speed, long range wireless LAN units/routers that provide connectivity to remote Ethernet networks. For single point-to-point links, a unit/router can be used in each building to create a wireless communication link. For multipoint links, a unit/router acts as the central base station, which controls the communication between multiple units/routers acting as CPE. The local router communicates with a remote unit/router on another LAN. This effectively creates an extended wireless network, spanning sites situated up to 25 miles apart (depending on the antenna configuration). This enables a central Ethernet LAN to be connected with one or more branch office LANs.

## Package Contents

- SPEEDLAN 9102
- Product registration card
- CD containing: Product manual, SPEEDView management software and SPEEDView Quick Start Guide
- Indoor junction box
- 10′ RF cable
- 3′ RF cable
- V-bolts

The following items are included with the installation kit, which can be purchased separately:

- cable ties (5)
- Lightning arrestor (1) current sensitive to ground
- Electrical tape (1)
- Waterproof putty tape (1)
- Specialized CAT5 cable

*Note: Antenna for the SPEEDLAN 9102 can be purchased separately.

Customer Sourced / Other

- open/closed or socket wrench to tighten the nuts on the V-bolts (5/16") (optional)
- Grounding rod clamps (can be purchased separately)
- Wall mounts (can be purchased separately)

## Installation Steps for the SPEEDLAN 9102

Some 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 of the SPEEDLAN 9102, page 2-17*.

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

To install your SPEEDLAN 9102 with an external antenna, do the following:

### Step 1.Verifying Line-of-Sight

Before installing the antenna and unit/router, make sure a clear line-of-sight exists. Line-of-sight can be defined as each antenna clearly seeing the other antenna, and seeing the remote locations when viewing from the central base location. Be sure to look level with the center of origin of the transmission (i.e., the middle of the antenna). Repeat this procedure from the remote location. Any disruption of the signal path due to trees, building, or any other obstructions may cause the link to function incorrectly. If you see any obstructions between two antennas, move one or both antennas to another location.

### Step 2. Mounting the Antenna

Follow the instructions below to mount the antenna.

**a)** On a side-building mount, position the bracket so there will be at least three feet (one meter) above the roof line where the pole is attached. This enables room for the antenna and reduces signal loss from building reflection.

**Note:** It is not recommended to mount the antenna onto any unstable object.

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

**c)** Assemble the antenna and mount it to the pole using the included V-bolt antenna mounting hardware. For a semi-parabolic grid type antenna, align the grid 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. Then, aim the antenna so it is pointed toward the receiving antenna on the other building. The radio signal radiates from the end of antenna like a wide-beamed flashlight. For optimal performance, you may need to test your link using both polarities. This configuration option varies with each location, as well as RF signals that may be present in the area.

### Step 3. Mounting the SPEEDLAN 9102

Select **one** of two options below:

- **Option A: Pole Mount**
  On a pole mount, position the router 5 to 10 feet below the antenna. Then, attach the router to the mounting pole using two included V-bolt clamps, one on the top of the unit/ router and the other on the bottom of router. Make sure you tighten the screws on the back of the pole mount.

OR

- **Option B: Wall or Concrete Mount**
  On a side building mount, position the router 5 to 10 feet below the antenna. Then, attach

the unit/router to the wall or concrete by using the concrete or wood mounting screws. Make sure it is secured.

### Step 4. Running and Securing All Cable

The installation kit includes two cables with ready-made connectors to fit your particular installation needs such as:

- 3’ RF cable
- 10' antenna cable (attaches to antenna one end and to lightning arrestor other end)
- Lightning arrestor (attaches to pigtail and to antenna cable)

a) Attach the 3’ RF cable to the RF port on the SPEEDLAN 9102.

b) Attach the 10' length of cable to the antenna. Next, attach the lightning arrestor to the lower end of the antenna cable.

c) Attach the other end of lightning arrestor to 3’ RF cable.

d) Run the main length of the specialized Ethernet cable from the router to the indoor junction box located inside the building.

e) Secure the cable with zip ties or cable clamps during this procedure.

**Note:** When running the cable through walls or obstructions, make sure that there is ample room for the connector to pass through without being damaged. Also, do not create extra pressure that would cause the cable to kink or be stretched or cut (i.e., pulling cable through tight locations).

f) Create a proper weatherproofing seal on all outdoor connections by wrapping it with electrical tape and sealing it with putty. This is the most crucial step of the installation. If this procedure is not completed, long-term and complex problems could occur. For more information on implementing this procedure, see *Weatherproofing Connectors, page 2-15*.

g) Next, ground the lightning arrestor. For more information, see *Grounding the Lightning Arrestor, page 2-15*.

**Step 5. Grounding the Lightning Arrestor**

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. The lightning arrestor is **NOT** waterproof.

**Step 6. Weatherproofing Connectors**

a) Seal the entire lightning arrestor with the black waterproof sealant insulation putty that is included in the installation kit.

b) Apply two layers of electrical tape to the connector, and leave approximately 3 inches of cable exposed on either side of the connector. An alternative is to begin at the lowest point, so the tape overlaps from bottom to top creating a shingled effect. (This creates an effective barrier against water runoff). Apply this "shingle effect" to each layer of the sealing process.

c) Apply one layer of insulation putty over the top of the electrical tape, and leave at least one inch of the cable jacket to ensure a good seal. Do not stretch the putty, as this causes thinning and reduces the effectiveness of a good seal.

d) Apply five layers of electrical tape over the insulation putty and extend at least one (1) inch past the putty. This is the most important step in creating a watertight seal. Make sure that there are no wrinkles in the tape and the final wrap must be completed from bottom to top.

**Step 7. Connect the Wireless Unit/Router to the Power Supply**

a) Connect power cord of AC-DC 24Vdc adapter to 110 or 220 Vac power outlet (the input voltage of this universal adapter can vary from 100 to 240 Vac).

b) Connect the DC output of the adapter (24 Vdc) to DC jack on the indoor junction box.

**Step 8. Connect the Router to Customer's Ethernet LAN**

a) Connect the RJ-45 connector on a standard Ethernet CAT5 cable to the RJ-45 port (color of port is white) on indoor junction box.

b) Connect the other end of the Ethernet CAT5 cable to your Ethernet hub, switch or router.

**Step 9. Adding Additional Units/Routers**

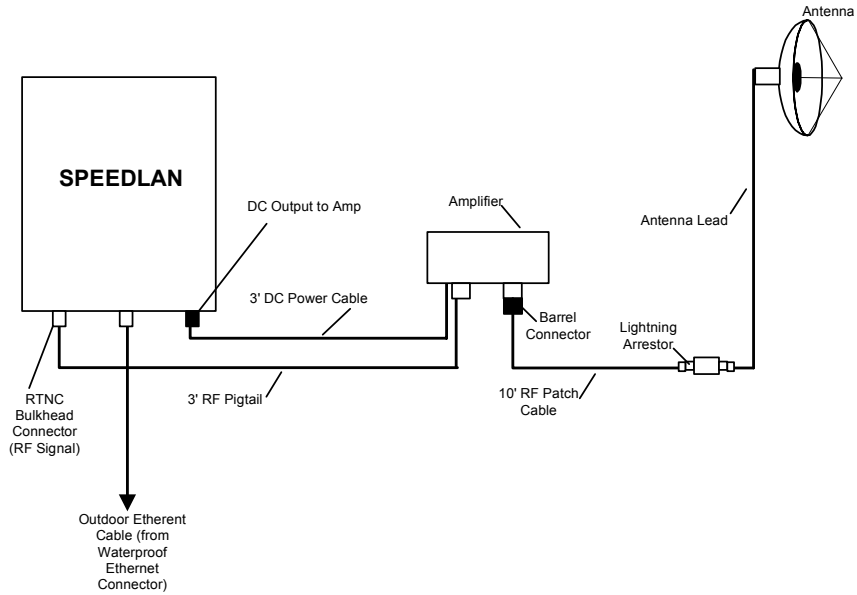
Repeat the steps above for all SPEEDLAN 9102 units/ routers that will be communicating with this one.

## If Using An Amplifier with the SPEEDLAN 9102

Items needed to install amplifier:

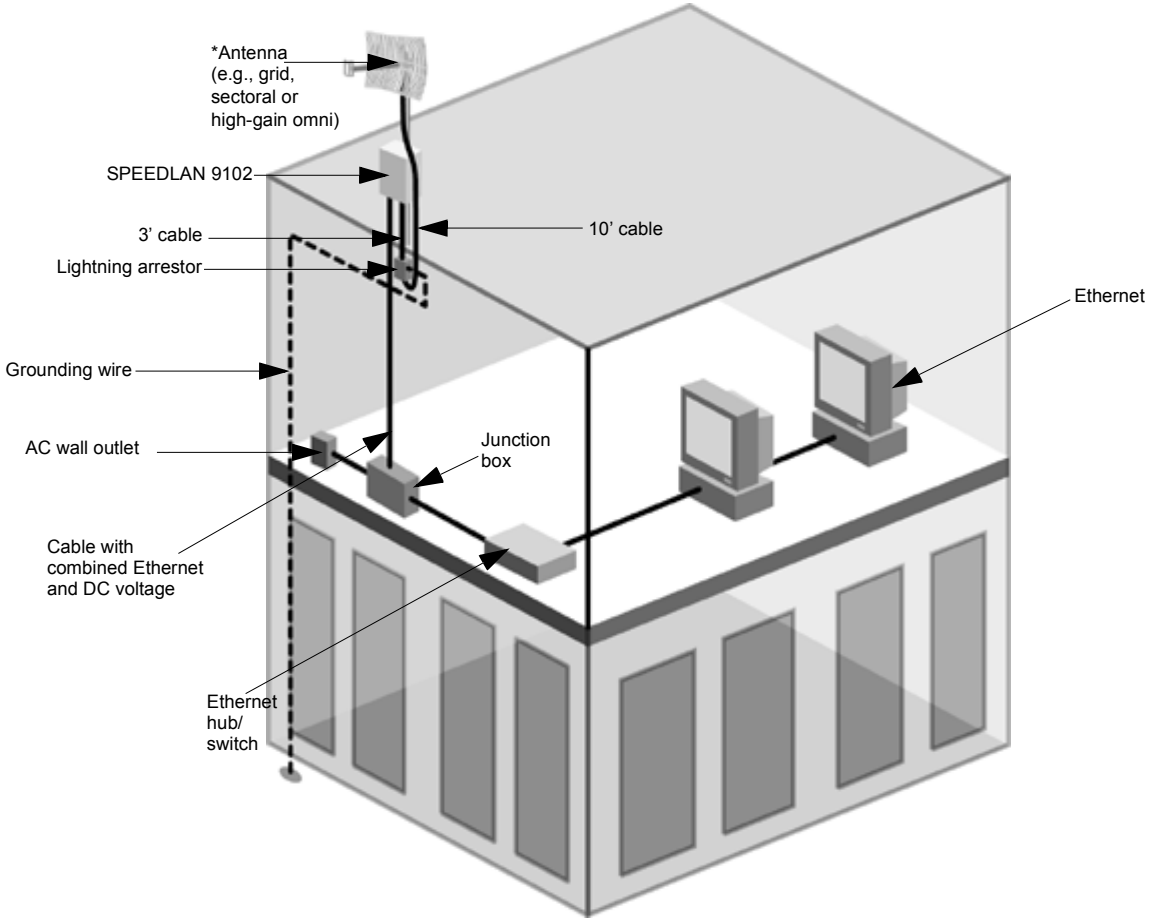
- one 3′ DC Power Cable
- one 3′ RF Pigtail
- one Barrel Connector
- one 10′ RF Patch cable

1. Connect the 3′ DC Power Cable from the unit/router to the amplifier.
2. Connect the 3′ Pigtail for the RF from the RF port of the unit/router to the RF “in” port of the amplifier.
3. Connect the barrel connector to the RF “out” port on the amplifier.
4. Connect the 10′ RF Patch cable from the barrel connector to your lightning arrestor.




**Note:** The External RF Amp (provides an average power of +12 dBm) or External Amplifier with Power Supply is considered an accessory and can be purchased separately, as well as the other items included in the list above.

## Installation Diagram of the SPEEDLAN 9102




***Note:** The sectoral, grid (directional) and high-gain omni antennas all follow the same installation instructions.

Notes:

# Chapter 3
# Using the SPEEDLAN 9000 Configurator

# Initial Configuration of the SPEEDLAN 9000

## Prerequisites

A PC that has the SPEEDView application installed and either Internet Explorer 5+ or Netscape Navigator 4+. (For more information about SPEEDView see the separate PDF called, "SPEEDView Quick Start Guide.")

Configuration of the SPEEDLAN 9000 is done through a web-based interface called the SPEEDLAN 9000 Configurator. In order to access the SPEEDLAN 9000 Configurator, you must first establish TCP/IP communication between the SPEEDLAN 9000 and your PC. You can arrange the cabling in one of two ways:

- If you have an Ethernet hub and two Ethernet cables, connect both the SPEEDLAN 9000 and the PC into the same hub.
- If you have an Ethernet cross-over cable, you can connect the SPEEDLAN 9000 directly to the PC.

Once cabling is established, you must get both the SPEEDLAN 9000 and the PC on the same TCP/IP network. You can do this in one of two ways:

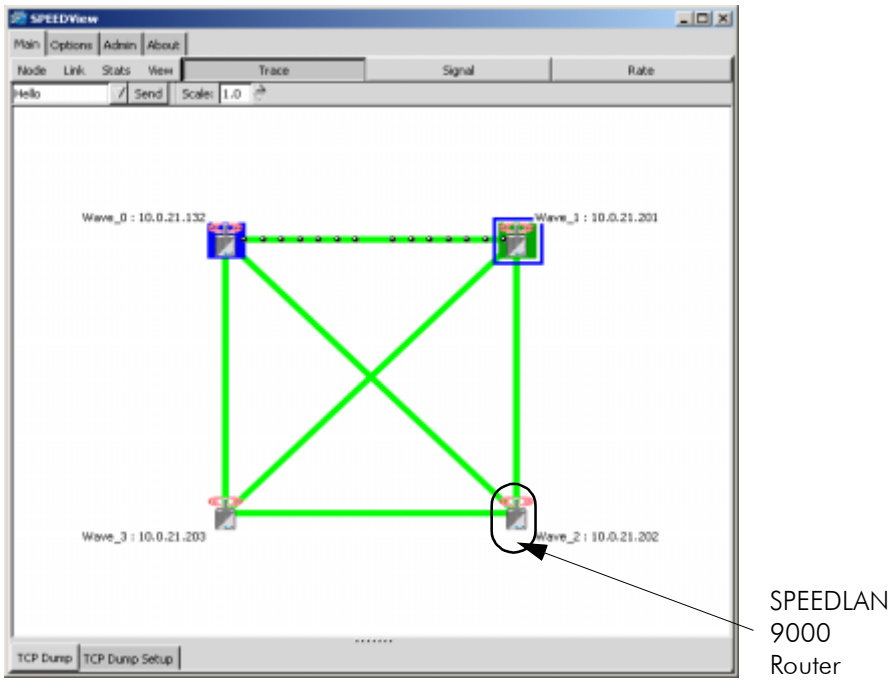
- If your network has a DHCP server and you are able to configure it, you can enter the hardware or MAC address into the DHCP server's settings. Then, have the DHCP server assign a known IP address to the 9000.
- You can assign an IP address to the PC in the 192.168.69.0 network. The SPEEDLAN 9000 will default to 192.168.69.1, so you will have to choose a different IP address for the PC.

The SPEEDLAN 9000 will attempt to obtain an IP address on its Ethernet port using DHCP when it first boots, and if it cannot obtain one it will revert to 192.168.69.1 after a 30 second timeout. The netmask will default to 255.255.255.0 (/24).

Before continuing you should verify that the PC has TCP/IP connectivity with the SPEEDLAN 9000. The most common way to do this is to run 'ping' 192.168.69.1 (or your DHCP assigned address) in a console. This command is available in a Windows 9x DOS prompt, a Windows 2000 / NT / XP command prompt, or any Unix console.

## Configuring the SPEEDLAN 9000

Once your PC can access the SPEEDLAN 9000, start SPEEDView and connect to 192.168.69.1 (or the DHCP supplied address). The SPEEDView Main tab will have a network diagram including all wireless SPEEDLAN 9000 routers (similar to the diagram shown below). For more information on SPEEDView, see the separate PDF document titled, "SPEEDView Quick Start Guide".




In order to configure a specific SPEEDLAN 9000 router, double-click the router in the network diagram. This will open the SPEEDLAN 9000 Configure Login page for that router in your web browser. When you are prompted to enter a password, refer to *Classes of Users, page 3-10* in this manual. The SPEEDLAN 9000 Configurator allows you to access all configurable options for the SPEEDLAN 9000. Alternatively, entering the IP address of any of the SPEEDLAN 9000s into your web browser will allow you to access this page directly.

SPEEDView will attempt to temporarily create a route on your PC from the Ethernet network of the cabled SPEEDLAN 9000 to the wireless SPEEDLAN 9000 network. This route is required if you want to double-click routers from SPEEDView or access remote SPEEDLAN 9000 routers directly from your web browser. You require administrator privileges to add this route. SPEEDView's attempt to set the route will fail if you do not.

## Wireless Interface IP Address Assignment

The SPEEDLAN 9000 by default will attempt to get an IP address from a DHCP server for its wireless interface. It too will revert to a static address after 30 seconds using an address from the 10.x.y.z network where x,y,z are the last three octets of the SPEEDLAN 9000s wireless interface. This method is used to ensure uniqueness. Because the last three octets of the IP address are variable a netmask of 255.0.0.0 (/8) is used in order for the SPEEDLAN 9000s to communicate on this network.

## Automating the Configuration of Multiple SPEEDLAN 9000s

Some of the configuration parameters for the SPEEDLAN 9000 are common to all SPEEDLAN 9000s in the same network, for instance the channel and data rate of the wireless interface. In order to automate the distribution of these parameters to each SPEEDLAN 9000 router, the SPEEDLAN 9000 Configurator has a "Replication" feature that will send common configuration items to one or more of the routers. For more information, see *Replication, page 3-42*.

## Completing Configuration

Certain configuration parameters require a reboot after they have been changed. Therefore, to ensure all changes have been activated, each SPEEDLAN 9000 should be rebooted when its configuration is complete. Multiple SPEEDLAN 9000 routers can be rebooted at the same time from either the SPEEDView application or the SPEEDLAN 9000 Configurator. To reboot the router in SPEEDView, click the **Admin** tab. To reboot the router in the SPEEDLAN 9000 Configurator, choose **Remote Control** from the **Admin** menu.

## Adding Additional SPEEDLAN 9000s to the Wired Network

If you need to add an additional SPEEDLAN 9000 to the wired network, do the following:

1. Connect the additional SPEEDLAN 9000 routers to a hub or switch on the network and have DHCP assign IP addresses dynamically.
2. Connect additional SPEEDLAN 9000 routers to a hub or switch on the network one at a time, changing the wired IP address of each router as it is added, to an address other than 192.168.69.1 (to avoid duplicate IP addresses).

If you need help, contact your system administrator.

# Overview of the SPEEDLAN 9000 Configurator Main Menu

- Interfaces
  Use this menu to view a list of the interfaces that exist on the router, such as wireless interfaces, fixed interfaces, or both. This is where you would assign either a static or dynamic Internet address for the unit/router. You will also be able to define the display name for the wireless or fixed device.
- System
  Use this menu to define information about the host, view information about the SPEEDLAN 9000 Configurator, or set the current password.
- Routing
  Use this menu to view and set the routing configuration.
- Wireless
  Use this menu to select the frequency and data rate of the wireless device.
- DHCP Server
  Use this menu to configure a DHCP server on one or more of the interfaces. You can also view log messages and view the interfaces being serviced with DHCP.
- DHCP Relay
  Click this menu to enable DHCP Relay and set the parameters it requires.
- NAT
  Use this menu to configure Name Address Translation (outgoing and incoming) on the SPEEDLAN 9000 unit/router.
- Diagnostics
  Use this menu to troubleshoot your SPEEDLAN 9000 network and reboot / power off the SPEEDLAN 9000 unit/router.
- Admin
  Use this menu to perform administrative tasks, such as setting up user password information and permissions. You can also replicate certain configuration to other SPEEDLAN 9000 units/routers from this menu to automate network configuration.

The SPEEDLAN 9000 Configurator main menu is displayed below.

**Note:** If you need to reference anything about IP addressing, refer to *Basics of IP Addressing, page 5-2*.

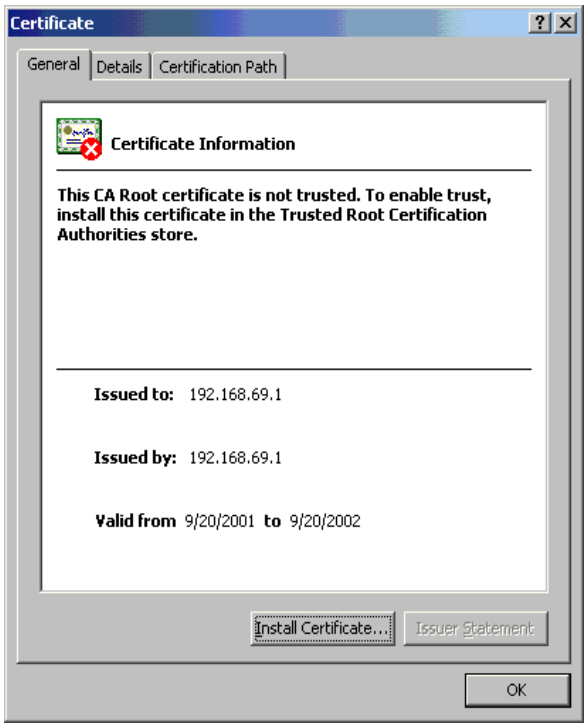
## Logging on to the SPEEDLAN 9000 Configurator

To access the SPEEDLAN 9000 Configurator, open your web browser and enter the following address: "https://192.168.69.1". You can also enter "http://192.168.69.1". However, the "https://192.168.69.1" address is the more secure address.

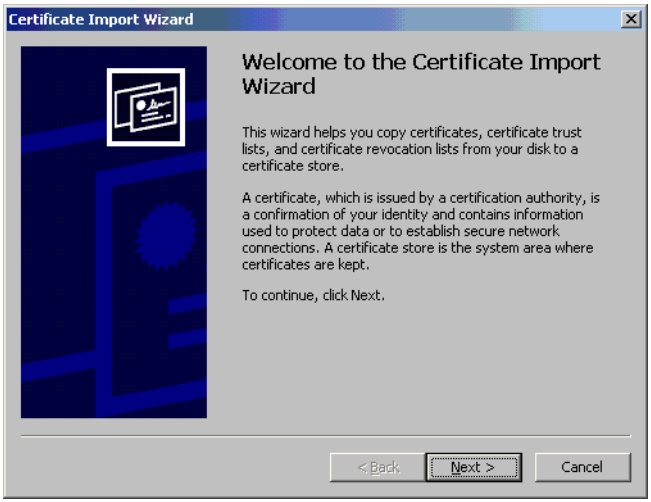
In order to avoid a security alert each time the SPEEDLAN 9000 Configurator is accessed, you must install it's security certificate into Internet Explorer. If the SPEEDLAN 9000's host name changes, you will have to repeat this process. Follow the steps below:

1 When the Security Alert dialog box appears. Click **View Certificate** (right most button on bottom of Security dialog box). The following dialog box will appear.

2 Click **Install Certificate**.

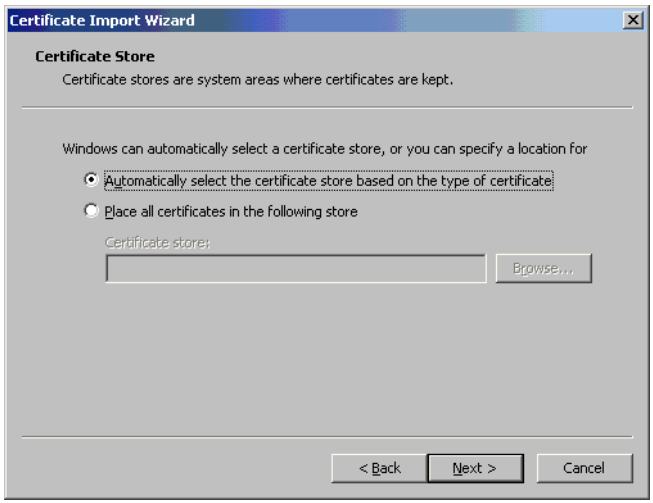


3 The Certificate Import Wizard will appear.




4. Click **Next**.

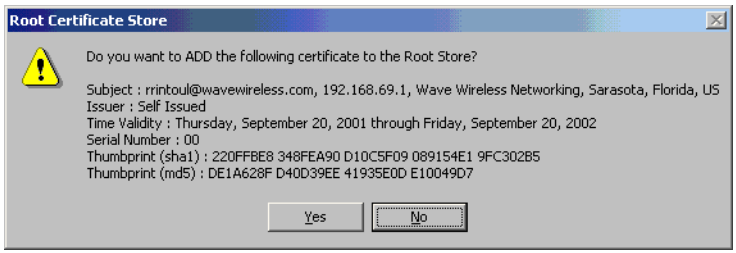
5 The following dialog box will appear.




6 Click **Next** again.

7 The following dialog box will appear.

8 Click **Finish**. This message will appear. Click **Yes**.




9 You will see a confirmation stating that the import was successful. Click **OK**. Click **OK** again. If the Security Alert dialog box appears, click **Yes**.

You should not get the Security Alert the next time you access this site. The SPEEDLAN 9000 Configurator web site will appear.

### Classes of Users

There are five classes of users on the SPEEDLAN 9000. The classes are as follows with their default passwords:

- Full Access (also known as a superuser): wave
- Wired Admin: wave_wired_admin (account for the private Ethernet network)
- Wired Read: wave_wired (account for the private Ethernet network)
- Wireless Admin: wave_wireless_admin (account for the wireless SPEEDLAN 9000 network)
- Wireless Read: wave_wireless (account for the wireless SPEEDLAN 9000 network)

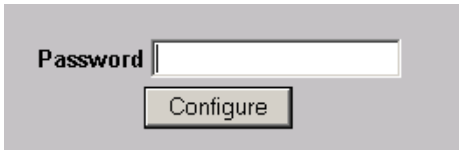
Admin accounts have administration rights to their appropriate network (wired or wireless), and Read Only accounts have only read only access.

If you are a network administrator and want to modify the default passwords and settings for any of the users, choose the **Admin** menu. For more information, see *, page 3-51*.

## Logging On

Follow the steps below to log on to the SPEEDLAN 9000 Configurator.

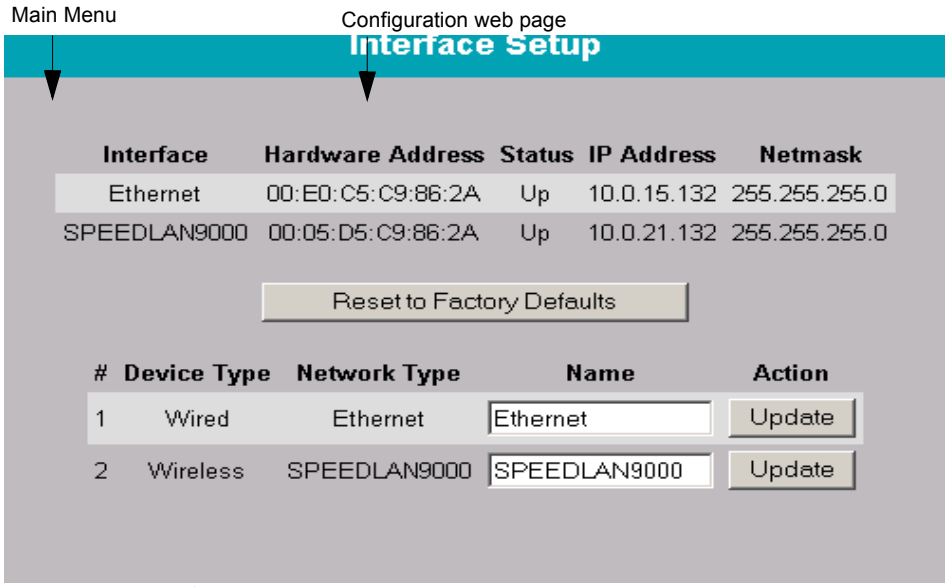
1. Make sure you entered the correct URL.




2. Enter the password in the **Password** text box. To know which password you should enter, see *Classes of Users, page 3-10*.
3. Click **Configure**. If your log on information is correct, then the Host Information page will appear.

## After Logging On

After you log on, you will see the Interface Setup page, as displayed below.




Lists current system information: host name and type (class) of user. For more information see the section called, "Classes of Users."

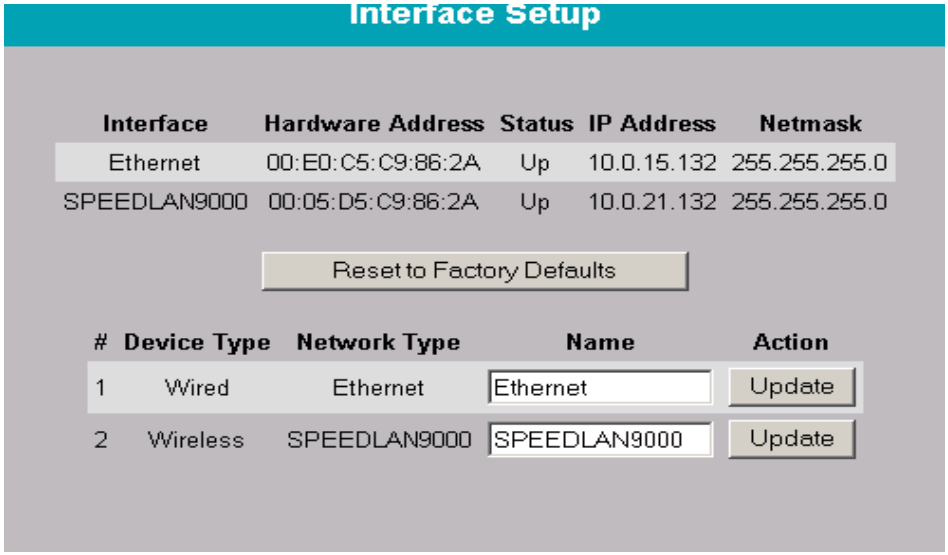
# Interfaces

There are two categories under the Interfaces menu: Setup and Interface Parameters (naming "Ethernet" for the wired unit/router or SPEEDLAN "9000" for the wireless unit/router.

- Choose **Setup** to name the interfaces that exist on the unit/router. To do this, one of the default names under the **Interfaces** menu. (To change these default names, see *Setup, page 3-12*.)
- Choose **Interface Parameters** to also assign a static or dynamic IP address. You can also view a list of interfaces that exist on the unit/router.

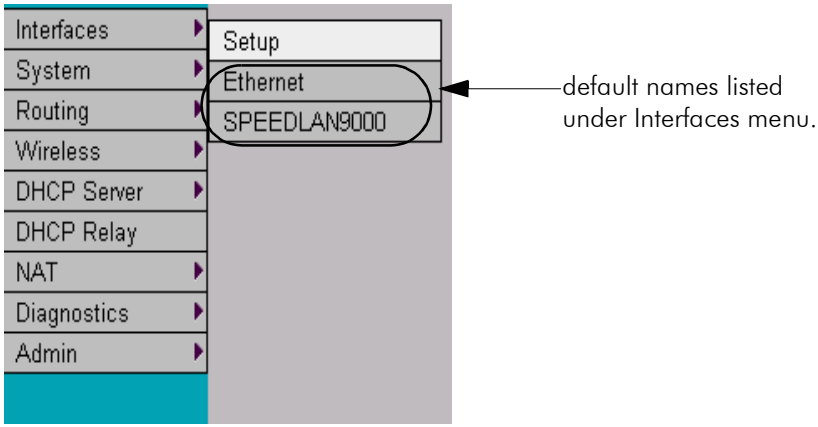
## Setup

This is where you enter the display name of the interface or the unit/router. When you choose **Setup** under the **Interfaces** menu, the Interface Setup page will appear.




- **Interface:** This is the fixed or wireless interface (e.g., eth1).
- **Hardware Address:** In a LAN environment each network interface contains its own Medium Access Control (MAC) address which is the embedded and unique hardware number.
- **Status:** This is the state of the interface. Up - ready to pass packets; Down - cannot pass packets; Testing - in some test mode.
- **IP Address:** This address tells the network how to locate the computers or network equipment connected to it.
- **Netmask:** The netmask is a 4-byte number that masks the network part of the Internet Protocol IP address, so only the host computer part of the address remains.
- **Reset to Factory Defaults:** Click to revert to factory default interface names.
- **#:** This is the number representing the wireless or fixed unit/router.
- **Device Type:** This is the name for the wireless or fixed unit/router (e.g., Wireless or Wired).
- **Network Type:** The type of network for the wireless or fixed unit/router.
- **Category:** The SPEEDLAN 9000 Configurator will adjust to the type of network you selected.

- **Name:** The default name for the routers.

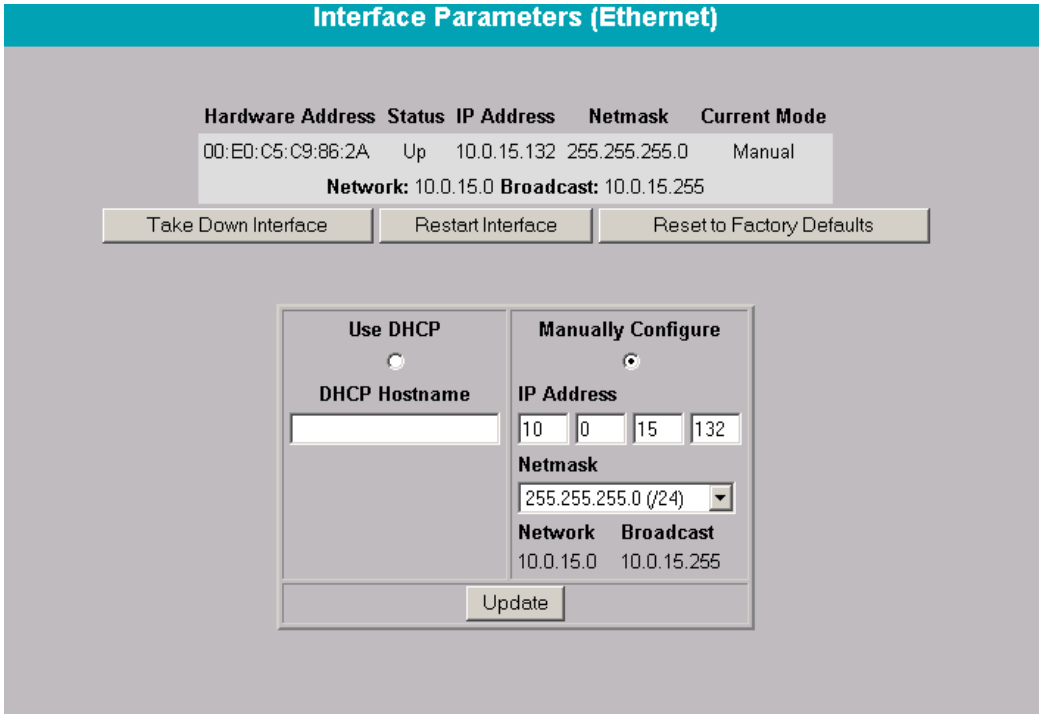



You can also change the default to the name of your choice for equipment operating on the wired or wireless network. The name you enter in the **Name** text box will represent the name of the interface you are configuring. This means that the second and third submenus under Setup will adjust to the name you entered. Click **Update** to modify a name, or click **Delete** to permanently remove a name.

## Interface Parameters

Interface Parameters contains a dynamic list of the interfaces that exist on the unit/router, such as wireless interfaces, fixed interfaces, or both. This is where you would assign either a static or dynamic

Internet Address, as well as entering the name of the DHCP host. To activate this page, choose the interface from the **Interfaces** menu. The following page will appear.




After you choose the appropriate interface, you will be able to view the following parameters:

- **Hardware Address:** In a LAN environment each network interface contains its own Medium Access Control (MAC) address which is the embedded and unique hardware number.
- **Status:** This is the state of the interface. Up - ready to pass packets; Down - cannot pass packets; Testing - in some test mode.
- **IP Address:** This address tells the network how to locate the computers or network equipment connected to it.
- **Netmask:** The netmask is a 4-byte number that masks the network part of the Internet Protocol IP address, so only the host computer part of the address remains.
- **Current Mode:** Manual or DHCP.

## CIDR Table (For Netmask Information Purposes)

| CIDR Length | Mask | # Networks | # Hosts |
|---|---|---|---|
| /8 | 255.0.0.0 | 1 A | 16,777,214 |
| /9 | 255.128.0.0 | 128 B | 8,388,352 |
| /10 | 255.192.0.0 | 64 B | 4,194,176 |
| /11 | 255.224.0.0 | 32 B | 2,097,088 |
| /12 | 255.240.0.0 | 16 B | 1,048,544 |
| /13 | 255.248.0.0 | 8 B | 524,272 |
| /14 | 255.252.0.0 | 4 B | 262,136 |
| /15 | 255.254.0.0 | 2 B | 131,068 |
| /16 | 255.255.0.0 | 1 B | 65,534 |
| /17 | 255.255.128.0 | 128 C | 32,512 |
| /18 | 255.255.192.0 | 64 C | 16,256 |
| /19 | 255.255.224.0 | 32 C | 8,128 |
| /20 | 255.255.240.0 | 16 C | 4,064 |
| /21 | 255.255.248.0 | 8 C | 2,032 |
| /22 | 255.255.252.0 | 4 C | 1,016 |
| /23 | 255.255.254.0 | 2 C | 508 |
| /24 | 255.255.255.0 | 1 C | 254 |
| /25 | 255.255.255.128 | 2 Subnets | 124 |
| /26 | 255.255.255.192 | 4 Subnets | 62 |
| /27 | 255.255.255.224 | 8 Subnets | 30 |
| /28 | 255.255.255.240 | 16 Subnets | 14 |
| /29 | 255.255.255.248 | 32 Subnets | 6 |
| /30 | 255.255.255.252 | 64 Subnets | 2 |
| /31 | 255.255.255.254 | none | none |
| /32 | 255.255.255.255 | 1/256 C | 1 |

- **Bring Up Interface/Take Down Interface:** If the status is "Up" the button will read "Take Down Interface." If the status is "Down" the button will read "Take Up Interface". These buttons allow you to temporarily disable a network interface and then enable it again for diagnostic purposes.
- **Restart Interface:** Click to restart the interface.
- **Reset to Factory Defaults:** Click to revert to factory default settings for this interface.
- **Use DHCP:** Select this option if you want to dynamically acquire an IP address or DHCP from a DHCP server. 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, it must be assigned a new IP address for that network. DHCP can be used to manage these assignments automatically. Then, click **Update**.

- **Manually Configure:** Select this option if you want to statically assign an IP address to the interface. For example: you may want to assign a "static" (permanent) address to a computer that will always be used as a server. 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. Then, click **Update**.
- **DHCP Hostname:** Enter the name of the DHCP Host.

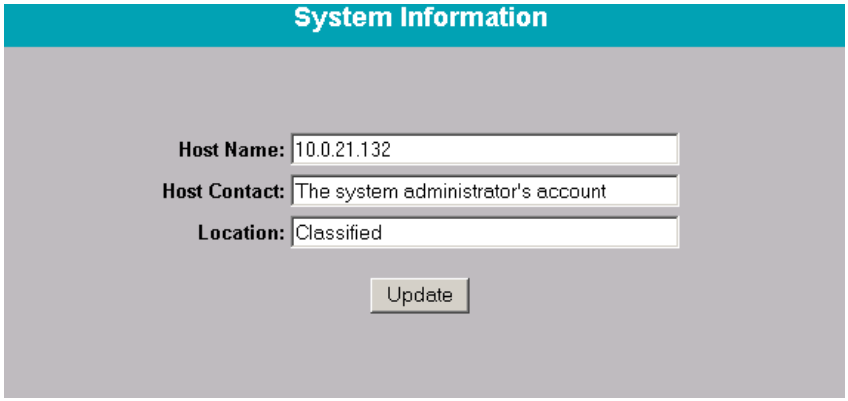
**Note:** If you selected the **Manually Configure** option, enter the Internet address that you want to assign to the interface in the **IP Address** text box. You will also enter the subnet/netmask for the IP address. Select the appropriate netmask in the **Netmask** drop-down list. If you need more information about netmasking, see the *CIDR Table (For Netmask Information Purposes), page 3-15*.

# System

There are three categories under the System menu: General, Performance and Password.

## General/System Information

This page contains information about the unit/router on the network. When you choose **General** under the **System** menu, the System Information page will appear as shown below.




Enter the following information:

- **Host Name:** The domain name of the unit/router (e.g., fatdog.devnet.wavewireless.net).
- **(Optional) Host Contact:** The person to contact if there is trouble with the unit/router (e.g., johndoe@aol.com).
- **(Optional) Location:** The location of the unit/router (e.g., building or closet).

If you modified any of the information above, click **Update**.

## Performance

This page displays information about the operating system, platform, up time and load average. When you choose **Performance** under **Host** menu, the System Performance page appears displaying the following information:.

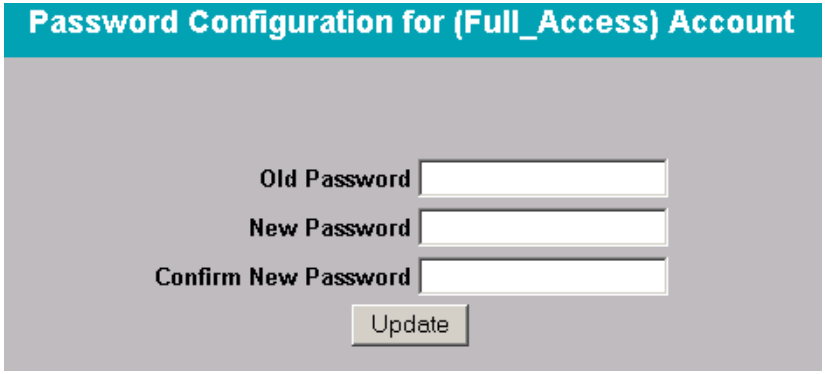
**System Performance**

| | |
|---|---|
| **Operating System:** | Linux 2.4.13 |
| **Platform:** | i686 |
| **Up Time:** | 19:28 hours |
| **Load Average:** | 0.00, 0.00, 0.00 |
| **Total Memory:** | 512,516 kB |
| **Free Memory:** | 153,812 kB |
| **Used Memory:** | 358,704 kB |
| **Total Swap:** | 265,032 kB |
| **Free Swap:** | 265,032 kB |
| **Used Swap:** | 0 kB |

- **Operating System**: Type of operating system that is running (i.e., Linux).
- **Platform**: The computer system that the application runs on (i.e., such as i686, etc.).
- **Up Time**: The time that the SPEEDLAN 9000 has been running.
- **Load Average**: It is the Unix standard indication of processor load.
- **Total Memory**: The total memory in kilobytes.
- **Free Memory**: Memory that is available.
- **Used Memory**: Memory that is being used.
- **Total Swap**: The total space on the hard disk that can be used as a virtual memory extension of the computer's real memory (RAM).
- **Free Swap**: Swap memory that is available.
- **Used Swap**: Swap memory that is being used.

### Password

This is where you modify the password for the current account on the SPEEDLAN 9000 Configurator. To modify password information, choose **Password** from the **System** menu. The following page will appear.




To enter a new password, do the following:

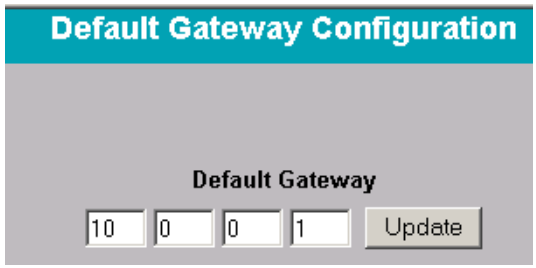
1. Enter the old Password in the **Old Password** text box.
2. Next, enter the new password in **New Password** text box.
3. Finally, confirm New Password in the **Confirm New Password** text box. Click **Update**.

## Routing

There are three categories under Routing: Def Gateway, Route Table and Static Routes (Local and Common).

### Def Gateway

If you want to modify the IP address of the default gateway, choose **Def Gateway** from the **Routing** menu. The following page will appear.



**Default Gateway:** Enter the IP address of the default gateway. This is the "door" where you want the data to travel. Then, click **Update** after modifying information.

## Route Table

The routing table displays routing information between destinations. To view routing information, choose **Route Table** from the **Routing** menu. The following page will appear.

**Route Table**

| Destination | Gateway | Mask | Interface |
|---|---|---|---|
| 10.0.15.0 | 0.0.0.0 | 255.255.255.0 | Ethernet |
| 10.0.21.0 | 0.0.0.0 | 255.255.255.0 | SPEEDLAN9000 |
| 10.0.21.201 | 10.0.21.201 | 255.255.255.255 | SPEEDLAN9000 |
| 10.0.21.202 | 10.0.21.202 | 255.255.255.255 | SPEEDLAN9000 |
| 10.0.21.203 | 10.0.21.203 | 255.255.255.255 | SPEEDLAN9000 |

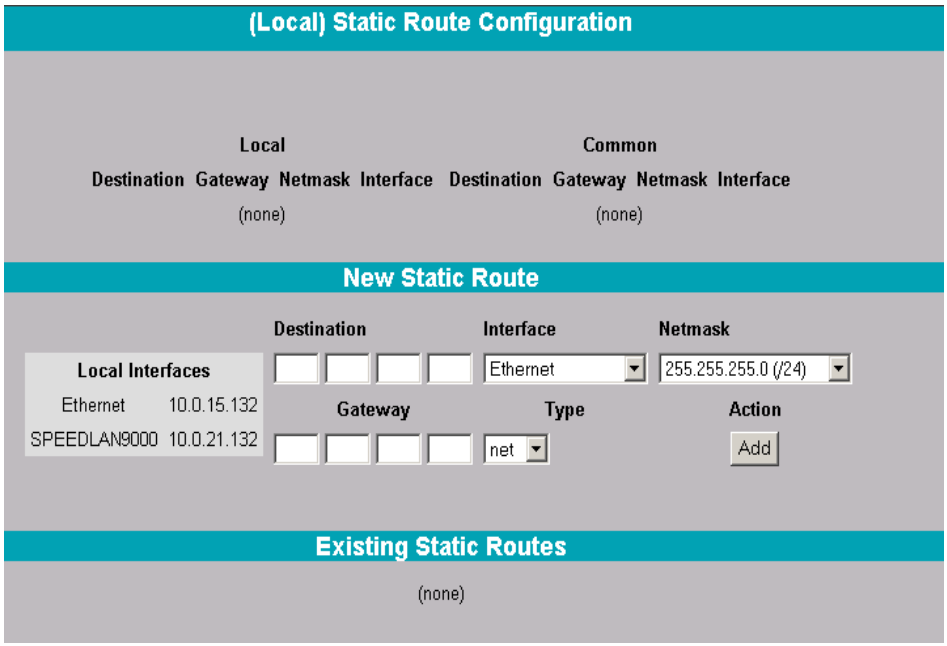
Each statistic is defined below:

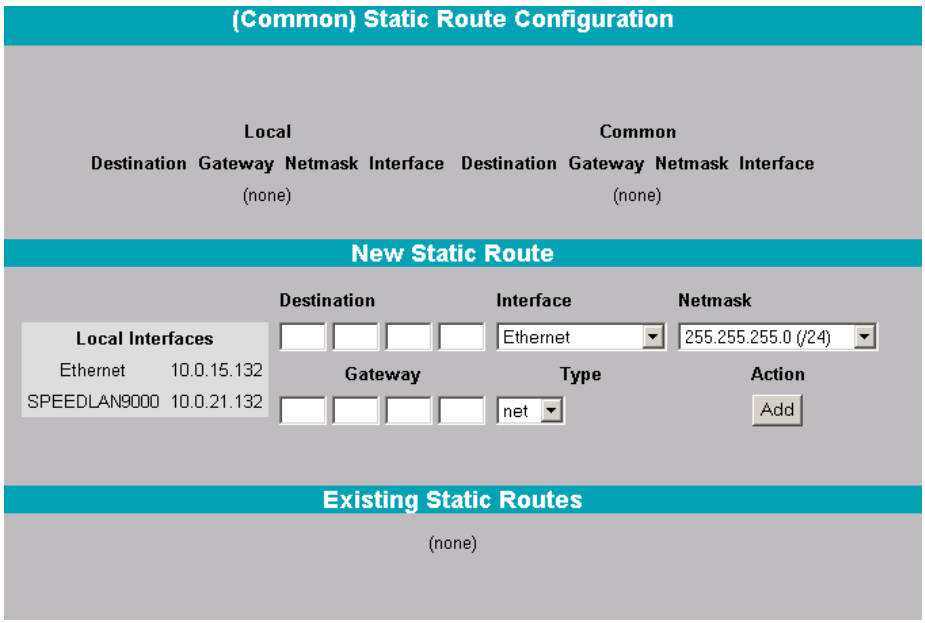
- **Destination:** The destination network or host.
- **Gateway:** This is a network point that acts as the "entrance door" to another network. This is the first "router" that takes you to the designated host (i.e., the next hop on the network).
- **Netmask:** The netmask is a 4-byte number that masks the network part of the Internet IP address, so only the host computer part of the address remains.
- **Interface:** Specifies which network interface the route will use.

## Static Route

The Static Route page allows you to add static routes as additional routes, default routes or routes that the SPEEDLAN 9000 routers do not contain in their routing table.

To open the Static Route page, choose **Static Routes** from the **Routing** menu. Then, choose either **Local** or **Common**.


(Local) Static Route Configuration
Local
Common
Destination Gateway Netmask Interface Destination Gateway Netmask Interface
(none)
(none)
New Static Route
Destination
Interface
Netmask
Local Interfaces
Ethernet 10.0.15.132
SPEEDLAN9000 10.0.21.132
Ethernet
255.255.255.0 (/24)
Gateway
Type
Action
net
Add
Existing Static Routes
(none)


(Common) Static Route Configuration
Local
Common
Destination Gateway Netmask Interface Destination Gateway Netmask Interface
(none)
(none)
New Static Route
Destination
Interface
Netmask
Local Interfaces
Ethernet 10.0.15.132
SPEEDLAN9000 10.0.21.132
Ethernet
255.255.255.0 (/24)
Gateway
Type
Action
net
Add
Existing Static Routes
(none)

- **Local Static Routes:** A local route is a route that is not shared between neighboring routers.
- **Common Static Routes:** A common route is a route that is shared between neighboring routers.

**Note: The netmask is ignored for routes to specific hosts.**

On the top of the pages above you will see a dynamic list about the local and common static routes.

On the bottom of the pages is where you can modify or add new static route information, and these are defined below.

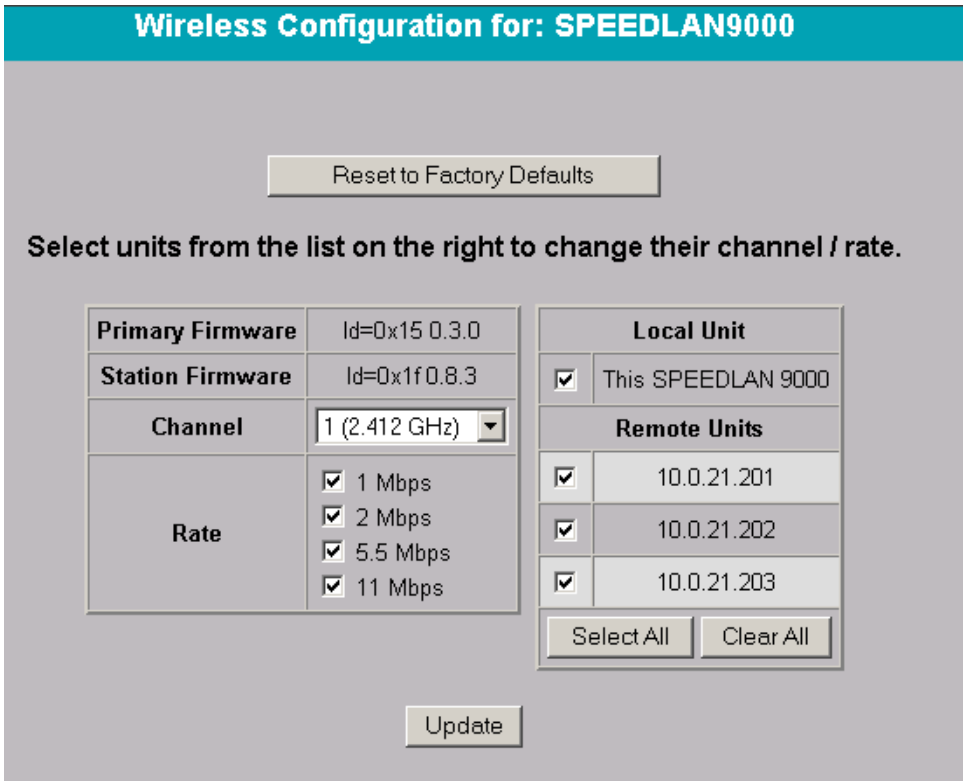
- **Destination:** The destination network or host.
- **Interface:** Select the appropriate interface from this drop-down list.
- **Netmask:** Select the appropriate value for the netmask (also in CIRD format from /8 to 30) in this drop-down list. This is an abbreviated method of entering the netmask. For more information, see *CIDR Table (For Netmask Information Purposes), page 3-15*.
- **Gateway:** This is a network point that acts as the "entrance door" to another network. This is the first "router" that takes you to the designated host (i.e., the next hop on the network).
- **Type:** Select either **net** or **host** from this drop-down list. *Net* - How it will route is destined to another. *Host* - How the route is destined to a specific host.
- Click **Add** to activate the new static route. Click **Delete** to remove a static route. Click **Update** to update static routing information.

## Wireless

Choose **Wireless** to set up the data and frequency rate for your unit/router.

## Configuration

To view the configuration wireless parameters, click the appropriate interface under the **Wireless** menu. Then, choose **Configuration**. A page similar to the following will appear.




The Wireless Configuration page allows you to select the appropriate channel and data rate for your network.

- **Reset to Factory Defaults:** Click to revert to factory settings for this interface.
- **Primary Firmware:** This is the current primary firmware version in use by the wireless card.
- **Station Firmware:** This is the current firmware version in use by the wireless card.
- **Channel:** This is the specific band of frequencies (from 1 to 14) to determine the data path between routers. All SPEEDLAN 9000 routers expected to communicate in each pico cell must have the same channel (frequency).

Select one of the following channels (all are represented in GHz):

**1** 2.412

**2** 2.417

**3** 2.422

**4** 2.427

**5** 2.432

**6** 2.437

**7** 2.442

**8** 2.447

**9** 2.452

**10** 2.457

**11** 2.462

**12** 2.467

**13** 2.472

**14** 2.484

- **Rate**: This setting refers to the RF data rate. The SPEEDLAN 9000 11 Mbps radios have four data rates that can be used. Select one of the following check boxes:
  - **1 Mbps**: This setting limits the card by providing 1 Mbps of bandwidth. The receiver sensitivity of the radio with this setting is -94 dBm.
  - **2 Mbps**: This setting limits the card by providing 2 Mbps of bandwidth. The receiver sensitivity of the radio with this setting is -91 dBm.
  - **5.5 Mbps**: This setting limits the card to providing 5.5 Mbps of bandwidth. The receiver sensitivity of the radio with this setting is -87 dBm.
  - **11 Mbps**: This is the full 11 Mbps data rate. This value is recommended for most installations. The receiver sensitivity of the radio with this setting is -82 dBm.
- **Local Unit**: This is the unit/router you want to change on the local side of the network, and this will be the last unit/router that will be changed.
  Click **Select All** to select all of the units, or click **Clear All** to deselect all units.
- **Remote Units**: These are the units that are visible on the remote side of the network. Remote units will be updated before local units on the network.
  Click **Update** after making changes.

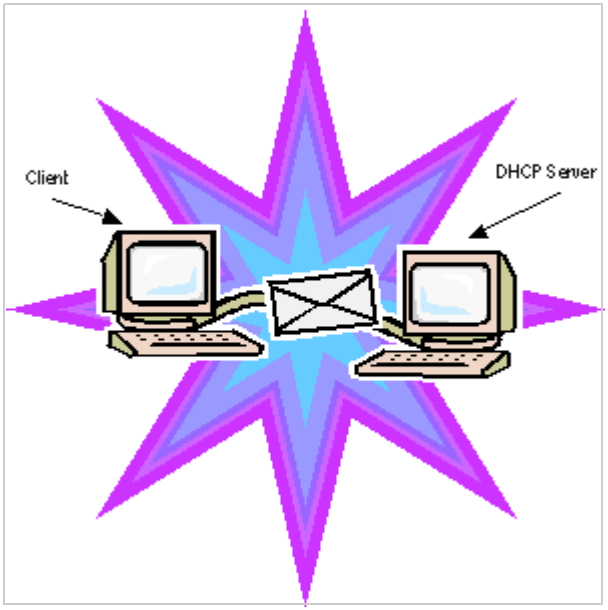
# DHCP Server

The SPEEDLAN 9000 Configurator allows you to define a DHCP server on the Ethernet interface. A DHCP server is configured with a table of Ethernet addresses, ranges of IP addresses and maps that are assigned to client network devices asking for netware settings. The DHCP server uses a "lease" to determine the length of time that a device or interface can use the assigned IP address.

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.

## How DHCP Assigns an IP Address

This section explains how a DHCP server assigns an address. If you are familiar with this terminology, skip to *Basic Instructions for Setting Up DHCP on an Interface, page 3-25*.




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

**Note:** The DHCP server allows IP addresses be assigned dynamically at the remote building. Distributing these administrative functions to each remote building significantly reduces the "administrative overhead" traffic that must travel back to the service provider's headquarters. A DHCP server is configured with a table of IP addresses that are assigned to client network devices asking for

network settings. The DHCP server uses a "lease" to determine the length of time that a device or interface can use the assigned IP address.

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.

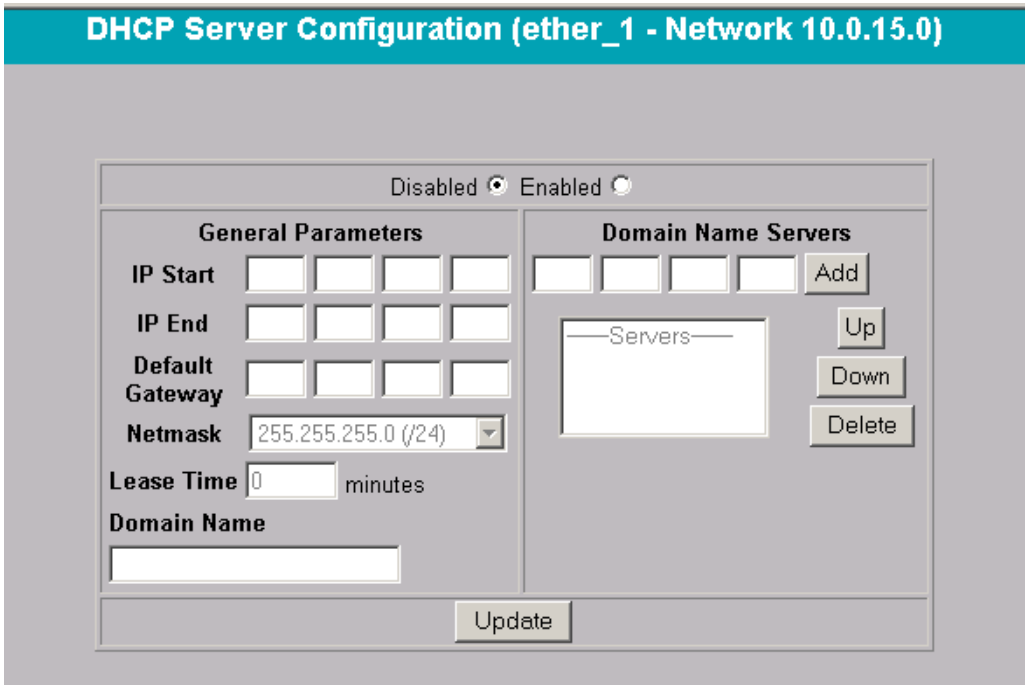
4. DHCP server confirms IP address and configuration.

The SPEEDLAN 9000 Configurator allows you to assign IP addresses via DHCP on the interfaces.

## Basic Instructions for Setting Up DHCP on an Interface

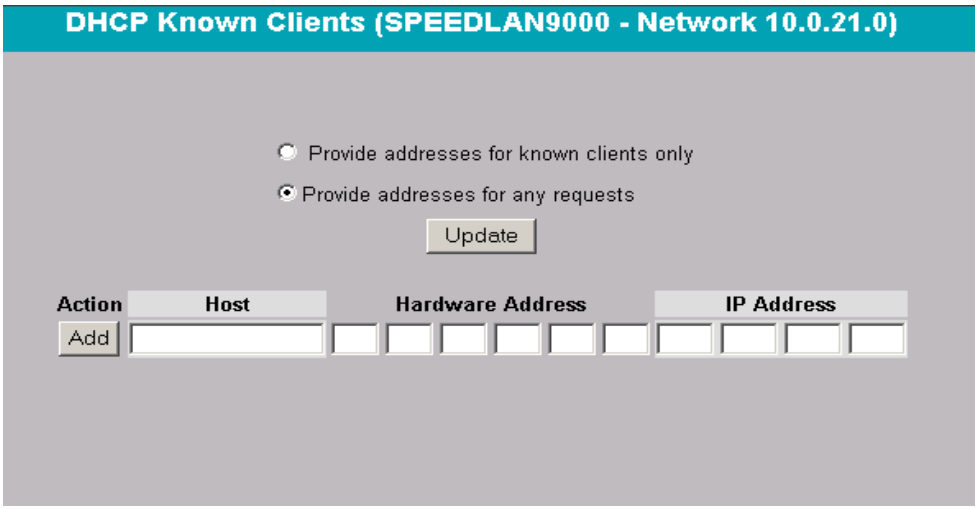
1 Choose **DHCP Server** from the main menu. Then, choose the appropriate interface where you want to offer DHCP.

2 This will bring up the DHCP page. Choose **General Clients** to assign an IP to your DHCP clients. When you define the scope of IP addresses to be assigned, make sure you do not include any of the static IPs that you have assigned on the network. The General Clients page is shown below (for definitions, see *General DHCP Elements Defined, page 3-28*):



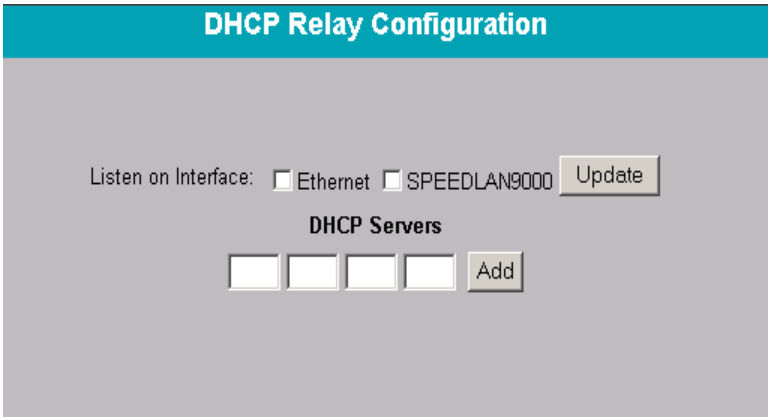

3 If you have IPs that should be assigned to a particular device, do the following:

**a**) Go back to the **DHCP Server** menu and choose the correct interface. Then, choose the **Known Clients** page. This page is shown below (for definitions, see *Known Clients Elements Defined, page 3-29*):




**b**) This is where you can then specify the computer name / MAC address and the corresponding IP address that should be assigned to that device at all times. DHCP can be configured on either interface, or both at the same times easing the administrator overhead when adding new computers or SPEEDLAN 9000 units/routers.

**c**) If your DHCP server is a machine separate from the SPEEDLAN 9000 units/routers, you will need to set up DHCP Relay (by choosing **DHCP Relay** from the main menu). This page is shown below (for definitions, see *DHCP Relay, page 3-30*):



**d**) When you choose **DHCP Relay**, you will be asked to enter the IP address of the DHCP server.

**e**) You then need to enable the Ethernet interface, SPEEDLAN 9000 interface or both. Next, enter the IP address of the DHCP server that is offering IPs to clients. Make sure that any SPEEDLAN 9000 units that are in route to the DHCP server have the DHCP relay enabled and point to the correct DHCP server IP address.

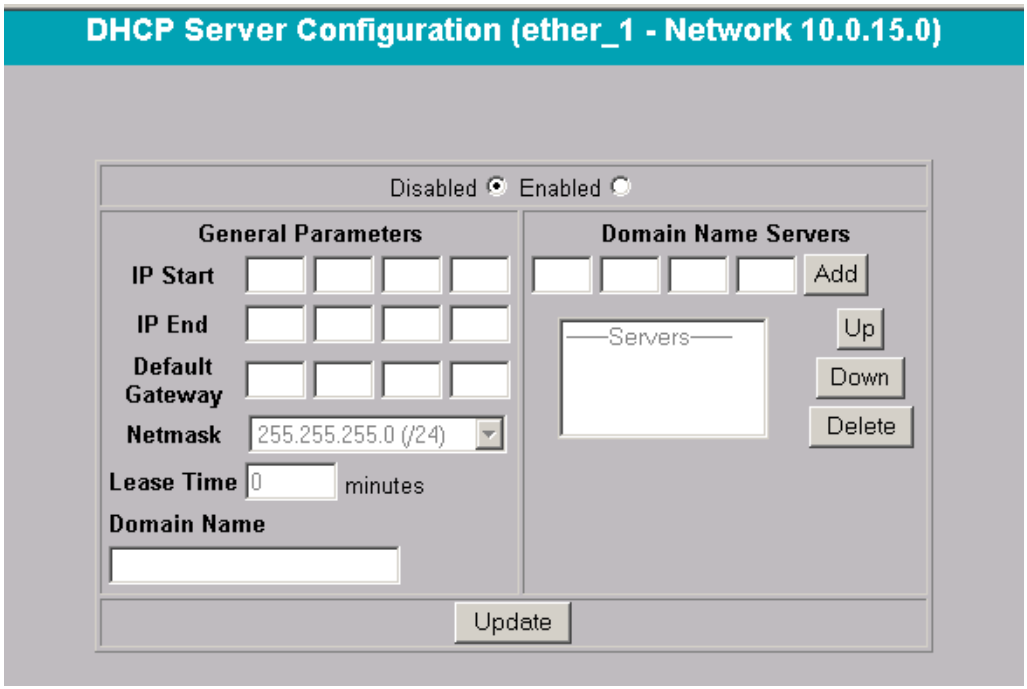
**f**) Once you have set up the SPEEDLAN 9000 unit/router, configure the clients to obtain an IP address from a DHCP server. If the SPEEDLAN 9000 is the DHCP server, it will get the IP address directly from it. If the DHCP server is located behind the SPEEDLAN 9000 units, the DHCP request will be forwarded to the DHCP server and then returned to the correct client machine.

## Elements Defined on the General and Known Client Pages

This section defines the elements described in the above section, called *Basic Instructions for Setting Up DHCP on an Interface, page 3-25*.

## General DHCP Elements Defined

To enter general information about the DHCP server, choose (interface) + **General** from the **DHCP Server** menu. The following page will appear.




- **Disabled**: Select this option to disable the DHCP server.
- **Enabled**: Select this option to enable the DHCP Server.

### General Parameters

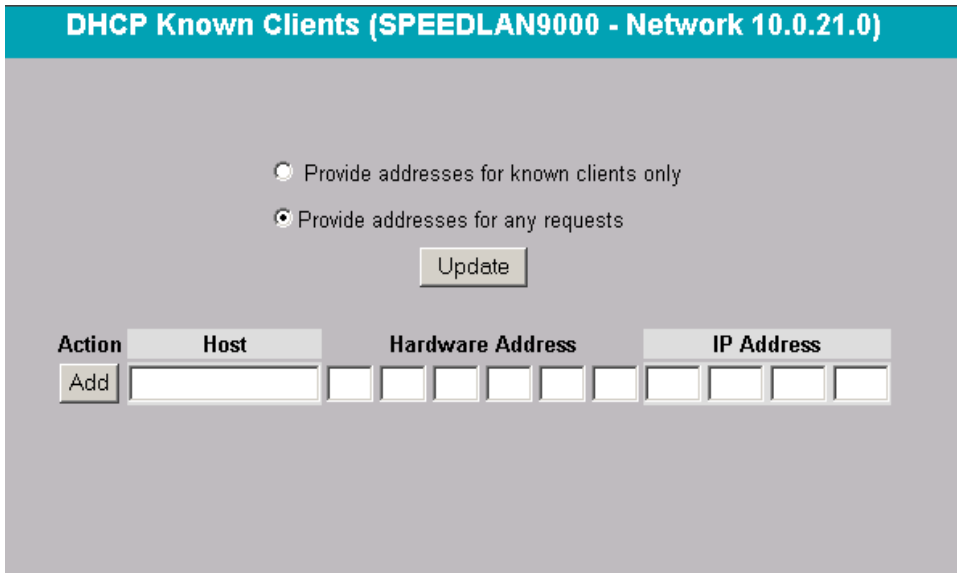
- **IP Start Address:** This is the start of the block of served IP addreses.
- **IP End Address:** This is the end of the block of served IP addresses.
- **Default Gateway:** This is the default gateway that will be assigned to DHCP clients.
- **Netmask:** The netmask is a 4-byte number that masks the network part of the Internet Protocol IP address, so only the host computer part of the address remains.
- **Lease Time (in minutes):** This is the amount of minutes that the interface, computer or device can use the assigned IP address. When the time is up, the IP address will revert to the pool of available addreses and can be reassigned to another computer.
- **Domain Name:** This is the internet domain name of the organization, such as "www.wavewireless.com". You do not enter the first portion of the domain name, leaving the entry as "wavewireless.com".

Domain Name Servers

- **Domain Name Servers (DNS) list box:** This is where the domain name servers reside. You can prioritize them (from highest to lowest) by selecting the DNS, and then clicking **Up** or **Down**.
  - **Up/Down:** After you select the DNS, use this button to prioritize (from highest to lowest) it.
  - If you want to remove any of the DNS parameters, click **Delete**.
- **Update:** If you want to change the DNS address, do one of the following:
  - **To change the Domain Name Server (DNS) address:** Select the DNS address in the **DNS** list box. The DNS address will appear to the left of the Add button. Edit the address and click **Update** when you're finished. The modified address will appear in the DNS list box.
  - **To add a new DNS address:** Enter the new DNS address (to the left of the Add button). Then, click **Add**. The new address will appear in the DNS list box. If you changed any of the DNS servers, click **Update**.

## Known Clients Elements Defined

The feature allows the DHCP server to allow or decline specific client requests. It also allows the mapping of specific IP address to certain specific network hosts. To specify known clients for the DHCP server, choose the appropriate interface + **Known Clients** from the **DHCP Server** menu. The following page will appear.



Select one of the following options:

- **Provide addresses for known clients only:** Provides addresses to those clients that the DHCP server does recognize, and declines address to those clients it does not recognize.
- **Provide addresses for any requests:** Provides addresses to any client.

Next, enter the Host, Hardware Address and IP Address. Click **Update** after you change any information. Click **Delete** to remove information. Click **Add** to add new information.

### Viewing Log Messages

If the DHCP server is not working properly, you can view system log messages by choosing **DHCP Server**. Then, choose **Log Messages.** The page will display log messages for the DHCP server.

### Enabled Interfaces

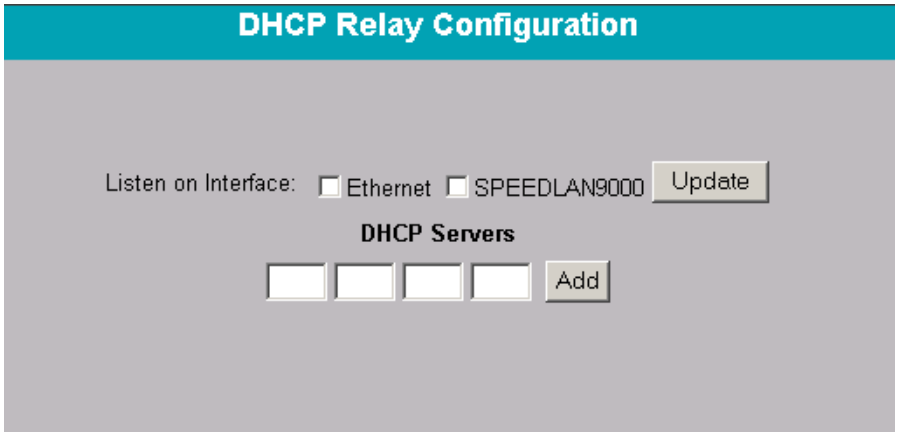
To view a summary of the interfaces that the DHCP server is currently running on, choose **DHCP Server**. Then, choose **Enabled Interfaces.** The page will display the enabled interfaces for the DHCP server.

## DHCP Relay

This section defines the elements described a few pages back in the section, called *Basic Instructions for Setting Up DHCP on an Interface, page 3-25*.

DHCP Relay allows you to configure the SPEEDLAN 9000 to relay (forward) any DHCP requests originating on the wireless interface to a DHCP server outside of the SPEEDLAN 9000 cloud. This allows you to use existing DHCP servers to assign IP addresses and other configuration parameters for SPEEDLAN 9000 routers via their wireless interfaces. If this service is enabled and no DHCP servers are listed, the SPEEDLAN 9000 will relay DHCP requests to the DHCP server that the SPEEDLAN 9000 used to get its wireless interface address. If this service is enabled and the SPEEDLAN 9000 did not use DHCP to get an address for its wireless interface, then there must be at least one DHCP server address listed for this feature to work. To set the DHCP Relay, choose **DHCP**

**Relay** from the main menu. The following page will appear.




Select the check box next to the interface of your choice. Select the appropriate settings for your DHCP Servers. Click **Update** when making changes. Click **Delete** when removing a DHCP Server. Click **Add** to add a new DHCP Server.

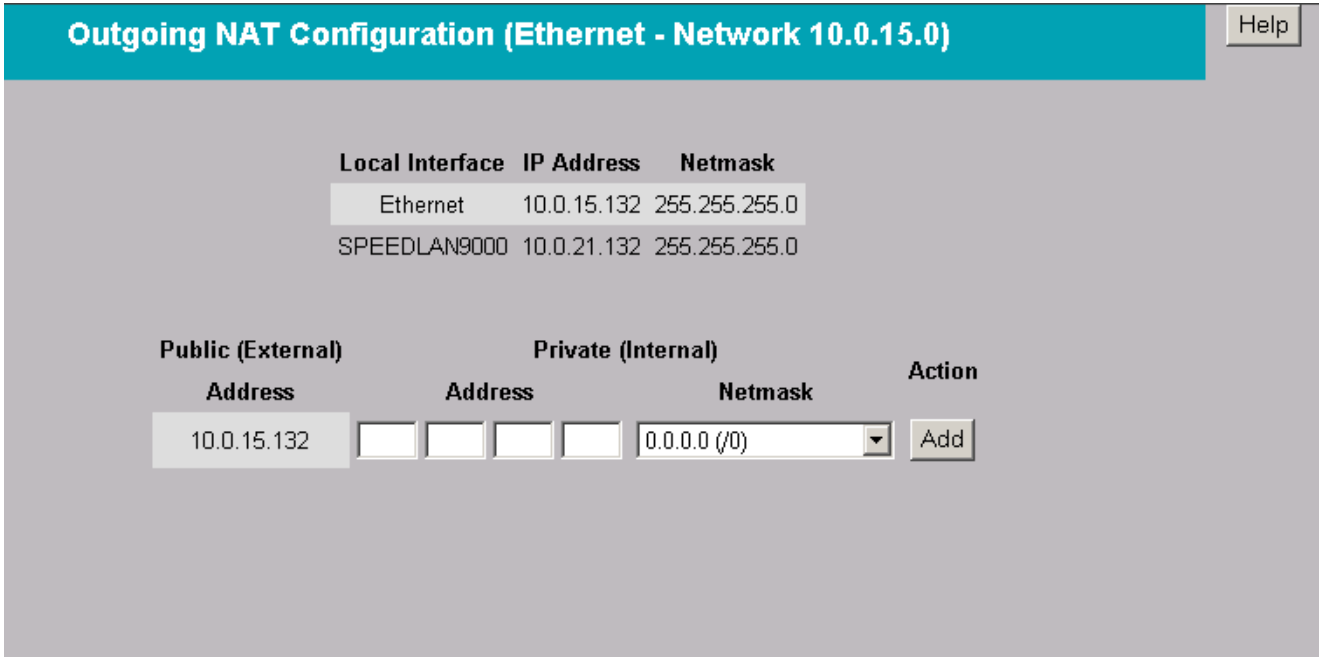
## NAT

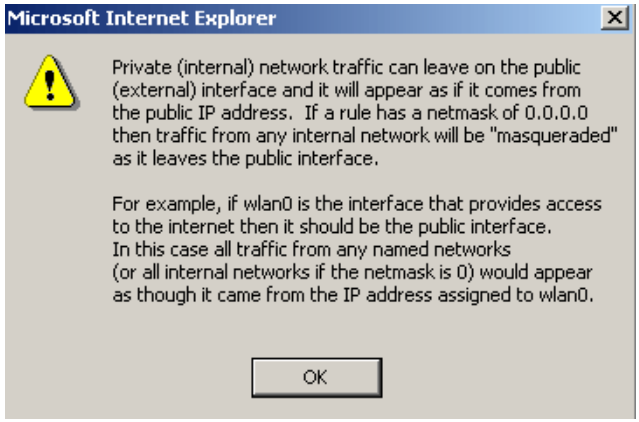
Network Address Translation (NAT) occurs when there is a translation among an Internet Protocol (IP address) used within one network (designated as inside network) to a different IP addresses within another network (designated as outside network). What differentiates from NAPT? NAPT (or Network Address Port Translation) not only translates the IP address but also the transport layer port. Thus, if an inbound packet addressed to port 80 on the NAPT device would be translated and passed to the private network's Web server. Without port translation, the device has no means of knowing which host in the private network can pass packets to other devices.

The SPEEDLAN 9000 Configurator allows you to define parameters for each interface rather than just using one interface for the entire unit/router.

## Outgoing NAT

To set up Outgoing NAT, choose **NAT** from the main menu. Next, choose the interface and **Outgoing NAT**. The following page will appear.




Displays when you press the Help button

The Outgoing NAT parameters are listed below:

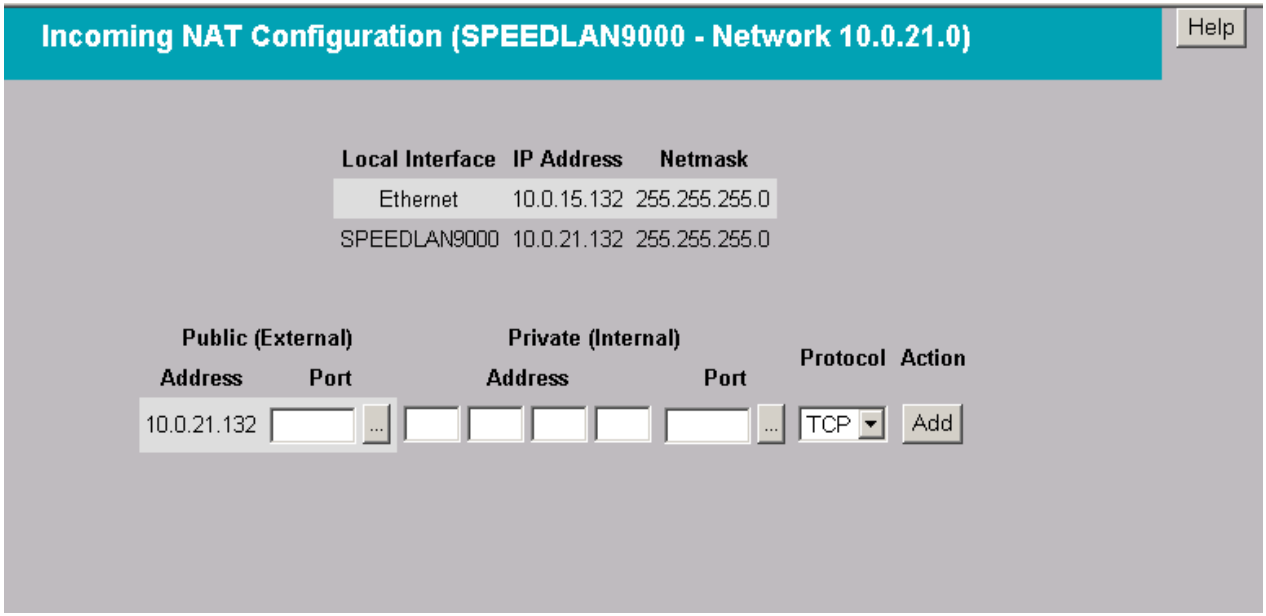
- **Public (External) Address:** Lists the IP address for the outside network.

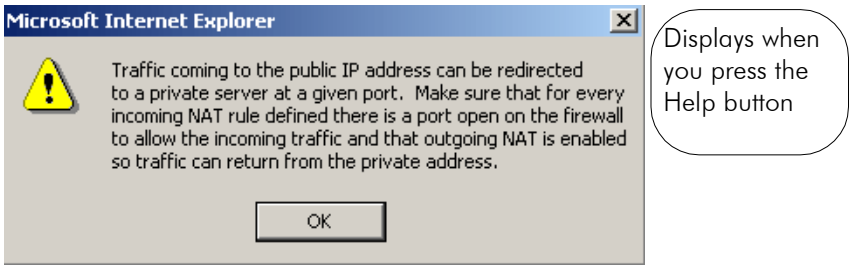
- **Private (Internal) Address:** Enter the IP address for the inside or private network. This address hides behind the Public IP address.
- **Private (Internal) Netmask:** Select the netmask assigned to the private network interface.

**To add a second Private (Internal) address, enter the address and select the correct mask**. Then, click **Add**.

## Incoming NAT

To set up Incoming NAT, choose **NAT** from the main menu. Next, choose the interface and **Incoming**. The following page will appear.




Incoming NAT allows you to specify ports on the private network (Building B) that you would like to be available on the public network (Building A and the Internet). For example, if a web server (IP

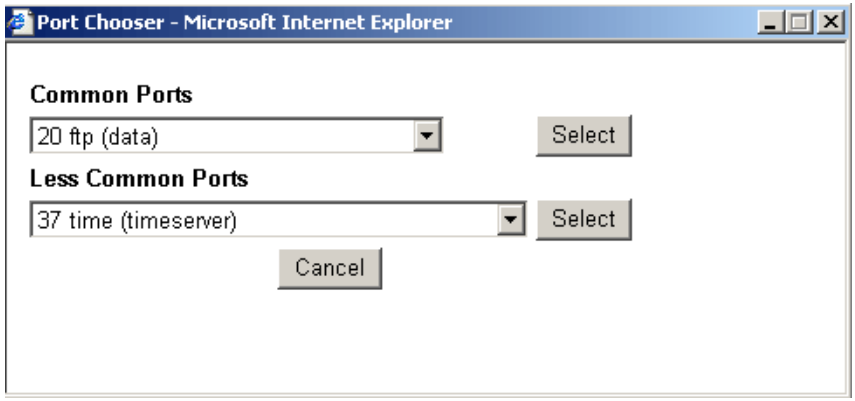
Address 10.0.0.3) is being hosted on a private network in Building B, you can create a pair that will specify that all requests on the public IP address, Port 80, be forwarded to IP Address 10.0.0.3 on the private IP address, Port 80.

The elements on the page are described below:

- **Public (External) IP Address and Port:** This is the desiged outside IP address and port for the outside network.
- **Private (Internal) IP Address and Port:** This is the desiged inside IP address and port for the inside network.
- **Protocol:** Select either **TCP** or **UDP** from this drop-down list.
- Click **Update** when needed to implement new settings.

**Note:** To add an internal address, enter the information (as mentioned above) and click **Add** when finished.

- ***If you want to modify the public address port, click the "..." button. The Port Chooser dialog box will appear, as shown below. Make your selections and click **Update on the Incoming NAT page**.



# Diagnostics & Troubleshooting

Choose **Diagnostics** to troubleshooting network problems. There are four options under this menu: Interface Statistics, ICMP Statistics, Connectivity and System Control.

### Special Note about Link & Ping Tests:

**Note: If you need to perform a link test to verify that your equipment is communicating properly at the RF level, SPEEDView is a excellent tool. This process will help you with the performance evaluation. For more information on how to perform a link test, see *Performing a Bandwidth Test, page 4-13*. You can also perform a ping test if need. For more information, see *Performing a Ping Test, page 4-14*.**

## Interface Statistics

The Interface Statistics menu lists the current available network interfaces. To view interface statistics, Statistics from the main menu. Then, choose the appropriate interface or unit/router. The Interface Statistics page provides traffic information for the appropriate interfaces.

To view the statistics of an interface, choose the appropriate network from the **Statistics** menu. The following page will appear.

**Interface Statistics (Ethernet)**

| Statistic | Number | Since Load | Seconds | Per Second |
|---|---|---|---|---|
| Octets In: | 18,552,472 | 0 | 0 | 0.00 |
| Unicast Packets In: | 49,283 | 0 | 0 | 0.00 |
| Errors In: | 0 | 0 | 0 | 0.00 |
| Octets Out: | 10,631,271 | 0 | 0 | 0.00 |
| Unicast Packets Out: | 38,043 | 0 | 0 | 0.00 |
| Errors Out: | 0 | 0 | 0 | 0.00 |

Refresh Automatically

Each statistic is defined below:

(row headings)

- **Octets In:** Total number of octets (bytes) received on the interface, including framing characters.
- **Unicast Packets In:** This is the number of unicast packets coming into the interface.
- **Errors In:** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **Octets Out:** The total number of octets (bytes) transmitted out of the interface, including framing characters.
- **Unicast Packets Out:** The number of subnetwork-unicast packets delivered to a higher-layer protocol.
- **Errors Out:** The number of outbound packets that were chosen to be discarded, even though they were deliverable. One possible reason for discarding such a packet could be to free up buffer space.

(column headings)

- **Statistic:** Type of statistic represented.
- **Number:** Represents the number of bytes, or number of errors.
- **Since Load:** The bytes or errors since this page was first loaded.
- **Seconds:** How many seconds ago this page was loaded.
- **Per Second:** Represents traffic information per second.

Click **Refresh** to automatically have the statistics continually updated every three seconds.

## ARP Table

ARP is the abbreviation for Address Resolution Protocol, which maps an IP address to a machine's hardware address. Network administrators use ARP to locate systems on the LAN that are configured with incorrect IP addresses.

To open the ARP table, choose **ARP Table** from the **Routing** menu. The following page will appear.

**ARP Table**

| IP Address | HW Type | Flags | HW Address | Interface |
|---|---|---|---|---|
| 10.0.0.1 | 0x1 | 0x2 | 00:30:85:7D:A7:80 | eth0 |
| 10.0.0.125 | 0x1 | 0x2 | 00:01:03:20:8E:07 | eth0 |

The ARP statistics are defined below:

- **IP address:** The IP address corresponding to the media-dependent 'physical' MAC address.
- **HW Type:** The hardware type as reported by Linux.
- **Flags:** The ARP flags as reported by Linux.
- **HW Address:** In a LAN environment each computer contains its own Medium Access Control (MAC) address which is the embedded and unique hardware number.
- **Interface:** The interface on which this entry is effective.

## ICMP Statistics

ICMP is the abbreviation for Internet Control Message Protocol. ICMP supplies messages and error reports for packets that travel between host servers and gateways. To view ICMP information, choose **ICMP Stats** from the **Routing** menu. The following page will appear.

**ICMP Statistics**

| In Bound | Value | ? | Out Bound | Value | ? |
|---|---|---|---|---|---|
| Msgs | 6 | ? | Msgs | 5 | ? |
| Errors | 0 | ? | Errors | 0 | ? |
| Dest Unreach | 0 | ? | Dest Unreach | 2 | ? |
| Time Exceeds | 0 | ? | Time Exceeds | 0 | ? |
| Param Problems | 0 | ? | Param Problems | 0 | ? |
| Src Quenches | 0 | ? | Src Quenches | 0 | ? |
| Redirects | 0 | ? | Redirects | 0 | ? |
| Echos | 3 | ? | Echos | 0 | ? |
| Echo Replies | 3 | ? | Echo Replies | 3 | ? |
| Timestamps | 0 | ? | Timestamps | 0 | ? |
| Timestamp Replies | 0 | ? | Timestamp Replies | 0 | ? |
| Addr Masks | 0 | ? | Addr Masks | 0 | ? |
| Addr Mask Replies | 0 | ? | Addr Mask Replies | 0 | ? |

**Description**

```
The number of ICMP Timestamp (request) messages received.
```

The In Bound statistics are defined below:

- **Msgs**: The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
- **Errors**: The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
- **Dest Unreach**: The number of ICMP Destination Unreachable messages received.
- **Time Exceeds**: The number of ICMP Time Exceeded messages received.
- **Param Problems**: The number of ICMP Parameter Problem messages received.
- **Src Quenches**: The number of ICMP Source Quench messages received.
- **Redirects**: The number of ICMP Redirect messages received.
- **Echos**: The number of ICMP Echo (request) messages received.
- **Echo Replies**: The number of ICMP Echo Reply messages received.
- **Timestamps**: The number of ICMP Timestamp (request) messages received.
- **Timestamp Replies**: The number of ICMP Timestamp Reply messages received.
- **Addr Masks**: The number of ICMP Address Mask Request messages received.
- **Addr Mask Replies**: The number of ICMP Address Mask Reply messages received.

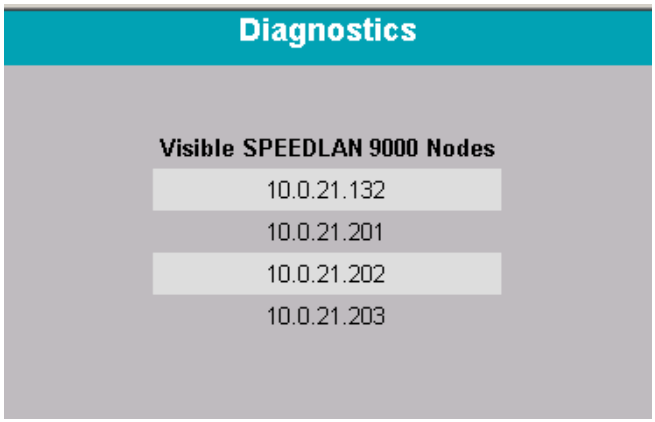
The Out Bound statistics are defined below:

- **Msgs**: The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
- **Errors**: The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
- **Dest Unreach**: The number of ICMP Destination Unreachable messages sent.
- **Time Exceeds**: The number of ICMP Time Exceeded messages sent.
- **Param Problems**: The number of ICMP Parameter Problem messages sent.
- **Src Quenches**: The number of ICMP Source Quench messages sent.
- **Redirects**: The number of ICMP Redirect messages sent.
- **Echos**: The number of ICMP Echo (request) messages sent.
- **Echo Replies**: The number of ICMP Echo Reply messages sent.
- **Timestamps**: The number of ICMP Timestamp (request) messages sent.
- **Timestamp Replies**: The number of ICMP Timestamp Reply messages sent.

- **Addr Masks:** The number of ICMP Address Mask Request messages sent.
- **Addr Mask Replies:** The number of ICMP Address Mask Reply messages sent.

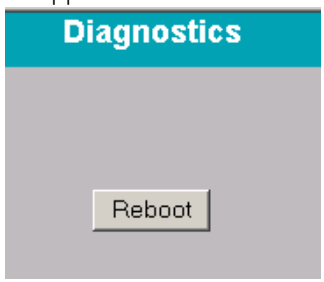
## Connectivity

The Connectivity page will list any other routers that the SPEEDLAN 9000 can currently see. To display this page, choose **Connectivity** from the Diagnostics menu. The following page will appear.




## System Control

To reboot or power off the current SPEEDLAN 9000, choose **System Control** from the **Diagnostics** menu. The following page will appear.




### Reboot

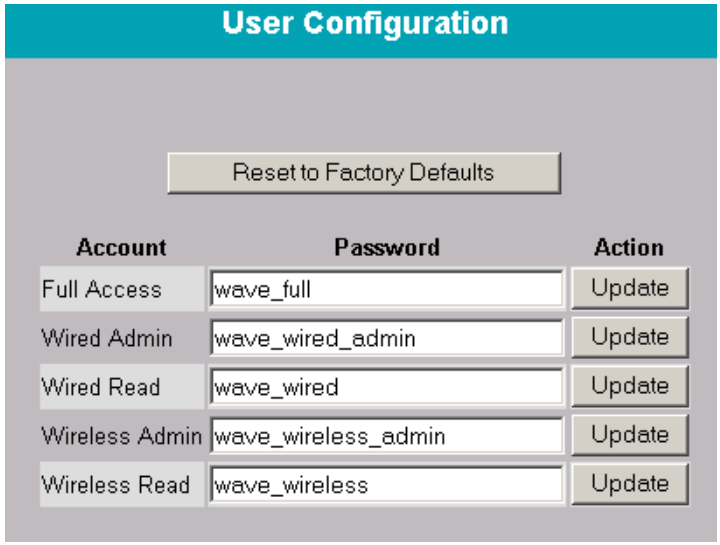
Click this button to reboot the SPEEDLAN 9000.

# Administrative Access Pages

If you want to limit administrative rights to certain users, choose the **Admin** menu. This is where you can restrict users by modifying information on the Users and Permissions pages. You can also replicate certain configuration settings from the current SPEEDLAN 9000 to other SPEEDLAN 9000s on the network by using the Replication submenu. For more information, see *Replication, page 3-42*. You can also remotely turn off or reboot other SPEEDLAN 9000s on the network by using the Remote Control submenu. For more information, see *Remote Control, page 3-43*. In addition, you can also reset the entire configuration of the SPEEDLAN 9000 factory default settings. For more information, see *Factory Reset, page 3-43*.

## User Configuration

When logged on with the full-access password, you will see the Users page. To activate this page, choose **Users** from the **Admin** menu. The following page will appear.




The classes of users are described in *Classes of Users, page 3-10*.

The User Configuration page allows you to set the SPEEDLAN 9000 Configuration edit the password for each type of user: Full Access, Wired Admin, Wired Read, Wireless Admin and Wireless Read. After you make any changes, click **Update**.

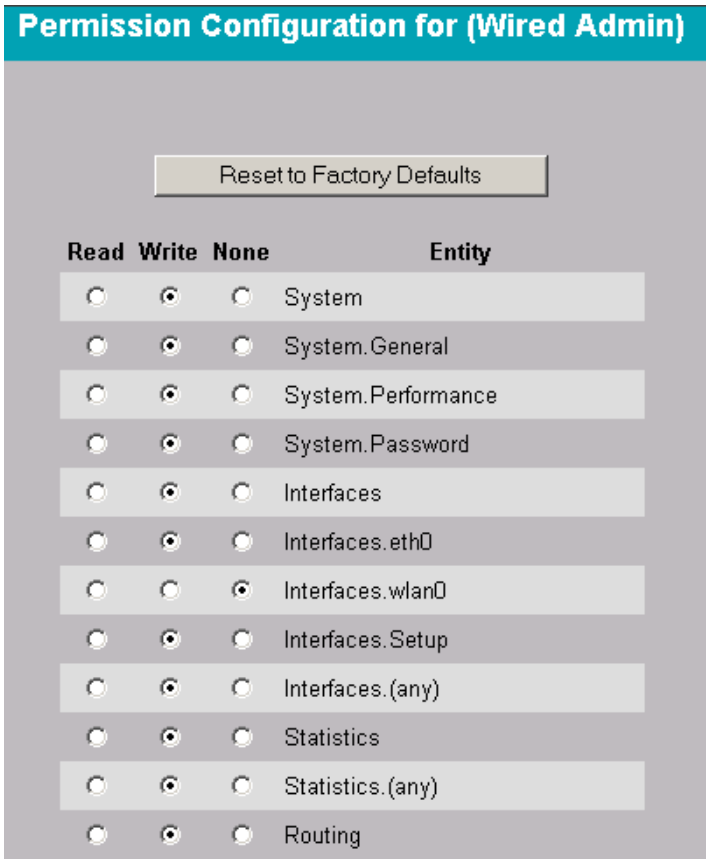
To revert to factory default settings, click **Reset to Factory Defaults**.

## Permissions

If you want to restrict certain settings to users, choose **Permissions** from the **Admin** menu. Then, click the appropriate selection:

- **Wired Admin**: To modify wired administrative user configuration.
- **Wired Read**: To modify wired read-only user configuration.
- **Wireless Admin**: To modify wireless administrative user configuration.
- **Wireless Read**: To modify wireless read-only user configuration.

On top of the page, you'll see four columns labeled: Read, Write, None and Entity. Then the following page will appear.



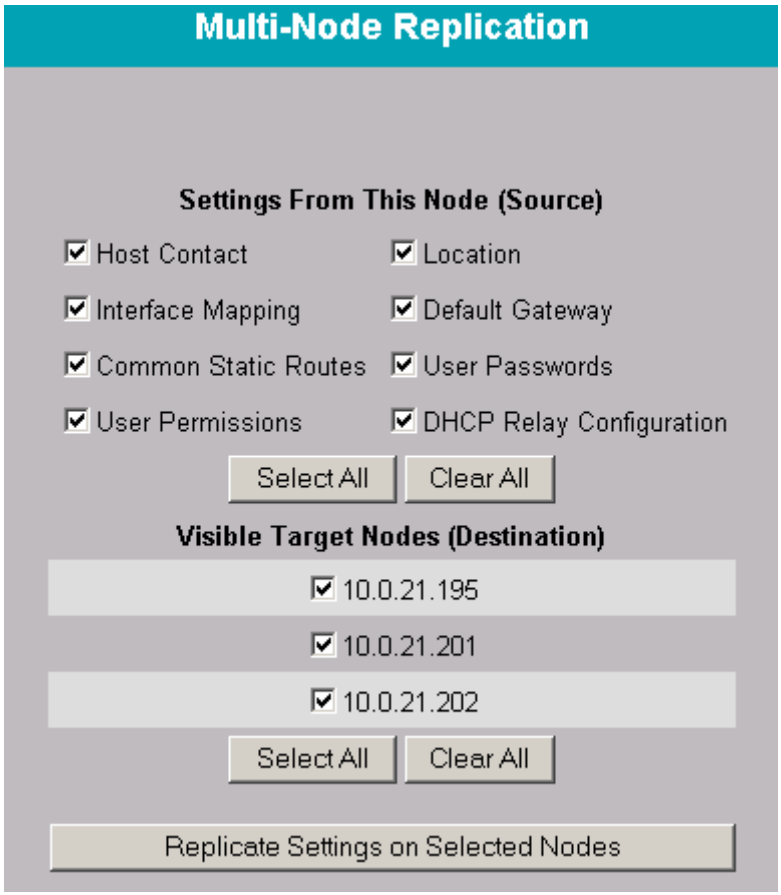

- **Read** column: Select the entities (web pages) that you want the full user to view. The user will not be able to edit any entities.
- **Write** column: Select the entities (web pages) that you want the user to edit.
- **None** column: Select the entities (web pages) that you do not want the user to view or edit.

- **Entity** column: Displays "configuration elements" that you want the "user" to access.

A description of each web page can be found in *Overview of the PH9000 Configurator Main Menu, page 5-7*. Be sure to click **Update** after you made your changes.

## Replication

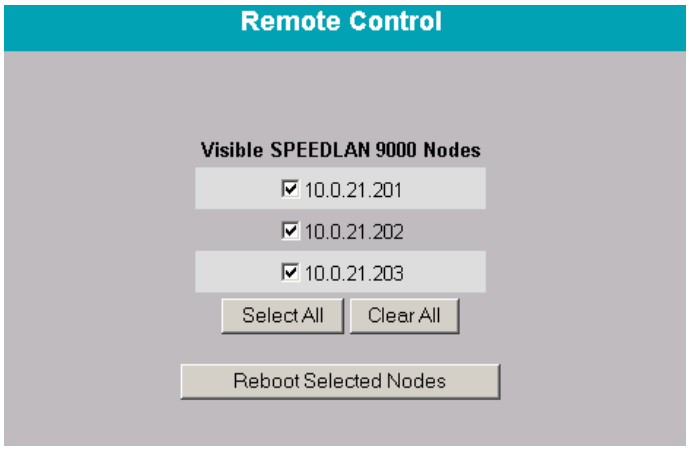
This page lets you copy setting from one unit to another unit on the network. To do this, choose **Replicate** from the **Admin** menu. The following page will appear.




Select the settings from the source router you want to replicate. Then, select the target router where the settings will be replicated. Next, click **Replicate Settings on Selected Nodes**.

## Remote Control

To remotely reboot or turn off SPEEDLAN 9000 routers, choose **Remote Control** from the **Admin** menu. The following page will appear.

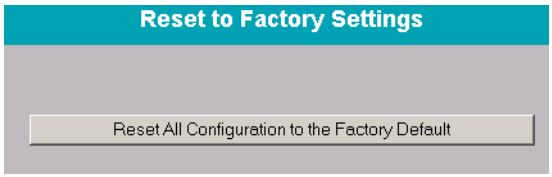



To reboot SPEEDLAN 9000 routers

Select the routers you want to reboot and click **Reboot Selected Nodes**.

## Factory Reset

If you need to reset the entire configuration of the SPEEDLAN 9000 to factory default settings, choose **Factory Reset** from the **Admin** menu. The following page will appear.




To implement the factory reset, simply click **Reset All Configuration to the Factory Default**.

Notes:

# Chapter 4
# Using SPEEDView

# What is SPEEDView?

SPEEDView provides an “at-a-glance” view of all the nodes currently on the network. Network managers can monitor and control management functions for local and remote SPEEDLAN 9000 nodes from a central location, or from anywhere on the network. SPEEDView operates on a Windows platform, or can be used on mobile hand-held devices, such as iPAQs for “on-site” monitoring.

Check your operations quickly with a dynamic graphical user interface, and view the performance of network links through an easy-to-read graphical format. SPEEDView uses display lines to indicate direct line-of-sight connections, obstructed connections (due to network bugs or improper mounting of the antenna) and non-existent physical connections. These indicators, along with included diagnostic testing features, will help network managers troubleshoot antenna alignment and located blocked nodes, so that paths can be re-routed for successful connectivity. In addition, you can double-click any node to monitor and update its configuration in a web-based browser called the SPEEDLAN 9000 Configurator.

## System Requirements

- Runs on the following Windows platforms: 98, NT (Service Pack 4.0), 2000 or XP
- 10 Megabytes of Hard Drive Disk Space
- CD-ROM Drive (for installation)
- Monitor (monochrome is sufficient but VGA or better is highly recommended)
- SPEEDView is compatible with SPEEDLAN 9000 products.

# Installation Instructions

1. Insert the **SPEEDView** CD into your CD-ROM drive. If the install program does not start automatically, proceed with the following steps:
   - Click **Start** on the Windows taskbar. The Start menu appears.
   - Choose **Run** from the **Start** menu. The Run dialog box appears.
   - Locate the executable (setup.exe), depending on the location of your CD-ROM.
2. Follow the installation prompts.

# Starting SPEEDView

1 When the installation is finished, start the **SPEEDView** application by doing one of the following:

- Click the **SPEEDView** shortcut icon on the desktop, as shown below.

- From the Windows **Start** menu, choose **Programs+WaveWireless+SPEEDView**. (If SPEEDView was installed in another folder, select the appropriate directory.)

2 The SPEEDView Login dialog box appears.

3 Enter the IP address (or hostname if you are using a Domain Name Server) of the 9000 node you want to connect to in the **Node IP Address** text box.

4 The passwords are defined, based on user class level, in the SPEEDLAN 9000 Configurator. Before you enter the password, decide which account level you should enter:

- Administrator: allows access to all of SPEEDView's features. You would enter "Full Access" in the **Password** text box.
- Read Only: limits the following features: Admin tab, TCP dump functions, bandwidth tests, bandwidth toolbar and block and unblock features (items under the Link menu). You would enter "Wired Read" for wired nodes or "Wireless Read" for wireless nodes in the **Password** text box.

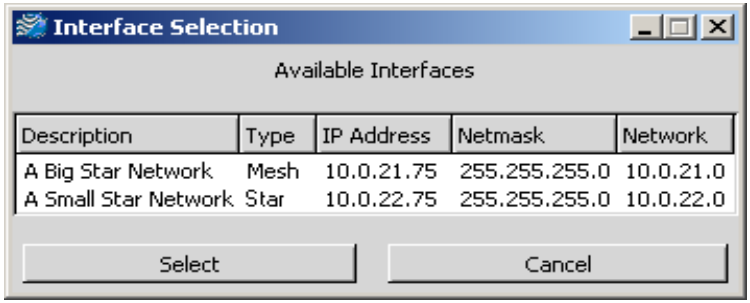
**Note:** If you want SPEEDView to recall the password for future logins, click **Remember Password**.

5 Click **Login**.

**Note:** The Status box (blank text box) at the bottom of the screen displays the status of the connection.

**Note:** You can change the default text for the SPEEDView application by clicking **Start**+**Settings**+**Control Panel**+**Display**+**Appearance** tab. Then, select the appropriate item in the **Item** list.

6 Next, the Interface Selection box appears which displays all the wireless interfaces that are connected to the SPEEDLAN 9000 system.

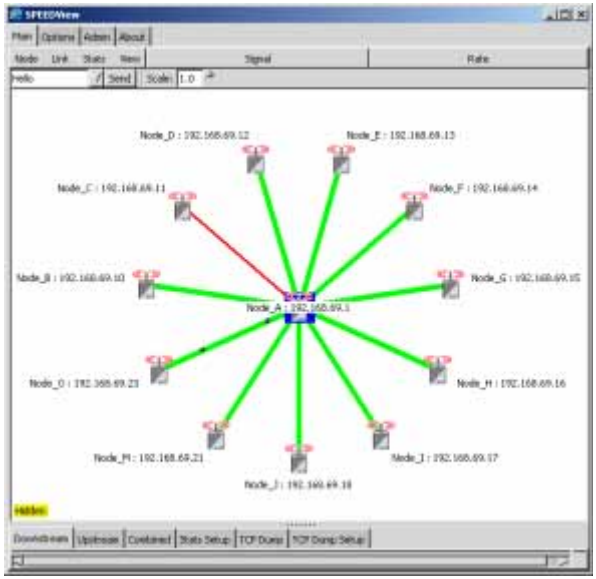



7 Highlight the interface and click **Select**.

8 The following elements are displayed on this box:

- **Description:** A name for the interface (e.g., where it is located). This can be changed in the Configurator.
- **Type:** Star (for base to CPE functionality) or mesh (nodes in a NLOS pico cell). The star or mesh network will display on the Main tab, as shown on the next page.
- **IP Address:** This address tells the network how to locate the computers or network equipment connected to it.
- **Netmask:** The netmask is a 4-byte number that masks the network part of the Internet Protocol IP address, so that only the host computer part of the IP address remains.
- **Network:** The address of the network.

## Star Network

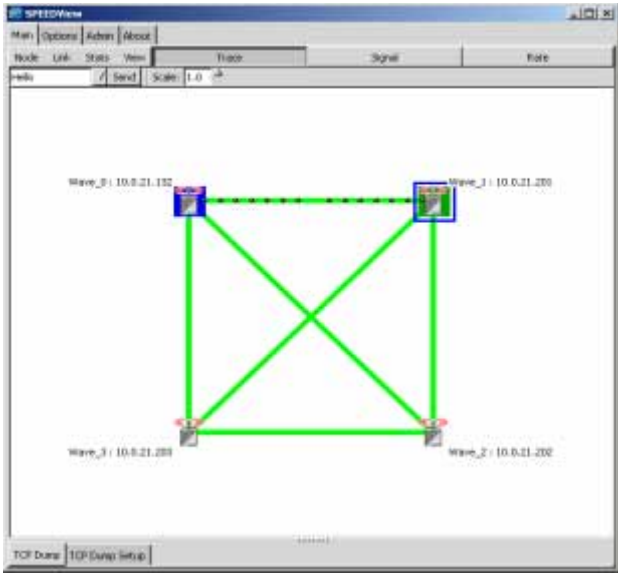


**Note:** A star network consists of a group of remote nodes, called Customer Premise Equipment (abbreviated as CPE) and a base station (in the center of the star). A star network is based on a star topology, thus each CPE must have clear line-of-sight to the base station. (The star node icons are aligned symmetrically.)

**Note:** You can adjust how many octets are displayed by clicking the **Options** tab.

**Note:** You can view other wireless networks attached to the current 9000 node. Do this by right-clicking on the node where SPEEDView is connected (on the network diagram). Next, a submenu will pop up on your screen that lists all of the available wireless interfaces. Select the appropriate network (star or mesh).

### Mesh Network




**Note:** A mesh network consists of nodes that have non-line-of-sight (NLOS) functionality, meaning they are able to route around obstructions by finding the next closest node within line-of-sight. Mesh nodes reside in a NLOS pico cell. Each node can communicate up to a 1/2 mile with its neighboring node. Nodes in the same NLOS pico cell do not need a central base station to communicate with each other, and any node can be reached. However, NLOS pico cells can be linked to other NLOS pico cells via gateways and base stations in other LOS networks to improve scalability.

**Note:** (For more information about star and mesh functionality, see *SPEEDLAN K2's Polling Protocol -- How it Works in Star Networks, page 1-5* and *SPEEDLAN 9000 Mesh Protocol -- How It Works in Non-Line-of-Sight Networks, page 1-8*.

## The Program Instructions

**Note:** The Options tab is used for altering the way data is displayed on the Main tab (e.g., font size, number of octets shown, etc.). The Admin tab is used for rebooting nodes on the 9000 network. The About tab contains version information about the SPEEDView application. The Options, Admin and About tabs are described in greater detail at the end of this document. For more information, see

*Options Tab, page 4-19.*

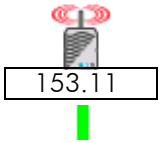
## The Main Tab

The elements on the Main tab are discussed in the following order:


- *The Main Tab Icons, page 4-8*
- *The Node, Link, Stats and View Menus (on the Main tab), page 4-10*
- *Buttons (on the Main tab), page 4-11*
- *Performing a Bandwidth Test, page 4-13*
- *Performing a Ping Test, page 4-14*
- *Accessing the Statistics Tabs on Bottom of Main Tab, page 4-15*

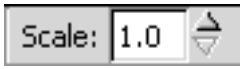
## The Main Tab Icons

Represents each SPEEDLAN 9000 node. The numerical digit (e.g., "51") represents the last octet(s) of the node's IP address. (This is also referred to as the IP address or IP label. For more information, see *Options Tab, page 4-19*.) To view more than one octet or change the font size of the octet(s), click the **Options** tab. If you want to display the hostname to the left of the IP address, click **Show Hostname** on the **Options** tab.

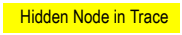



The signal, noise and bit rate for each node pair are indicated inside square boxes, as shown to the left of this paragraph. The higher the signal, the better. The lower the noise, the better. These values are dynamic and change constantly to reflect the current state of the network. To include the signal and noise level, click **Signal** (on the Main tab). To include the bit rate, click **Rate** (on the Main tab). To include the noise level, click **Show Noise** on the **Options** tab. To view signal and noise in dBm, click **Show dBm** on the **Options** tab. For more information, see *Options Tab, page 4-19*.

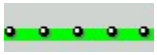
A test message (i.e., Hello, Goodybe, Testing, Marco!, Polo!) can be sent to any node in the network. The message is automatically echoed by the receiving node and displayed on your screen to verify end-to-end connectivity between the nodes. In addition, if another user is currently logged into the destination node via SPEEDView, he will see your message flash on his the upper left-hand corner of his network diagram.



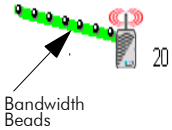

The zoom in/zoom out icon is displayed to the right of the test message. Click the **up** arrow to zoom in, and click the **down** arrow to zoom out. If you click on the network diagram, you can also move it around the desktop.




Black text on yellow indicates that one or more nodes are hidden, and this message box will be displayed in the lower left-hand corner of the Main tab. For directions on how to hide a node, see, "Hide" under the *The Node, Link, Stats and View Menus (on the Main tab), page 4-10*.



Represents a Trace Route test. Trace Routes are used for mesh networks only. For directions on how to create a trace route, see, "Trace" under the *Buttons (on the Main tab), page 4-11*.




In a star topology, bandwidth on any given link is shown as a series of black beads, as shown to the left. When the bandwidth beads are closer, this indicates that more bandwidth is being used. When these beads are further apart, less bandwidth is being used.

Blue, box outlines indicate that the node is selected. Solid green boxes indicate that the node is the target of a trace route.

Solid, blue squares indicate which 9000 node SPEEDView is connected to. The IP address of the node will be displayed on top of each node. You can display the full IP address or part of it by selecting how many octets you want displayed. For more information, see *Options Tab, page 4-19*.

**Can the nodes hear each other?**



Green lines indicate direct line-of-site connections between SPEEDLAN 9000 nodes.



Solid, red lines indicate that there is not enough signal strength to reliably exchange data between the node pair, but some signal was detected on at least one end of the connection.



Dashed, red lines indicate no signal between the node pair.

Red lines are used for debugging and adjusting antennas (e.g., who can hear and why). If a solid, red line appears, the system would still use an indirect route or hop in order for the two nodes to exchange data.

A redline without any signal level means that there is no direct communication between the node pair, and data will automatically be routed through the 9000 network in order for the node pair to communicate. It is a user configurable option as to whether a dashed red line, or no line at all, appears between the node pair without direct communication.

## The Node, Link, Stats and View Menus (on the Main tab)

There are several commands located under the Node, Link, Stats and View menus on the main tab.

### Node menu

- Configure: Choose **Configure** to launch the SPEEDLAN 9000 Configurator, which is a web browser used to view/configure many parameters and services for that node. This is the same as double-clicking any node. See the SPEEDLAN 9000 Series Installation and Operation Manual for further instructions.
- Hide: If there are too many nodes to comprehensively view on the 9000 network, select the nodes you want to hide and choose **Hide**.
- Show: Choose **Show** to display any nodes that were previously hidden using the "Hide" feature.
- Select All: If you want to select all of the nodes on the 9000 network (including hidden), choose **Select All**. This is useful for hiding a large number of nodes.

### Link menu

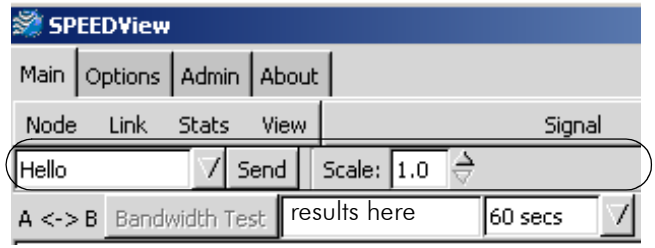
- Bandwidth Test: Choose **Bandwidth Test** and a node pair or link to verify that your equipment is communicating properly at the RF level. This process will help you during your performance evaluation. See *Performing a Bandwidth Test, page 4-13* for further instructions.
- Ping Test: Choose **Ping Test** to verify node connectivity. See *Performing a Ping Test, page 4-14* for further instructions.
- Block: (This command is used with mesh networks only.) Select the node pair or link. (Press the **Ctrl** key on your keyboard to select more than one node or link at a time.) Next, choose **Block**. When you "block" a connection, the node pair will not be able to communicate.
- Unblock: (This command is used with mesh networks only.) Select the nodes or links you want to unblock. Next, choose **Unblock** to clear the "blocked" path.

### Stats menu

- Show All Link Stats: Choose **Show All Link Stats** to display all the statistics of all of the links in the statistics window (bottom half of Main tab).
- Clear Stats: Choose **Clear Stats** to remove the statistics of the links in the statistics window (bottom half of Main tab).

View menu

- Message Toolbar: Choose **Message Toolbar** to display the test message box just under the Node menu.
- Bandwidth Toolbar: Choose **Bandwidth Toolbar** to display a short-cut version of the bandwidth test (displays results of traffic moving in both directions of the selected link). Next, you will see the bandwidth toolbar appear on the top of the Main tab, as circled below.




Choose the duration: 15, 30 or 60 seconds. Then, click **Bandwidth Test**. The results will be displayed in the box to the right of the Bandwidth Test button.

- Zoom: Choose **Zoom** to zoom in or out.

## Buttons (on the Main tab)

- Send: Click this button to send a UDP-based test message to any node on the 9000 network. Select the test message from the drop-down list such as: Hello, Goodbye, Testing, Marco or Polo (located just under the Main tab).

Then, select the node where you want to send the test message and click **Send**. The remote node automatically echoes the message back to the originating node.

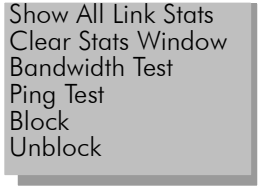
If successful, you will see your message flash (in blue) on your network diagram. This indicates a successful round trip of the data.
**Note:** If someone is monitoring the remote node with another instance of SPEEDView, he will also see your message appear.

- Trace: (This button appears for mesh networks only.) Click this button to trace the data flow between the node pair or link. To set up a trace route, select the destination node. (The node you are connected to is the source.) Then, choose **Trace**. You will see the links chosen by the routing algorithm in order to send data from the source node to the destination

node. The screen shot on the Main tab with a mesh network (*Mesh Network, page 4-6*) displays a trace route --> .

- Multi-sel: (This button is used for iPAQs only; all Windows operating systems will use the standard Ctrl key command to select more than one node.) This button allows iPAQ users to select more than one node. To deselect nodes, simply click anywhere on the white screen of the Main tab. Alternatively (and for Windows operating systems), you can deselect any individual node by clicking on that node. This button is useful when setting up "blocked" paths (under the Link menu), or "hiding" nodes (under the Node menu).
- Signal: Click this button to display the signal strength. Higher values show stronger received signal strength. The values range from 1-255.
- Rate: Click this button to view the data rate (in Mb/s).

**Note:** If you right-click on the white area in the network diagram, a pop-up submenu will appear displaying short-cut features depending on the type of network selected.

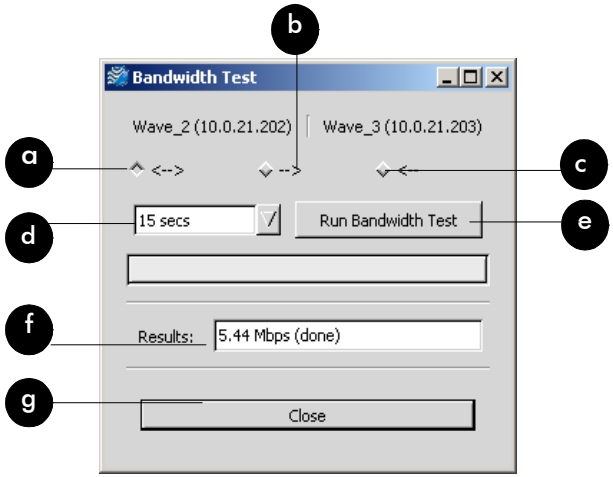



These short-cuts are described above.

**Note:** Block and Unblock are used for mesh networks only.

## Performing a Bandwidth Test

1. Click the node pair or link that you want to test.
2. Choose **Bandwidth Test** under the **Link** menu. The Bandwidth Test dialog box will appear, as shown below:



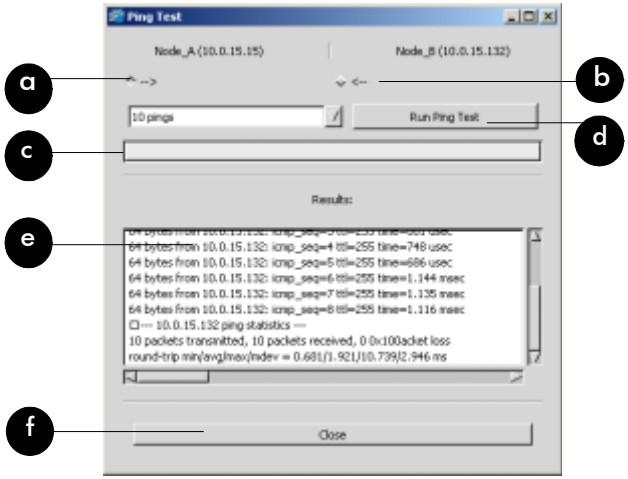

The elements on the Bandwidth Test dialog box are described below:

- **a**: Tests the full duplex path (e.g., from Node A to B and then from Node B to A).
- **b**: Tests the path going to the right (e.g., from Node A to Node B).
- **c**: Tests the path going to the left (e.g., from Node B to Node A).
- **d**: The length of time (in seconds) for the bandwidth test.
- **e**: Executes the bandwidth test.
- **f**: Displays results of the bandwidth test (in Mb/s).
- **g**: Closes the Bandwidth Test dialog box.

## Performing a Ping Test

1 Click the node(s) you want to ping.

2 Choose **Ping Test** from the **Link** menu. The Ping Test dialog box will appear, as shown below:

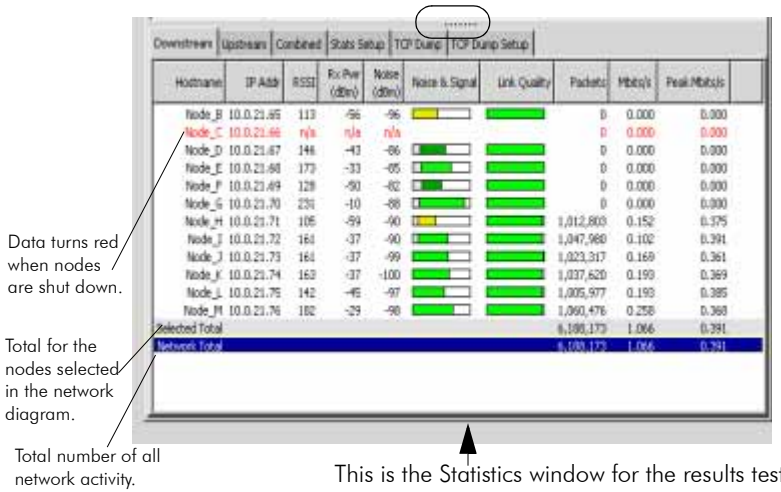



The elements on the Bandwidth Test dialog box are described below:

- **a**: Pings the path to the right (e.g., from Node A to Node B).
- **b**: Pings the path to the left (e.g., from Node B to Node A).
- **c**: The status bar.
- **d**: Executes the ping test.
- **e**: Displays the results of the ping test.
- **f**: Closes the Ping Test dialog box.

## Accessing the Statistics Tabs on Bottom of Main Tab

If you want to enlarge the statistics window, place your mouse on the splitter bar ".....", as circled below.




Next, you will see a double arrow pointing up and down, as shown below:

Click and push up (to enlarge the window) or down to (decrease the size of the window). The statistic tabs look similar to the Statistics window shown above.

**Note:** If you want to remove a link from the Statistics window, right click your mouse in the window, choose the link row and choose **Remove Link** (as shown below).

### Downstream Tab

This tab displays information regarding the number of packets moving downstream in the network. This tab is used only with star networks.

### Upstream Tab

This tab displays information regarding the number of packets moving upstream in the network. This tab is used only with star networks.

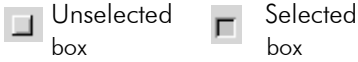
## Combined Tab

This tab displays information regarding the total number of packets moving downstream and upstream in the network. This tab is used only with star networks.

**Note:** In star networks upstream is from CPE to base and downstream is from base to CPE.

## Stats Setup Tab

This tab allows you to set up the statistics that display on the Downstream, Upstream and Combined tabs. This tab is used only with star networks. Select the boxes next to the statistics that you would like to be displayed, as shown below.



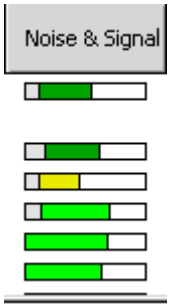

- You can also click **Select All** (to display all statistics) or **None** (to select no statistics).
- Click **Zero Counters** to temporarily set all packet, byte, polls and missed counters to zero (0).
- Click **Reset Counters** to put the counters back to their original values.

The following are statistics you can select to display on the Downstream, Upstream and Combined sub tabs:

**Note:** All statistics on this tab are updated every 3 seconds.

- **Hostname:** The name of the host. Hostnames are set using the SPEEDLAN 9000 Configurator.
- **IP Address:** This is the IP address of the node.
- **Uptime:** The amount of time the node has been running.
- **RSSI:** The Receive Signal Strength Indicator, not measured in dBm.
- **Noise:** The amount of interference before the packets were received (not measured in dBm), the lower the better.
- **Rx Pwr (dBm):** This is the signal strength expressed in dBm.
- **Noise (dBm):** The noise before the packets were received in dBm.
- **SNR (dB):** The Signal-to-Noise Ratio, the higher the better.

- **Noise & Signal:** A combined graphical depiction of signal and noise percentage.




Noise: gray = noise

Signal:
Light green = good activity,
Dark green = acceptable activity,
and yellow = poor activity

- **Link Quality:** The percentage of polls the CPE responds to. The higher the number, the better. This displays the quality of the link. Light green = good activity (50% or higher). Dark green = acceptable activity. Yellow = Poor activity).
- **Polls:** The number of times the station has been polled.
- **Missed (Polls):** The number of polls that the base station sent that the CPE did not respond to. This statistic is also updated every 3 seconds.
- **Packets:** The number of packets that were received (downstream, upstream or combined).
- **Bytes:** The number of bytes that were sent to the interface.
- **Kbits/s:** The current bandwidth (downstream, upstream or combined).
- **Mbits/s:** The current bandwidth (downstream, upstream or combined).
- **Peak Kbits/s:** The highest rate of data transfer reached (downstream, upstream or combined).
- **Peak Mbits/s:** The highest rate of data transfer reached (downstream, upstream or combined).
- **Protocols:** (UDP, TCP, ICMP, HTTP, POP3, SMTP, TELNET, FTP, FTP_DATA and SSH).

Notes:

- Statistics related to mesh networks on this tab are the following: hostname, Mbits/s, IP address, Peak Mbits/s, RSSI, Rx Pwr (dBm), Kbits/s and Peak Kbits/s.
- Statistics related to star networks on this tab are the following: Hostname, Noise (dBm), Packets, Protocol-related information, IP address, Bytes, Uptime, Noise and signal, Kbits/s, RSSI, Link quality, Peak Kbits/s, Noise, Polls, Mbits/s, Rx Power (dBm), Missed polls and Peak Mbits/s.

## TCP Dump Tab

This tab allows you to look at packet headers on a given network interface as they occur. This is useful for determining what traffic a node is receiving when debugging a network connection. This tab is used with star and mesh networks.

- **Start:** Click the node that you want to "tcp dump" and click this button.
- **Stop:** Stops the tcp dump.
- **Clear:** Click to clear all information in the output window.
- **Show Routes:** Click to query the current routing table for the selected node.
- **Save to File:** Click to save all text in the output window for diagnostic purposes.

## TCP Setup

This tab allows you to set up TCP Dump. This tab is used with star and mesh networks.

- **Use:** Select this box to activate the item you want to include.
- **Item:** The item to filter.
- **Src:** The filter item only applies to the source of the packet.
- **Dest:** The filter items only applies to the destination of the packet.
- **IP Address:** Use this to include (exclude) the display of packets destined for or coming from (or both) to a given network host.
- **Port:** Use this to include (exclude) the display of packets destined for or coming from (or both) a given network port. Select port by protocol: HTTP (80), POP3 (110), SMTP (25), TELNET (23), FTP (21), FTP_Data (20), SSH (22) or Custom (the port you enter).
- **Protocol:** Select either **arp** (Address Resolution Protocol), **ip** (Internet Protocol), **tcp** (Transmission Control Protocol), and **udp** (User Datagram Protocol)
- **Interface:** The wired (i.e., eth1) or wireless (i.e., wlan1) interface where the device is connected.
- **Include Selected From Above:** Click to enter the selected criteria into the “Include” filter list.
- **Exclude Selected From Above:** Click to exclude the selected criteria into the "Exclude" filter list.
- **Remove Selected:** Highlight the filter criteria you want to remove and click this button.
- **Clear:** Click to remove all filter criteria items from this box.

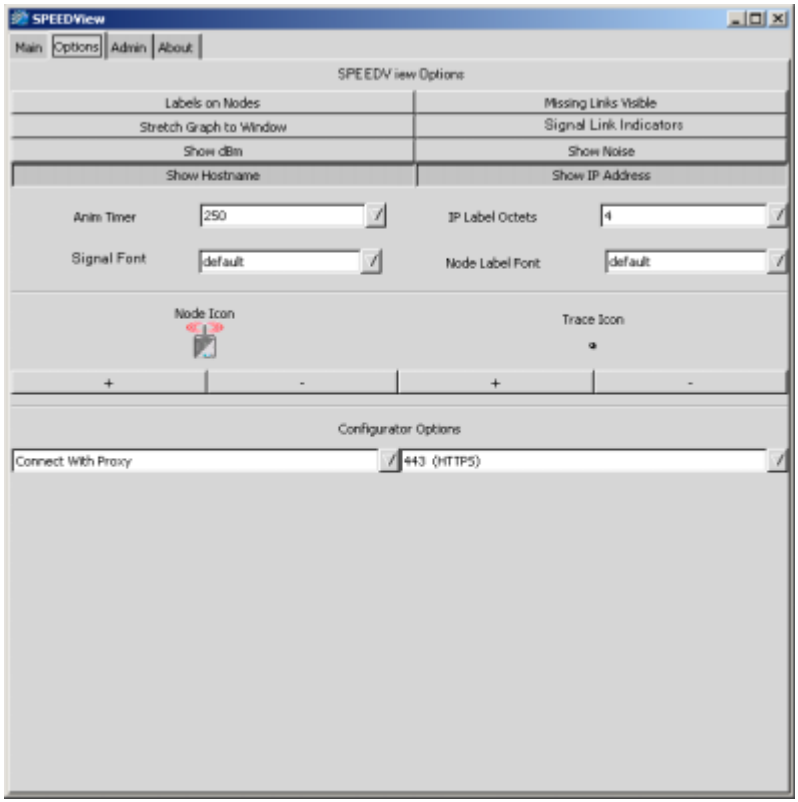
Select the boxes next to the filter item that you would like to define, as shown below.

Unselected box

Selected box

# Options Tab

To customize how the network diagram will appear on the Main tab, click the **Options** tab. The following tab will appear.




Elements on Options Tab:

- **IP Labels on Nodes:** Click to display the IP address (IP label) on the node. If this item is not selected, the IP label will be displayed next to the node.
- **Stretch Graph to Window:** Click if you want the network diagram to use all of the available window space.
- **Show dBm:** Click to show the dBm (decibels per milliwatt). 0 dBm is defined as 1 mw at 1 kHz of frequency at 600 ohms of impedance (displays near node on Main tab).
  Note: Signal (on the Main tab) must be selected to show the dBm.
- **Show Hostname:** Click to show the hostname of the wireless node (displays on node on Main tab).
- **Missing Links Visible:** Click to display broken links. The broken (or disconnected) link will appear as a red, dashed line. This link appears when there is no signal strength between nodes. If this item is not selected, the link will be absent between the broken links.

- **Signal Link Indicators:** Selecting this item will produce graphical link indications to show which link a Signal label is attached to. This is useful for a large number of nodes. In order to display the signal, you must have clicked **Signal** (on the Main tab).
- **Show Noise:** Click to show the noise for the wireless node (displays to the right of the Signal on the Main tab). In order to display the noise, you must have clicked **Signal** (on the Main tab).
- **Show IP Address:** Click to show the IP address for the wireless node (displays on node on Main tab).
- **Anim Timer (Animation Timer):** Select this drop-down list to change the animation speed during a trace route test. The speed is measured in milliseconds.
- **Signal Font:** To change the font size of the signal, click this drop-down list and select one of the following: **default**, **tiny**, **small**, **medium** or **large**.
- **IP Label Octets:** To change how many octets appear for the label (IP address or IP label) on the **Main** tab, click this drop-down list. You can select up to 4 octets. (Note that selecting "**4**" will display the full IP address.)
- **Node Label Font:** This is the font used to display the IP Label. To change the size, click this drop-down list and select one of the following: **default**, **tiny**, **small**, **medium** or **large**.
- **Node Icon:** This displays how the SPEEDLAN 9000 node will appear on the Main tab. You can select one of the following: **Smiley Face**, **Node**, **SPEEDView** icon (small and large) or a **Computer** icon.
- **Trace Icon:** This displays which Trace Route icon (**star** or **black** dot) will appear on the network diagram (on the Main tab). The default is shown below).

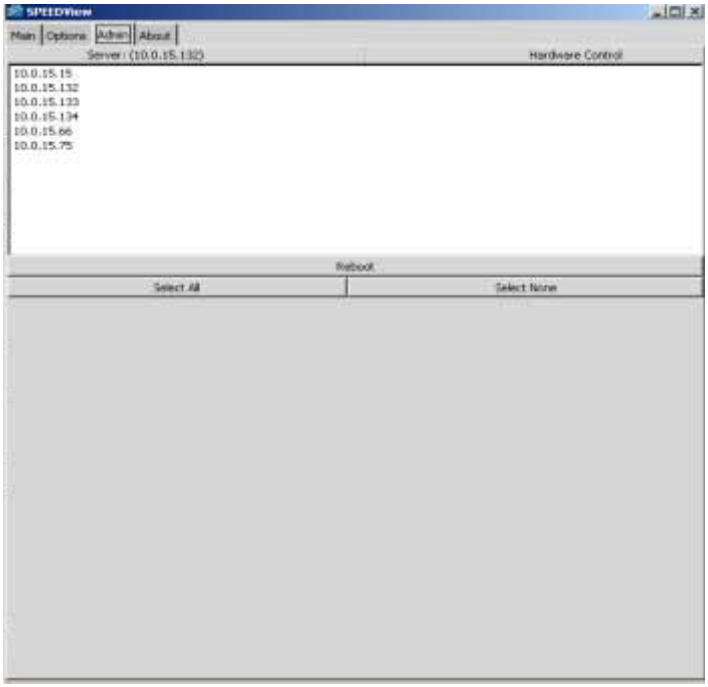
- "**+**" **button:** Select this button to move forward.
- "**-**"**button:** Select this button to move backward.
- **Configurator Options:**
  - The drop-down list to the left lets you connect directly to SPEEDView or via proxy. Using **Connect with Proxy** is the default because you will likely not have a TCP route to all nodes in the SPEEDView network diagram. In this mode the connection is proxied through the 9000 node where it is connected. Selecting **Connect Directly** is faster, but it assumes you do have a direct route to the 9000 node you are trying to configure (and it must have a route back to your computer).
  - The drop-down list to the right allows 4 available ports to configure each 9000 node. The first two are the standard HTTP port (80) and the standard HTTPS port (443). Over an insecure network using HTTPS is preferred to protect configuration passwords. There are two alternate ports for configuration (6589 and 6590). That is, in case you

have forwarded the standard HTTP and HTTPS ports on the 9000 node that you are trying to configure (for the web servers behind it).

## Admin Tab

If you want to reboot one or more 9000 node(s), click the Admin tab. The Admin tab will appear (as displayed on the right side of this page).

- To reboot all nodes (under the Server section), click **Select All**.
- To reboot only specific nodes, choose the first node you want to reboot. Then, hold down the **CTRL** key and click any additional nodes you want to reboot.
- If you do not want to reboot any nodes, click **Select None**.




**Note:** To view version and license information, click the **About** tab.

Copyright/Liability
Copyright ©2002. Wave Wireless Networking. All rights reserved. SPEEDLAN and SPEEDCOM are registered trademarks of Wave Wireless Networking. SPEEDView, Wave Wireless Networking and the Wave Wireless Networking logo are trademarks of Wave Wireless Networking. All other trademarks mentioned in this document are the property of their respective owners.

Notes:

# Chapter 5
# Basics of IP Addressing

Main sections in this chapter:


- *What is an IP address?, page 5-2*
- *Internet Address Classes, page 5-2*
- *How does a network administrator assign an IP address?, page 5-7*
- *What is DHCP?, page 5-7*
- *What is NAT?, page 5-9*
- *NAPT, page 5-9*
- *Diagram of Outgoing NAT, page 5-10*
- *Diagram of Incoming NAT, page 5-11*

# Basics 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 units/routers, by reading just the first three bits of the address field, designate which network class it belongs to. This selection simplifies the way units/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 unit/router discovery packets to learn all of the units/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 units/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.

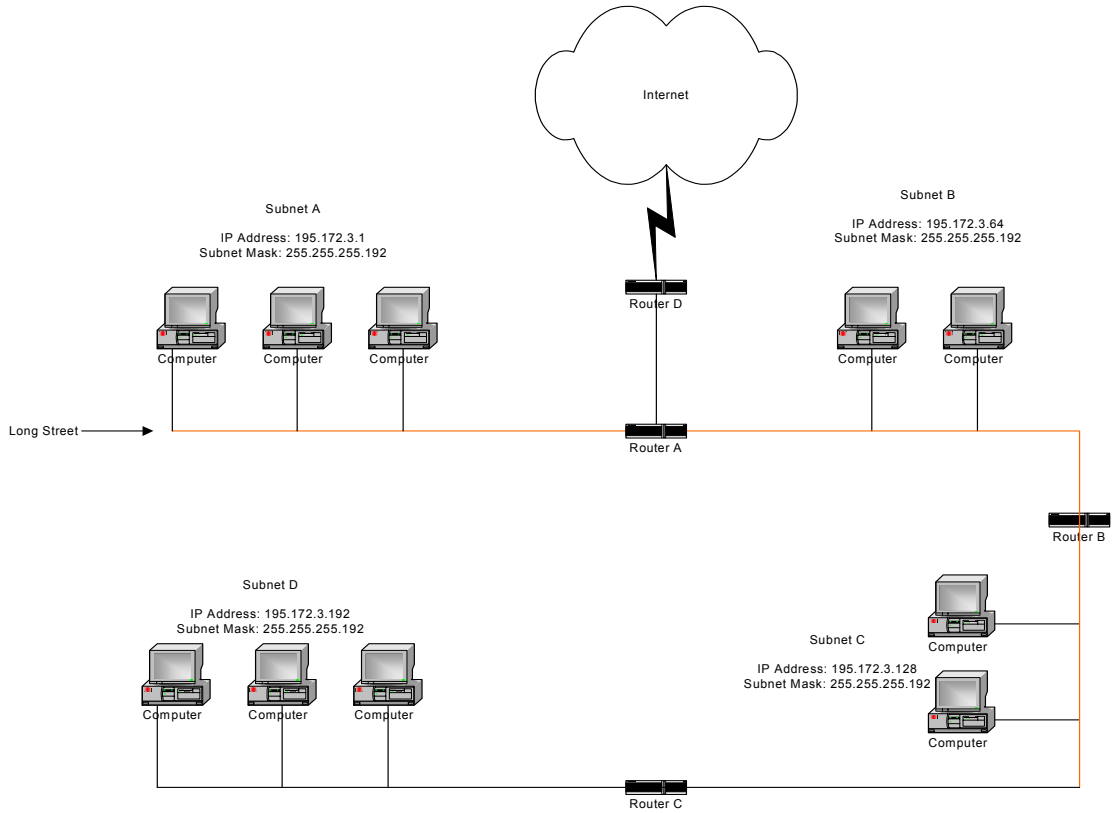
For more information on subnetting, see the example below and *Diagram of Subnetting a Network, page 5-6*.

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 Unit/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 units/ 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. Unit/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 unit/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 SectorPRC interface 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 - Is 'Manually Configure' option on Interfaces Parameters page of 9000 Configuator**
  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 - Is 'Use DHCP' option on Interface Parameters page of 9000 Configurator**
  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.

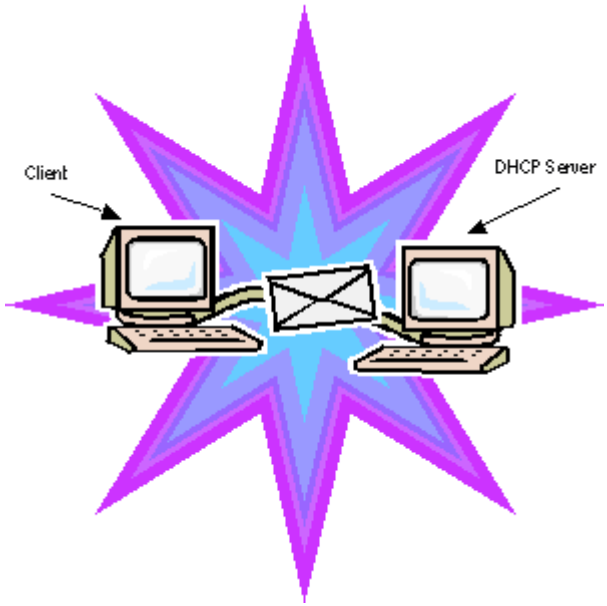
## What is DHCP?

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 and 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.

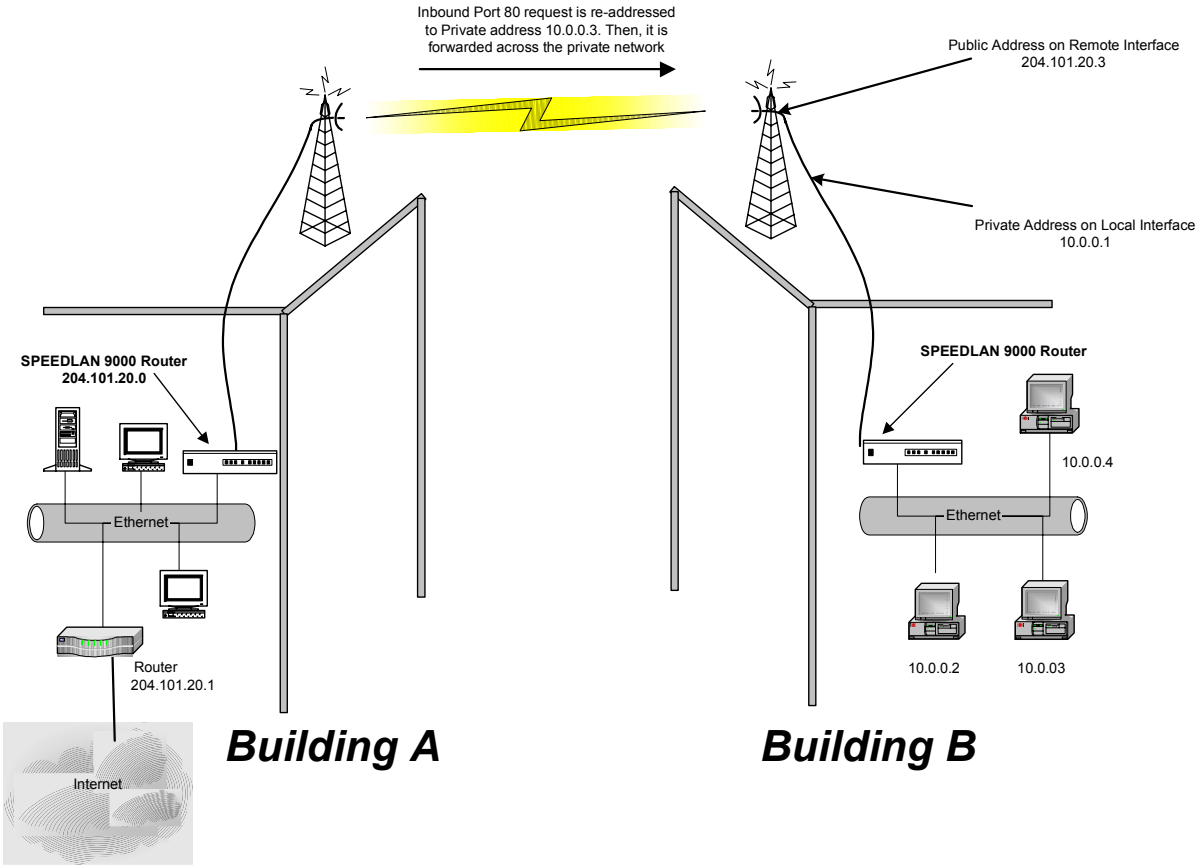
Network Address Translation (NAT) occurs when there is a translation among an Internet Protocol (IP address) used within one network (designated as inside network) to a different IP addresses within another network (designated as outside network). Network Address Translators (NATs) allow companies to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

## NAPT

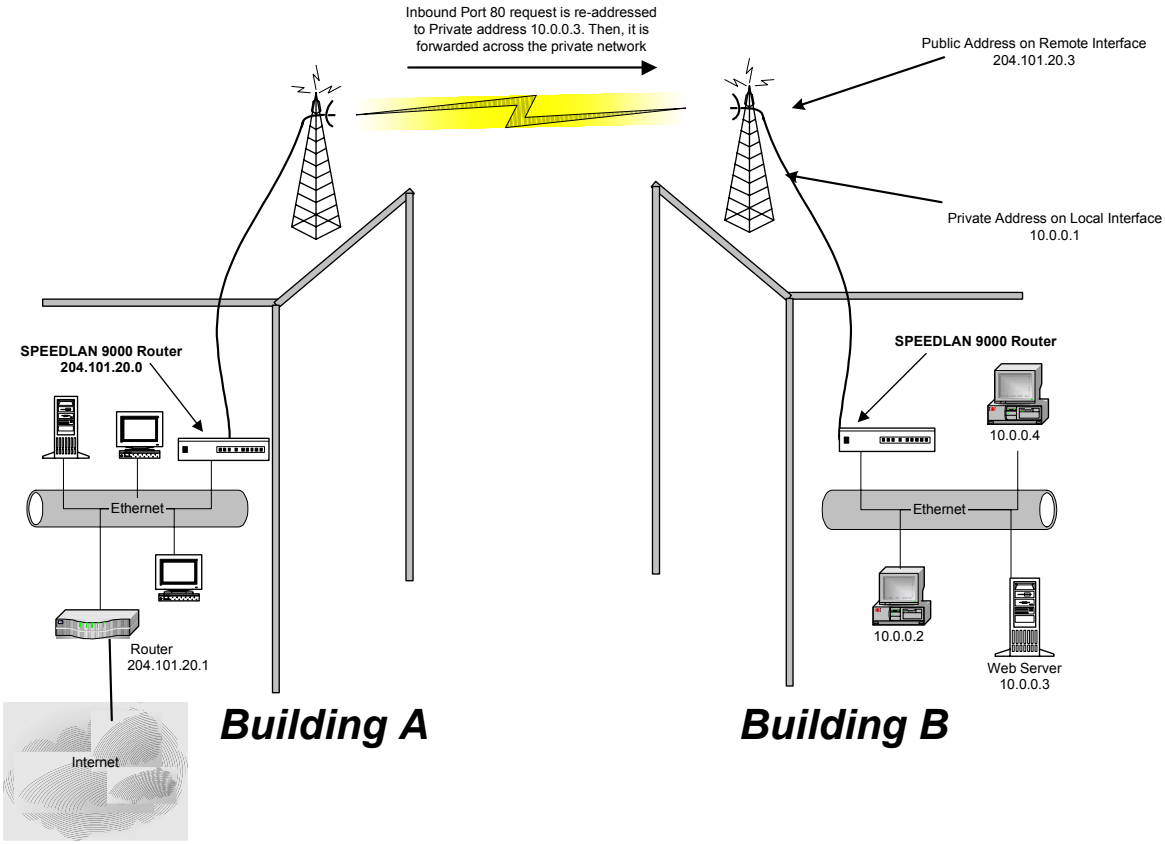
What differentiates NAPT from NAT? NAPT (or Network Address Port Translation) not only translates the IP address but also the transport layer port. Thus, if an inbound packet addressed to port 80 on the NAPT device would be translated and passed to the private network's Web server. Without port translation, the NAT device has no means of knowing which host in the private network can pass packets to other devices. For an example see, *Diagram of Incoming NAT, page 5-11*.

## Diagram of Outgoing NAT




As the packet is transmitted from the private network (in Building B) across the public network (public address in Building A and the Internet), the packet will be re-addressed as 204.101.20.3 (public address). When the packet returns to SPEEDLAN SectorPRC interface 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




Incoming NAT allows you to specify ports on the private network (Building B) that you would like to be available on the public network (Building A and the Internet). For example, if a web server (IP Address 10.0.0.3) is being hosted on a private network in Building B, 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.

Notes:

# Glossary for Standard Data Communications

# Glossary for Standard Data Communications

### Alignment
In order to create a successful link, all related equipment should be associated to its respective attachments or equipment.

### Amplitude
The magnitude of a waveform when measured from the mid-point to the peak of the wave.

### Analog
A signal in the form of a continuously varying quantity such as voltage, frequency or phase.

### Antenna
Device used to concentrate and direct the energy of a signal into a tight beam. Parabolic or dish, grid, and Yagi are different varieties of antennas.

### Antenna Gain
The ratio of the power radiated by an antenna in a specific direction versus the power required to produce this same strength if an isotropic antenna were used.

### Attenuation
The measure of the loss of power in a microwave signal as it travels between two points. It is measured in decibels (dB).

### Attenuator
Attenuators simulate antennas during bench tests.

### Azimuth
This is the direction of antenna pointing relative to true north.

### Band
A portion of the electromagnetic frequency spectrum.

### Bandwidth
The range of frequencies over which a device will transmit information.

### Bit
An abbreviation for binary digits.

### Bit Error Rate

A measure of the number of errors in a digital transmission. Typically given as an exponential number that represents the ratio of errors to total bits. Example: 1E-03 = 0.001 = 1.0 x 10-3 and 1.0E-6 = 0.000001 = 1.0 x 10-3. A single element in a binary code. A measure of the number of errors in a digital transmission. Typically given as an exponential number that represents the ratio of errors to total bits. Example: 1E-03 = 0.001 = 1.0 x 10-3 and 1.0E-6 = 0.000001 = 1.0 x 10-3.

### Bridge

The function of a bridge is to connect separate networks together. This device operates at the DataLink Layer of the OSI model. Bridges connect different network types (such as Fast Ethernet and Ethernet) or networks of the same type. Bridges allow only necessary traffic to pass through the designated segments. When the bridge receives a packet, the bridge determines the destination and source segments. If the segments are the same, the packet is dropped, or filtered. If the segments are different, then the packet is "forwarded" to the correct segment. Additionally, bridges do not forward bad or misaligned packets. Bridges are also called "store-and-forward" devices because they look at the whole Ethernet packet before making filtering or forwarding decisions. Filtering packets, and regenerating forwarded packets enables bridging technology to split a network into separate collision domains.

### SectorPRC interface

This device is a combination of a 9000 router and a bridge in one product.

### Byte

A data unit consisting of eight bits.

### Cable

A transmission medium of copper wire or optical fiber wrapped in a protective cover.

### Channel

A specific band of frequencies designated for a specific purpose; the data path between two nodes.

### Channel Service Unit/Data Service Unit (CSU/DSU)

Manages digital transmission and monitors signals for problems. Performs many functions similar to a modem with the exception of converting digital signals to/from analog since the end device and transmission facility are both digital.

### Channel Spacing

The amount of space signals can flow through.

### Class

Understanding this methodology is difficult, even for customers. Therefore, let's explain this in easier terms. The first octet (or octets) defines the "class" (indicated by the word "net" in this example) of the address, which is the only method to tell the size of the network (how big) and where the internet address belongs. The remaining octets indicate availability for network equipment (i.e., computer or other network equipment). The three main classes are: Class A, Class B, and Class C.

- Class A: Net, Node, Node, Node 255.**0.0.0** (last three octets are available for equipment)
- Class B: Net, Net, Node, Node 255.255.**0.0** (last two octets are available for equipment)
- Class C: Net, Net, Net, Node 255.255.255.**0** (last octet is available for equipment)

### Coaxial Cable

A type of transmission line consisting of a center conductor wire surrounded by insulation that is in turn surrounded by a conductive shield made of metal foil or wire braid. Often used to connect the RF unit and modem unit of a wireless system.

### Code Division Multiple Access (CDMA)

A system in which all users occupy the same bandwidth. Uncorrelated codes are used to allow for higher bandwidth occupancy. This is also known as the spread spectrum system.

### Common Management Information Protocol (CMIP)

A network management protocol that is consistent with an Open Systems Interconnection (OSI) network communication model.

### Company name

This is the name of the company that owns or maintains the radio given to the terminal.

### Console

This device allows you to communicate through the Telnet client to access the configuration software.

### Crimp

Crimp the connector to secure the conductors.

### Customer Premise Equipment (CPE)

Any equipment located at the customer site. Usually in reference to those that are connected to a network.

### Data Communication Equipment (DCE)

A definition of an interface standard that determines how it is connected to another device. For most modems, it resolves issues of interface between Data Terminal Equipment (DTE) and the network.

**Data Terminal Equipment (DTE)**
Hardware that provides for data communications. See also DCE above.

**dBm**
Decibels (dB) relative to 1 milliwatt.

**dBw**
Decibels (dB) relative to 1 watt.

**Decibel (dB)**
The standard unit of measurement for expressing relative signal power. It is dimensionless and is instead referenced to a certain level.

**Diffraction**
The distortion of a wave as it is partially obstructed by an object in its path.

**Digital Signal Processor (DSP)**
A specialized computer chip designed to perform speedy and complex operations on digitized waveforms.

**Direct Sequence (DS)**
A type of spreading technique that multiplies a higher rate PN code to the signal in order to spread the energy of the narrow band signal over a much wider bandwidth for transmission.

**Direct Sequence Speed Spectrum (DSSS)**
DSSS may be seen as the result of two processes. Data is multiplied with a higher rate digital sequence (spreading code). The sequence has many “chips” for every data bit. The resultant signal modulates the RF carrier.

**E1**
European Standard also used in South American nations, among others. Speed is 2.048 Mega bits per second (Mbps). Uses the G.703 data interface.

**Elevation**
1. Height above sea level. 2. The vertical angle in degrees between the ground and the direction the antenna is pointed.

**ESD**
Electro-Static Discharge happens when there is a transfer between objects at diverse voltages.

### Ethernet

This is the most popular physical layer LAN technology in use today. Other LAN types include Token Ring, Fast Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and Local Talk. Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace, create the ability to support virtually all-popular networks and make Ethernet an ideal networking technology for most computer users today. The Institute for Electrical and Electronic Engineers (IEEE) defines the Ethernet as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet, as well as specifying how elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols will communicate efficiently.

### Ethernet Switch

This device helps expand the Ethernet network. LAN switches can link four, six, ten or more networks together, and have two basic architectures. This switch "cuts through" and "stores and forwards" as well. This technique takes more time to examine the entire packet, but it allows the switch to catch certain packet errors and keep them from propagating through the network. A switch also operates between the DataLink and Network Layer of the OSI model. It reads the MAC address and will either bridge it to the Physical Layer or route to the Network Layer.

### Fade Margin

The difference between the receiver signal input level and the receiver sensitivity. Fade margin is usually considered the safety factor allowing the system to remain operating under additional forms of attenuation.

### Fading

The loss of signal strength due to changes in the atmosphere.

### Fault

This section of the browser gives the user a detailed list of alarm activity. Along with the alarm activity, the Event Log also time stamps an alarm, so the user is able to determine when an event occurred, and at what time the event cleared. The date and time fields are derived from the time read by the radio on the network time server.

### Federal Communications Commission (FCC)

Government organization appointed by the U.S. President that regulates interstate communications (by use of licenses, standards, rates, etc.).

### Firmware

Alterable programs in semitransparent storage (e.g., some type of read-only or flash reprogrammable memory).

### Forward Error Correction (FEC)

The ability of a receiving station to correct a transmission error. The transmitter sends redundant information along with the original bits and the receiver uses this information to find and correct errors. This can increase the throughput of a data link operation.

### Framing

Dividing data for transmission into groups of bits, and adding a header and a check sequence to form a frame.

### Frequency

The number of complete cycles per second existing in a waveform. Note that frequency is measured in Hertz (Hz).

### Frequency Hopping (FH)

A type of spreading technique using a PN code to change the signal's frequency between several pre-assigned values (hopping). Although the signal itself looks like a narrow band signal at any given point in time, it acts like a spread signal because of the frequency hopping.

### Fresnel Zone

An imaginary ellipse surrounding the direct transmission path formed by all the points from which a reflected wave would have an increased path length of multiple of the transmitted signal's wavelength. At least 60% of the Fresnel zone must be unobstructed.

### Full Duplex

Independent, simultaneous two-way transmission going in both directions.

### Gain

The increase in signal power caused by a device such as a transmitter or antenna.

### GHz

GigaHertz. Billions of Hertz.

### Ground elevation

This is the approximate mean sea level (AMSL) of the terminal.

### Half Duplex

A one-way directional communication line going in both directions. Only one signal can be transmitted or received at a time

**Hertz (Hz)**
A unit of measurement equal to one cycle per second.

**Hexadecimal (Hex, or H)**
A Base-16 numbering system. This means 16 sequential numbers are used as a base unit (i.e., "0-9" and "A-F").

**Hop**
A term used to describe a single radio path between two points.

**Host**
This term is interchangeable with the definition "node," which means this is a point on the network. The host is also any device on the network that has two-way communication to any point on the network, as well as the Internet.

**Hot-standby**
A condition whereby when the primary method of communication goes down, the secondary method instantly takes over.

**Hub**
This device on a network collects, receives, and repeats data to its forwarded destination on the network. A hub is also known as a switch.

**HyperTerminal**
This provides you details of the internal configuration of the ODU. In the HyperTerminal, you can also change the port settings for the modem connection and adjust the settings to make a call.

**IDU**
Indoor Unit (i.e., Modem Unit).

**IF Cable**
In an SPEEDCOM system, this is the coaxial cables that connects the modem unit to the RF unit. These cables are terminated with male TNC-type connectors at both ends.

**Interface**
The standard signal for connecting a microwave system to the connecting equipment.

**Interference**
Unwanted signals that cause performance degradation or loss of information.

### Intermediate Frequency (IF)

The frequency to which a microwave signal is converted to permit signal processing. This range is typically around 70 to 200 MHz.

### Internet

This is a system of linked networks that are worldwide in scope and facilitates data communicate service such as remote login, file transfer, electronic mail, the World Wide Web and newsgroups. With the meteoric rise of demand for connectivity, the Internet has become the communications highway for millions of users. The Internet was initially restricted to military and academic institutions in its infancy, but now it is a full-fledged information channel for any and all forms of information and commerce. Internet web sites now provide personal, educational, political and economic resources to every cornet of the planet.

### IP Address

This address 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.

### ISM (Industrial, Scientific, and Medical Bands

Ranges are 900 to 928 MHz; 2.4 to 2.4835 GHz; and 5.725 to 5.85 GHz. The FCC for unlicensed use allocated these bands with a restriction on the output power.

### Isotropic

Uniform in all directions.

### Kbps

Thousands of bits per second.

### KHz (KiloHertz)

Thousands of Hertz. Each wireless phone call occupies only a few KiloHertz.

### LAN

This is a local area network that enables computers, network equipment, or other peripherals to communicate on a small network.

### Last mile

Any type of telecommunications technology where data (voice, video, etc.) is traveled within relatively short distances to maintain to highest quality of bandwidth and throughput.

**Latitude**
This is the geographic latitude of the location of the terminal.

**LED**
This is a light-emitting diode, which is a semiconductor, that sends out visible light when an electrical current moves through it.

**Left arrow**
This is the left arrow key on your keyboard.

**Light Emitting Diode (LED)**
An electronic device that emits light with little generation of heat.

**Line Interface Unit (LIU)**
The first unit inside the modem units encountered by signals from the user.

**Line of Sight (radio) (LOS)**
A condition whereby the antennas of a given link have a sufficient path for communication. It requires that at least 60% of the Fresnel zone between them be unobstructed. (Do not confuse with Loss of Signal.)

**Liquid Crystal Display (LCD)**
The display on the Modem Unit used to configure and monitor the system.

**Local Area Network (LAN)**
A short distance data communications network used to link together computers and peripheral devices (such as printers) under some form of standard control.

**Loopback**
This is the process of sending out a test signal to the device on the network so that you know if your signal was successful or unsuccessful.

**Loss of Signal (LOS)**
The signal from the user's device does not appear in the DSX or E1 interface. (This is not to be confused with Line of Sight.)

### MAC address
In a LAN environment each computer contains its own Medium Access Control (MAC) address which is the embedded and unique hardware number. For computers on Ethernet LANs, this is the same number as its Ethernet address. This address is controlled at the DataLink Layer of the OSI model, and is in a hexadecimal format separated by four octets (i.e., 82.39.1E.38).

### Major alarm
Indicates that the alarm may cause service interruption.

### MAN
This is a metropolitan network that enables computers, network equipment, other peripherals, and more than one LAN to communicate within the city or nearby limits.

### Management Information Base (MIB)
A database of network parameters used by SNMP and CMIP to monitor and change network device settings. It provides a logical naming of all information resources on the network pertinent to the network's management.

### Mean Time Between Failure (MTBF)
A measure of the theoretical times a component or device will operate without failing.

### MHz (MegaHertz)
Millions of Hertz.

### Minor alarm
Indicates that the radio is placed in a condition that may affect the 100 Mb throughput, but can be restored (i.e., turning off loopback functions).

### Modulation
The process of varying characteristics of a carrier signal to represent changes in the transmitted information.

### MOdulator-DEModulator (MODEM)
A device that converts a digital signal to analog, or vice versa, and is used to transfer data between computers over communications lines.

### Msps
Million of samples per second.

### Multi-path fading
The condition in which the "true" signal from an antenna reflects off an object (usually the ground) and, as a result, the reflected signal causes destructive interference at the receiving antenna. Multi-path fading affects linearly polarized signals more than circularly polarized signals.

### Network
A set of connections that allow them to exchange data with each other, which enables multiple users to share to communicate data through the accepted path(s).

### Network
Two or more locations tied together with equipment and communications channels.

### Node
This is a point on the network such as a computer, server, peripheral (printer, scanner, etc).

### Noise
Any unwanted signal or disturbance that degrades the quality of a transmitted signal.

### Obstruction
Any man-made or natural object that blocks, diffracts, or reflects a transmitted signal.

### Octet
There are four octets in an IP address. Each octet contains 8 bits, which are equivalent to 1 byte. Each octet is separated by a period (.).

### OD
Outside diameter of pipe for mounting an antenna.

### Outdoor Unit
The Outdoor Unit (ODU) provides the baseband and RF signal processing required to convert the 100Base-T signal from the CPI to an RF frequency at 23, 26, 29, or 38 GHz. The ODU mounts to an antenna through an integral "Quick-Fit" connection that does not require any external waveguide. The ODU housing is ruggedized to protect the RF and modem electronics contained inside. It is capable of simultaneously transmitting and receiving 100 Mbps of data traffic over the air.

### Packet
A unit of data transmitted between a receiver and a sender. Each packet contains embedded information, as well as place to go on the network (known from the IP address).

### Part 15 (of FCC rules)
The section of the FCC Code of Federal Regulations defines the restrictions regarding the use of Spread Spectrum systems.

### Passive Repeater
A re-radiation device associated with a transmitting/receiving antenna system that re-directs intercepted radio frequency energy without boosting or processing the signal.

### Path Length
The distance between two ends of a wireless system.

### Path Loss
The decrease in signal power experienced when a signal is transmitted between two points.

### Path Profile
A drawing of the terrain (including buildings, trees, hills, lakes, etc.) along a transmission path to determine if a given path is viable for the communication link. This is usually done with a computer.

### Personal Communication Services (PCS)
A lower powered, higher frequency competitive technology to cellular.

### Polarization
The direction of the amplitude of a radio wave. Polarization is usually horizontal or vertical.

### Pole Height
This is the height of the antenna supporting structure.

### Power Output
The power produced by a transmitter. This is measured in decibels per meter (dBm).

### Processing Gain
The ability of the spread spectrum decoder to recover the received signal out of noise. It is essentially the increase in ability to recover the signal in the presence of an interfering carrier of the same or greater level.

### Propagation
The transmission of a wave along a given path through a medium.

### Protocol

A network protocol is the standard that allows computers to communicate with each other. A protocol defines how computers identify one another on the network, the form that the data should take in transit, and how this information is processed once it reaches its final destination. Protocols also define procedures for handling lost or damaged transmissions or "packets." IPX (for Novell Netware), TCP/IP (for UNIX, Windows NT, Windows 95 and 98 and other platforms), DECnet (for networking Digital Equipment Corp. computers), AppleTalk (for main Macintosh computers), and NetBIOS/NetBEUI (for LAN and Windows NT networks) are some of today's most popular networks. Although each network protocol is different, they all share the same physical cabling. This common method of accessing the physical network allows multiple protocols to peacefully coexist over the network media, and allows the builder of the network to use common hardware for a variety of protocols. This concept is known as "protocol independence," which means that devices that are compatible at the physical and data link layers allowing the user to run many different protocols over the same medium.

### Pseudo-random Noise code (PN code)

A high rate digital code that mimics random noise-like properties. It is multiplied with a lower rate data signal in order to achieve spread spectrum transmission signals. The receiver then multiplies the same code back into the transmission to recover the data signal.

### Public Switched Telephone Network (PSTN)

This refers to a worldwide voice telephone network accessible to all those with telephones and access privileges.

### Quadrature Amplitude Modulation (QAM)

A method for modulating a signal by which more than one bit can be sent simultaneously.

### Quadrature Phase Shift Keying (QPSK)

Phase-shift keying in which there are four phase states or positions in the time or frequency domains within a single period.

### Radiation

The flow of electromagnetic energy from a transmitter.

### Radiation Pattern

An illustration of the energy level radiated by an antenna in every direction.

### Radio address

This is the physical location (street name) of the terminal. This is also displayed at the bottom of the web page.

### Radio Frequency (RF)

The frequency at which microwave systems transmit.

### Received Signal Strength Indicator (RSSI)

The RSSI Voltage provided at the output of the RF Unit that is used to indicate the RF Input Level.

### Reflection

The sharp change in direction of a wave after hitting an obstruction in its path.

### Refraction

The bending of a wave as it moves from one medium to another.

### Reliability

A measure of the percentage of time the system is operating. Reliability is usually a measure of both the availability of the signal and the MTBF of the equipment.

### Responsible personnel

This is the person(s) responsible for maintaining the radio system.

### RF Signal Level

The strength of the power received by the RF Unit from the antenna.

### Right arrow

This is the right arrow key on your keyboard.

### 9000 router

This device filters out network traffic by specific protocol rather than by packet address. This device operates at the Network layer of the OSI model. 9000 routers also divide networks logically instead of physically. An IP 9000 router can divide a network into various subnets so that only traffic designated for particular IP addresses can pass between segments. Network speed often decreases due to this type of intelligent forwarding. Such filtering takes more time than exercised in a switch or bridge, which only looks at the Ethernet address. In more complex networks, overall efficiency is improved by using 9000 routers.

### Rx (Receiver)

This is where the packet is going.

### Server

A computer that is responsible for tracking, as well as receiving and sending requests from other computers connected to it (on the same network).

### Sidelobe

These are 20 dB lower than the main lobe, and it is critical from a performance standpoint that antennas are aligned with respect to the main lobe. Failure to do so may cause the radio to be interfered with or the radio may interfere with other systems.

### Signal level

This is the value of the signal level at the receiving end of the transmission path.

### Simple Network Management Protocol (SNMP)

The standard protocol for TCP/IP network management that has the most common worldwide use.

### Site ID (Unique)

This is the alphanumeric site address given to the terminal by you (the user).

### Spread Spectrum Technology (SST)

A method of encoding (with a PN code) a digital signal in a transmitter so as to spread it over a wide range of frequencies so that the average signal power is close to the noise floor. The same code is known to the receiver and is used to decode the signal. Keeping the code secret provides communications security.

### Submask

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.

### 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.

### Symbol Threshold

After a signal has been acquired, the acquisition algorithm in the spread-spectrum chip continues to run a cross-correlation between the expected PN sequence and the received signal, but now uses the Symbol Threshold for comparison. If the result of the cross-correlation drops below the Symbol Threshold, the signal is considered to have been lost, and the algorithm begins trying to acquire the signal again.

### System Gain

The sum of the transmitter power output and the receiver sensitivity. System gain is an important measure of a system's ability to overcome attenuation and perform to a satisfactory level. These are measured in decibels per meter (dBm).

### Tx (Transceiver)

This is where the packet is coming from.

### WAN

A wide-area metropolitan network is a connection between LANs, which may be privately owned or rented.

Notes:

# 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 router. This License does not extend to any copyrights to the program nor does it license use of the program on more than one 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.

The Customer or Reseller is granted a non-exclusive License to use the licensed program on a single 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.

## Software License Agreement

The installation and use of this SOFTWARE indicates your understanding and acceptance of the following terms and conditions. This license shall supersede any verbal or prior written, statement or agreement to the contrary. If you do not understand or accept these terms, or your local regulations prohibit “after sale” license agreements or limited disclaimers, you must cease and desist using this product immediately.

The following terms govern your use of the enclosed Software:

### License Grant

Wave Wireless Networking (hereafter referred to as Wave) grants you a license to Use one copy of the Software on one single-user PC, notebook, or laptop computer. It may not be installed on multiple devices and may not be shared by more than one individual while in use on a single device. “Use” means storing, loading, installing, executing or displaying the Software. You may not modify the Software or disable any licensing or control features of the Software. Uses of this software other than those expressly defined herein are forbidden. Wave does not provide support for, nor will it accept return of, this Software if it is used in any manner other than those outlined here.

### Ownership

The Software is owned and copyrighted by Wave or its third party suppliers. Your license confers no title or ownership in the Software and is not a sale of any rights, other than the limited right of Use defined above, in the Software. Wave and Wave’s third party suppliers may protect their rights in the event of any violation of these License Terms.

### Copies and Adaptations

You may only make copies or adaptations of the Software for archival purposes or when copying or adaptation is an essential step in the authorized Use of the Software. You must reproduce all copyright notices in the original Software on all copies or adaptations. You may not copy the Software onto any bulletin board or similar system.

### No Disassembly or Decryption

You may not disassemble or decompile the Software unless Wave's express prior written consent is obtained except in those jurisdictions where Wave's consent is not required for disassembly or decompilation. Upon request, you will provide Wave with reasonably detailed information regarding any disassembly or decompilation. You may not decrypt the Software for any reason.

### Transfer

Your license will automatically terminate upon any transfer of the Software or equipment containing the Software. Upon transfer, you must deliver the Software, including any copies and related documentation, to the transferee. The transferee must accept these License Terms as a condition to the transfer.

### Termination

Wave may terminate your license upon notice for failure to comply with any of these License Terms. Upon termination, you must immediately destroy the Software, together with all copies, adaptations and merged portions in any form.

### Export Requirements

You may not export or re-export the Software or any copy or adaptation in violation of any applicable laws or regulations.

### U.S. Government Restricted Rights

The Software and documentation have been developed entirely at private expense and are provided as "Commercial Computer Software" or "restricted computer software". They are delivered and licensed as "commercial computer software" as defined in DFARS 252.227-7013 (Oct 1988), DFARS 252.211-7015 (May 1991) or DFARS 252.227-7014 (Jun 1995), as a "commercial item" as defined in FAR 2.101 (a), or as "Restricted computer software" as defined in FAR 52.227-19 (Jun 1987) (or any equivalent agency regulation or contract clause), whichever is applicable. You have only those rights provided for such Software and Documentation by the applicable FAR or DFARS clause or the Wave standard software agreement for the product.

## WAVE WIRELESS NETWORKING LIMITED WARRANTY STATEMENT

1.Wave warrants to you, the end-user customer, that Wave hardware, accessories and supplies, will be free from material defects in materials and workmanship after the date of purchase, for the period specified above. If Wave receives notice of such defects during the warranty period, Wave will, at its option, either repair or replace products which prove to be defective.

2. **Wave warrants to you that Wave software will not fail to execute its programming instructions after the date of purchase, for the period specified above, due to defects in material and workmanship when properly installed and used.** If Wave receives notice of such defects during the warranty period, Wave will replace software media which does not execute its programming instructions due to such defects.

3. Wave does not warrant that the operation of Wave products will be uninterrupted or error free. Wave products may contain remanufactured parts equivalent to new in performance or may have been subject to incidental use. If Wave is unable, within a reasonable time, to repair or replace any product to a condition as warranted, you will be entitled to a refund of the purchase price upon prompt return of the product.

4. The limited Warranty does not apply to defects resulting from (a) improper or inadequate maintenance or calibration, (b) software, interfacing, parts or supplies not supplied by Wave, (c) unauthorized specifications for the product, or (d) improper site preparation or maintenance.

5. ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE IS LIMITED TO THE DURATION OF THE EXPRESS WARRANTY SET FORTH ABOVE. Some states or provinces do not allow limitations on the duration of an implied warranty, so the above limitation or exclusion might not apply to you. This warranty gives you specific legal rights and you might also have other rights that vary from state to state, or province to province.

6. THE REMEDIES IN THIS WARRANTY STATEMENT ARE YOUR SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED ABOVE, IN NO EVENT WILL Wave BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (INCLUDING LOST PROFIT), OR OTHER DAMAGE, WHETHER BASED IN CONTRACT, TORT, OR OTHERWISE. Some states or provinces do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

## 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.

### 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 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.

# Appendix - Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Wave Wireless 9000 series.

This appendix contain the following sections:

- Manufacturers Federal Communication Commission Declaration of Conformity Statement
- Department of Communications -- Canada
- Declaration of Conformity for RF Exposure

# Manufacturers Federal Communication Commission Declaration of Conformity Statement

Models: SL910x
FCC Certification number: NCBSL9101, NCBSL9102
Manufacturer: Wave Wireless Networking
7020 Professional Parkway East
Sarasota, FL 34240

This device complies with Part 15 rules. Operation is subject to the following two conditions:

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

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

Reorient or relocate the receiving antenna.

Increase separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from which the receiver is connected.

Consult the professional installer or an experienced radio/TV technician.

**Note:** The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

Caution

The part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using the antennas: 24 dBi grid antenna and 8 dBi omni antenna.

# Department of Communications -- Canada

## Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada. This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and

2. This device must accept any interference received, including interference that may cause undesired operation.

The device is certified to the requirements of RSS-139-1 and RSS-210 for 2.4-GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

# Declaration of Conformity for RF Exposure

The radio module has been evaluated under FCC Bulletin OET65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. For the 24-dBi antenna, the equipment should be positioned more than 2 m from your body or nearby persons. For the 8-dBi antenna, the equipment should be installed more than 20 cm from your body or nearby persons.