SPEEDLAN 9000 Series

Installation and Operation User Guide Version 3.03

Last Revised: July 3, 2003

A SPEEDCOM WIRELESS CORPORATION

Copyright/Liability

Copyright ©2002, 2003. Wave Wireless Networking. All rights reserved. SPEEDCOM, SPEEDSignal and SPEEDView are registered trademarks of Wave Wireless Networking. SPEEDLAN, 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 1-3
IP Router Functionality 1-3
Network Management 1-3
Features (and Benefits) 1-4
Equipment Features 1-5
SPEEDLAN Polling Protocol -- How it Works 1- 6
Point-to-Point Functionality 1-6
Point-to-Multipoint Functionality 1-6
SPEEDLAN 9000 Mesh Protocol -- How It Works in Mesh Clouds 1-8
SPEEDLAN's Mesh Cloud Architecture 1-10
SPEEDLAN 9000 Mesh Core Components 1-10
Network Expansion: Connecting Buildings in a SPEEDLAN 9000 Network 1-12
What's New for Version 3.03 1-14
What's New for Version 3.0 1-15
Contacting Technical Support 1-18

Chapter 2 SPEEDLAN 9101, 9102, 9103 & 9104 Hardware 2-1
Rooftop and Tower Installations Warning 2-2
General Safety Requirements for Installation of SPEEDLAN 9000 Models 2-2
Hardware Overview 2-3
Drawings of Outdoor, Remote-Mounted Components 2-4
Indoor Junction Box 2-4
The SPEEDLAN 9101(with an Integrated 8 dBi Omni) 2-5
SPEEDLAN 9104 (with 5 dBi Omni) 2-6
Bottom View of SPEEDLAN 9101/9104 2-7
System Description 2-7
Package Contents 2-7
Installation Steps for the SPEEDLAN 9101/9104 2-8
Installation Diagram of the SPEEDLAN 9101/9104 2-10
The SPEEDLAN 9102 and 9103 (CPE and Base Station Use) 2-12
As a 9102 CPE/Point-to-Point with Grid or Directional Antenna 2-12
As a Base Station with Sectoral Antenna 2-13
As a Base Station with High-Gain Omni Antenna 2-14
Bottom View of SPEEDLAN 9102 and 9103 2-15
System Description 2-15
Package Contents 2-15
Installation Steps for the SPEEDLAN 9102 and 9103 2-16
9102/9103 Installation Diagram 2-22

Chapter 3 - General Functions of the Configurator 3-1
Manual Initial Configuration of the SPEEDLAN 9000 3-2
Prerequisites 3-2
Connecting a SPEEDLAN 9000 and a Client PC 3-3
Configuring the SPEEDLAN 9000 3-5

Wireless Interface IP Address Assignment 3-6
Automating the Configuration of Multiple SPEEDLAN 9000s 3-6
Completing Configuration 3-6
Adding Additional SPEEDLAN 9000s to the Wired Network 3-6
Overview of the SPEEDLAN 9000 Configurator General Main Menu 3-7
Logging on the SPEEDLAN 9000 Configurator 3-10
Classes of Users (and Passwords) 3-10
Logging On 3-11
Logging Off 3-13
Understanding the Security Alert Screens 3-13
After Logging On 3-17
Helpful Information to Know... 3-18
How do you select the router? 3-18
References on Setting Up the Router 3-18
Caching - viewing the most recent version of a page 3-18
Session Activity 3-19
9000 Firmware Updates, SPEEDView or Other Utility Programs 3-20
If You Need a Temporary IP Address 3-20
The Configuration Menu 3-20
Network Menu 3-20
Network Interfaces 3-20
IP Address Configuration 3-20
Virtual Addresses 3-24
System Menu 3-25
Configuration Summary 3-25
Version 3-28
Host Name 3-29
Password 3-30
Reboot 3-31
Routing Menu 3-31
Def Gateway 3-32
RIP2 Setup 3-33
RIP Settings 3-34
Route Table 3-36
Static Route 3-37
DHCP Server Menu 3-39
How DHCP Assigns an IP Address 3-39
Basic Instructions for Setting Up DHCP on an Interface 3-40
Elements Defined on the General and Known Client Pages 3-44
Viewing Log Messages 3-47
Status 3-47
DHCP Relay Menu 3-47
Forwarding Menu 3-48
Services 3-49
Three Features of NAT 3-54
Address Sharing 3-56
Internal Servers 3-58
1:1 NAT 3-60

Firewall 3-61
IP Sessions 3-66
Diagnostics Menu (Troubleshooting the Network) 3-67
Interface Statistics 3-68
ARP Table 3-70
ICMP Statistics 3-71
Admin Menu 3-73
User Configuration 3-74
Permissions 3-74
Software Update 3-76
Support 3-77
Current Sessions 3-79

Chapter 4 - Using the Configurator to Set Up Special Parameters for a Base Station 4-1
Network Menu 4-2
Interfaces for Base Mode 4-2
Wireless menu 4-10
Channel and Rates 4-10
Max Tx Retries and Signaling Rate Fallback 4-12
Max Throughput (Regulating Bandwidth) 4-14
Admin Menu 4-15
Remote Control 4-15
Software Update 4-16
Updating the Software on a Base Station and CPE 4-17

Chapter 5 - Using the Configurator to Set Up Special Parameters for CPE Routers 5-1
Network Menu 5-2
Interfaces for CPE Mode 5-2
Base Station Information 5-3
Authentication 5-4
Wireless menu 5-5
Channel and Rates 5-6
Max Tx Retries and Signaling Rate Fallback 5-8
Max Throughput (Regulating Bandwidth) 5-10
Admin Menu 5-11
Software Update 5-11

Chapter 6 - Using the Configurator to Set Up Special Parameters for Point-to-Point Routers 6-1
Network Menu 6-2
Interfaces for Point-to-Point Mode 6-2
Point-to-Point Settings 6-3
Primary Station Information 6-6
Authenticating a Point-to-Point Secondary Router Only 6-6

Wireless menu 6-7
Configuration for Point-to-Point 6-7
Channel and Rates 6-8
Max Tx Retries and Signaling Rate Fallback 6-10
Max Throughput (Regulating Bandwidth) 6-12
Admin Menu 6-13
Remote Control for Point-to-Point Primary Routers 6-13
Software Update for Point-to-Point Primary or Secondary Routers 6-13
Updating the Software on a Local Router and Remote Router: Primary Mode Only 6-15

Chapter 7 - Using the Configurator to Set Up Special Parameters for Mesh Routers 7-1

Network Menu 7-2
Interfaces for Mesh Mode 7-2
Mesh Nodes 7-3
Security 7-3
Wireless menu 7-5
Configuration 7-5
Channel and Rates 7-6
Max Tx Retries and Signaling Rate Fallback 7-8
Max Tx Retries 7-8
Signaling Rate Fallback 7-9
Max Throughput (Regulating Bandwidth) 7-10
Receive (Rx) Threshold Parameter 7-11
Blocked Links 7-12
Admin Menu 7-13
Remote Control 7-13
Software Update 7-14
Updating the Software on a Local Router and Remote Router 7-15

Chapter 8 - Using SPEEDView 8-1

What is SPEEDView? 8-2
System Requirements 8-2
Installation Instructions 8-2
Starting SPEEDView 8-3
Star Network 8-6
Mesh Network 8-7
The Program Instructions 8-8
The Main Tab 8-8
The Main Tab Icons 8-9
The Node, Link, View and Stats Menus (on the Main tab) 8-11
Buttons (on the Main tab) 8-12
Performing a Bandwidth Test 8-14
Performing a Ping Test 8-15
Accessing the Statistics Tabs on Bottom of Main Tab 8-16
Options Tab 8-22

Chapter 9 - Basics of IP Addressing 9-1

Basics of IP Addressing 9-2
What is an IP address? 9-2
Internet Address Classes 9-2
Subnetting a Network 9-5
How does a network administrator assign an IP address? 9-7
What is DHCP? 9-8
What is NAT? 9-9
NAPT 9-10
Diagram of Outgoing NAT 9-11
Diagram of Incoming NAT 9-12
Basics of Routing 9-13

Glossary for Standard Data Communications ..... Glossary - 1

Glossary for Standard Data Communications 2

Appendices

Changing the Router's Topology Mode ..... Appendix A-2
What is IP Recovery? ..... Appendix A-2
Installing the IP Recovery Program ..... Appendix B-2
System Requirements ..... Appendix B-2
Installation Instructions ..... Appendix B-2
Starting IP Recovery ..... Appendix B-3
Setting a Temporary IP Address ..... Appendix B-5
Transmit Power Test ..... Appendix B-6
SPEEDLAN 9000 Configurator and SPEEDSignal Passwords ..... Appendix C-2
SPEEDView Passwords ..... Appendix C-3
IP Recovery Password ..... Appendix C-4
Rooftop and Tower Installations Warning ..... Appendix D-2
General Safety Requirements for Installation of SPEEDLAN 9000 Models ..... Appendix D-2
Manufacturer Information ..... Appendix D-3
Regulatory Information ..... Appendix D-3
Declaration of Conformity for RF Exposure ..... Appendix D-4
Manufacturers Canadian (IC) Declaration of Conformity Statement ..... Appendix D-4
European Telecommunications Standards Institute (CE) Statement of Compliance ..... Appendix D-5
Radio Approvals ..... Appendix D-6
9000 Series Technical Specifications ..... Appendix E-2
9000 Series Product Model Information ..... Appendix E-4

What is SPEEDSignal? ..... Appendix F-2
How This Document is Structured ..... Appendix F-2
How to Install SPEEDSignal on a Desktop PC ..... Appendix F-2
How to Install SPEEDSignal on a Pocket PC PDA ..... Appendix F-4
Enabling/Disabling SPEEDSignal (for Pocket PC PDAs) ..... Appendix F-7
Opening SPEEDSignal on the Desktop PC ..... Appendix F-8
Opening SPEEDSignal on the Pocket PC PDA ..... Appendix F-9
SPEEDSignal's Scanned Results ..... Appendix F-10
Adjusting SPEEDSignal Settings ..... Appendix F-11
How To Exit SPEEDSignal on the Pocket PC PDA ..... Appendix F-13
Troubleshooting ..... Appendix F-14

Chapter 1
Introduction

Note: All cross references in the Adobe PDF contain hyperlinks.

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 mesh, star and building-to-building topologies, they provide the network manager powerful tools to build complex networks. This allows wireless broadband networks and services to be extended on a greater scale, and to connect more buildings than ever before. The 9000 series are all remote-mounted 11 Mb/s routers. These routers are installed on the building's rooftop to help reduce signal loss.

In a mesh topology, the SPEEDLAN 9000 routes traffic around physical limitations, eliminating the line-of-sight (LOS) issue present in star topology-only networks. Each mesh router will communicate with other mesh routers in a radius of up to 2 miles depending upon the model and signaling rate selected. This creates a multi-hop IP routed cloud: self-healing, load balancing, and scalable 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.

In a star topology, the 9000 router can act as a polling central base station or as a remote Customer Premise Equipment (CPE), which is polled by a base station. This process helps overcome problems inherent to 802.11-based products with hidden transmitters, conserve wireless bandwidth and reduce equipment costs as well.

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: point-to-point, point-to-multipoint, and self-healing mesh. For information on the type of routers included in the SPEEDLAN 9000 series, see *Equipment Features, page 1-5*. For more information on point-to-point and point-to-multipoint networks, see *SPEEDLAN Polling Protocol -- How it Works, page 1-6*. For more information about mesh, see *SPEEDLAN 9000 Mesh Protocol -- How It Works in Mesh Clouds, page 1-8*.

ISP Functionality

The SPEEDLAN 9000 products are tailored to fit the needs of Internet Service Providers and Broadband Telecommunications Providers. Two features particularly useful to Internet Service providers are Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP). NAT helps to ensure network security and allows an entire company to share a single global IP address for communication on the Internet. This enables companies to communicate with other devices on the Internet. DHCP servers provide efficient use of IP addresses by assigning them dynamically or statically to the wireless router location. DHCP allows network administrators to dynamically assign IP addresses for the period of time needed to connect to the Internet or network. By providing a DHCP server within the CPE and the base station, the SPEEDLAN 9000 series allows the DHCP transactions to be handled locally at the remote building. This reduces the load on the entire wireless network.

IP Router Functionality

The SPEEDLAN 9000 is a highly configurable wireless IP router which supports both star and mesh topologies. In addition to being configurable via a standard web browser, the router also includes an "at a glance" network monitoring/analysis tool to allow constant feedback of the network as a whole.

Network Management

- SPEEDView® is a flexible Windows-based management tool that allows you to quickly isolate and resolve network problems. SPEEDView gives you an "at-a-glance" view of your network, presenting you all of the nodes on the network. Network managers can monitor local and remote SPEEDLAN 9000 nodes from a central location, or from any location on the network. SPEEDView also allows you to troubleshoot network bugs and non-existent physical connections. You can also perform bandwidth and diagnostic tests.
- The SPEEDLAN® 9000 Configurator is a web-based management tool that allows a network manager to configure routers.

Other Helpful Tools

- SPEEDSignal™ allows you to communicate with SPEEDLAN 9000 routers via their wireless or wired interface. Since the wireless version runs on a Pocket PC Personal Digital Assistant, installers can easily troubleshoot antenna alignment problems in the field.

- If you changed the IP address on the router and forgot it, you can find the configured IP address of the Ethernet interface using the IP Recovery application.

Features (and Benefits)

- 11Mb/s radio (High performance and low cost)
- 2.4 GHz License-free ISM band (No lengthy licensing delays)
- Mesh and Star topologies (Maximum network flexibility)
- NAT & DHCP server/client (Secure and efficient network)
- SPEEDView (Troubleshoot network problems)
- Web-based configuration
- SPEEDView, a flexible Windows-based network management tool, gives you an "at-a-glance" view of all nodes on a network
- Multihop, Self-healing (Increased network stability and performance)
- Polling base station (Robust performance)
- AES 128-bit encryption (Trusted data security)
- SPEEDSignal (Antenna alignment)
- IP Recovery (Creating a temporary IP address)

Note: Advanced Encryption Standard was adopted by the National Institute of Standards and Technology in October of 2000. AES presents a new level in computer networking security, especially important in wireless communications because wireless circuits are easier to tap than their hard-wired counterparts. AES is more difficult to crack than its predecessor Data Encryption Standard. SPEEDLAN 9000 products use an AES 128-bit encryption key. **Encryption Note! A Web browser must support 128 bit encryption in order to be used with SPEEDLAN 9000 Configurator.** For more information about AES, visit http://www.nist.gov.

Equipment Features

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

- **SPEEDLAN 9101 (for business or residential):** A router used in a non-line-of-sight pico cell (using the Mesh protocol). This router contains an integrated 8 dBi, omni antenna which is directly attached on the top. You do not need an additional external antenna. In addition, the parameters are configured with the Mesh protocol in the SPEEDLAN 9000 Configurator. This router uses an integrated 8 dBi omni-directional antenna. 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 Mesh Clouds, page 1-8*.
- **SPEEDLAN 9102:** This model can be configured as Customer Premise Equipment (CPE) at one end of the point-to-point or point-to-multipoint link. It could also be configured as a mesh router in a mesh cloud (via an external omni). (This router is also referred to as a "Flexnode" because it is a star (CPE) and mesh topology solution.)

- **SPEEDLAN 9103:** This model is pre-configured as a base station but can be reconfigured to function as a CPE router or as one end of a point-to-point or point-to-multipoint link. The 9103 can also be configured as a mesh node via an external omni.

- **SPEEDLAN 9104 (for residental applications only):** The 9104 contains all of the following features of the 9101 except RIP routing. The 9104 uses an integrated 5 dBi omni and is intended for residential applications. This router also supports one device on the local interface as well.

The SPEEDLAN 9000 series is housed in a waterproof, cast enclosure that mounts outside the building, on a mast, or tower. The 9000 series allows up to 300’ of specialized, outdoor Ethernet cable to be used between the LAN and the RF device, without loss of any radio signal. This increases the effective wireless link distance and reduces or even eliminates the need for an amplifier.

SPEEDLAN Polling Protocol -- How it Works

K^2 is the name of the Wave Wireless' polling protocol. It enables communication between a base station and a CPE router. A base station continuously polls CPE routers and tells them where and when to send data. CPE routers only transmit when polled by the base station, maximizing available bandwidth and preventing "hidden node" problems common with 802.11b based products.

Enterprise customers may use the SPEEDLAN 9000 star products to provide point-to-point and point-to-multipoint connectivity between buildings that are within line-of-sight (LOS).

Point-to-Point Functionality

Figure 1-1: SPEEDView illustrating a point-to-point network

The point-to-point network is the simplest form of the fixed wireless network: a single link between two wireless routers having line-of-sight (as shown in Figure 1-1 on page 1-6). A fixed wireless building-to-building connection is a common alternative to leased lines and trenching cable or fiber. Point-to-point links work well for dedicated connections but limit network expansion. If any of the routers are unable to see each other, a base station must be used to repeat traffic to the next router in line.

For a simple point-to-point link, use two 9102 routers.

Point-to-Multipoint Functionality

A point-to-multipoint network consists of a group of routers (Customer Premise Equipment, hereon abbreviated as CPE) and a base station. The network is based on a star topology (as shown in Figure 1-2 on page 1-7), thus CPE routers must have clear LOS to a base station. A base station acts as the "traffic cop" within the network, making use of the K^2 polling protocol in order to control the flow of data between buildings.

The amount of traffic a 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.

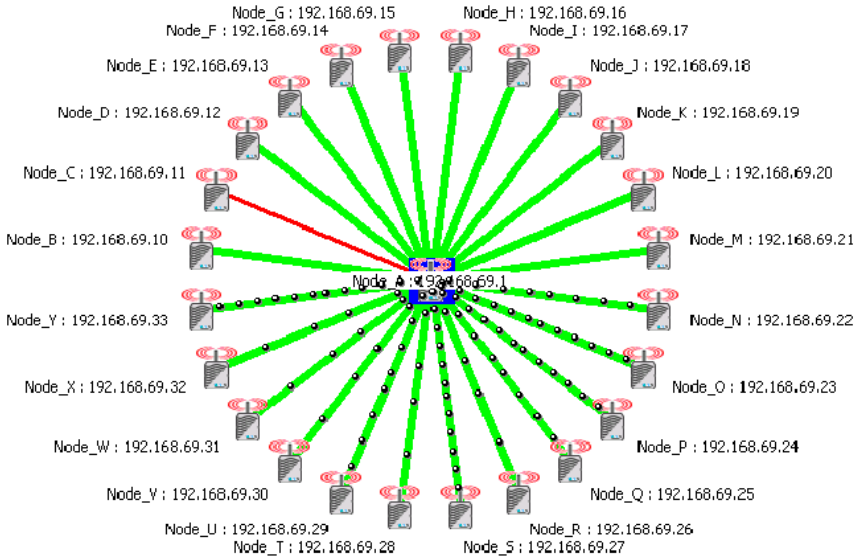


Figure 1-2: SPEEDView illustrating a point-to-multipoint network

Using SPEEDView, Figure 1-2 on page 1-7, illustrates a point-to-multipoint network. A base station (indicated by blue square in the middle) polls each CPE and controls when and which CPE can transmit.

SPEEDLAN 9000 Mesh Protocol -- How It Works in Mesh Clouds

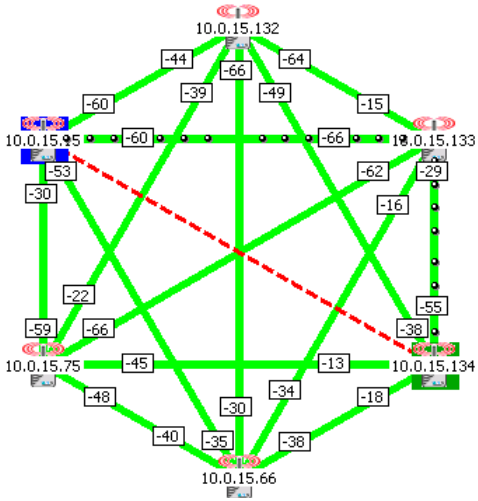


Figure 1-3: SPEEDView illustrating a mesh network

SPEEDLAN 9000 routers provide the unique ability to "self-heal" the wireless network as the topography changes over time, thereby increasing the overall stability and performance of the network while allowing traffic to reach buildings blocked by obstructions of line-of-sight.

What is happening in Figure 1-3 on page 1-8?

- You will notice negative numbers next to the routers, or referred to as nodes on the network diagram. These numbers represent the receive signal strength (expressed as dBm) for the links in the network diagram.
- The black dots in a mesh network diagram indicate a trace route, which maps out the current data flow between the selected pair of nodes. A user would select the trace feature to view the data flow between a node pair (for mesh networks only).

- This illustration also shows that every router in the mesh cloud can be heard by every other router in the cloud, except for the link represented with a red, dashed line indicating that there is no signal between those two nodes. SPEEDView allows you to block traffic over any link in the cloud. This is done using the "Block" feature. The broken (or disconnected) link will appear as a red, dashed line. This link also appears when there is no signal between two nodes.
- SPEEDView can also be used to perform bandwidth, link and ping tests.

Routing Around Obstacles

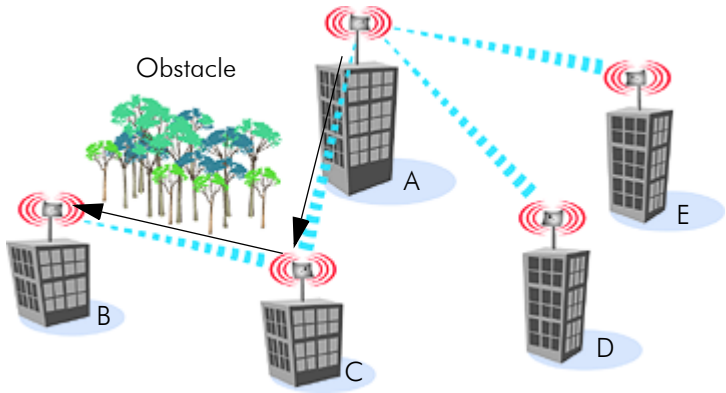


Figure 1-4: Routing around obstacles

Explaining this scenario on the simplest level (using the Mesh protocol as shown in Figure 1-4 on page 1-9). A can route a packet to B, despite the tree obstruction (block of trees) within the path. How does this procedure work?

1. A has line-of-sight to C but not to B.
2. C has line-of-sight to A and 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 router (in this case C, and B and detect a clear path to C). Therefore, the packet is successfully 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 Mesh Cloud Architecture

Separate multi-user and residential models (SPEEDLAN 9101 for business and residential use, as well as the SPEEDLAN 9104 for residential use) are specifically designed to meet the connectivity demands for everyone from single users to large corporations. These models will communicate with every other mesh router within an unobstructed 1/4 mile radius to a 1/2 mile radius.

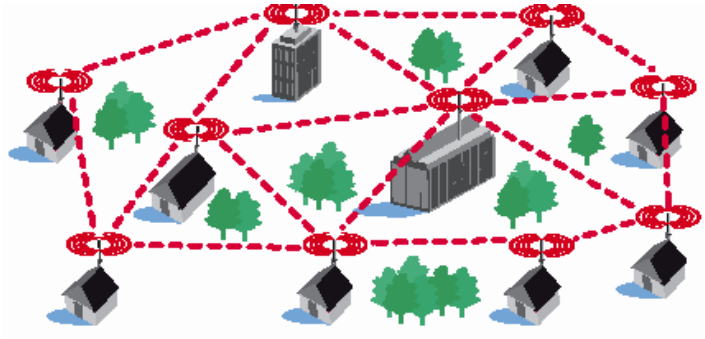


Figure 1-5: An example of a mesh network

SPEEDLAN 9000 Mesh Core Components

SPEEDLAN 9000 Mesh protocol includes three central components which are neighbor discovery, topology updates, and routing.

Neighbor Discovery

Neighbor discovery occurs when each router sends a broadcast "hello" message to detect those routers to which it has line-of-sight. The "hello" sender acknowledges those replies, whereupon the sender and the neighboring router add each other to their respective active neighbor lists. Neighbor discovery protocol messages are sent by each router on startup and periodically thereafter. The periodic messages are required to determine when a former neighbor can no longer be reached, whereupon it is removed from the active neighbor list. Neighbor discovery messages are relatively short and are sent infrequently enough that they don't constitute significant overhead.

Topology Updates

When a router adds or deletes a neighbor to or from its active neighbor list, it propagates that information to the rest of the routers in the wireless mesh LAN. Unlike classic wired routing protocols, topology update notifications are not flooded. Instead they are sent via a spanning tree, such that each router receives only one notification of a particular event. (A brief explanation of the spanning tree algorithm is explained in the note below.) This approach also conserves bandwidth for use in forwarding user traffic. Since each router knows the topology of the entire wireless LAN, it can determine the shortest path to each peer router in the wireless LAN.

Note: In short, the spanning tree algorithm enables units to dynamically locate a subset of the topology that is loop-free. The spanning tree algorithm determines the best path a unit can use to send a message.

Routing

Routing is simply the act of forwarding a received Internet Protocol (IP) datagram (a block of data) toward its destination. The router compares the destination IP address to entries in its routing table. If the destination is a wireless neighbor or a node connected to the router's wired LAN, the router sends the datagram directly to the destination. Otherwise, it sends the datagram to another router, which must be on the wired LAN or be a wireless neighbor.

In wired broadcast LANs, all routers on the LAN can hear each other. Therefore, a datagram only passes through a router when it is moving from one LAN to another LAN along the path to its destination. In a mesh wireless LAN, not all routers can hear each other. Therefore, a router within a wireless LAN may forward a datagram to a neighbor router within the same wireless LAN, in order to send the datagram toward its destination. For each datagram, the routing algorithm minimizes the number of router-to-router hops within the wireless LAN, thereby also conserving bandwidth for other user traffic.

Why SPEEDLAN Outperforms Other Routing Equipment

The SPEEDLAN 9000 outperforms other 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 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 routers.

Network Expansion: Connecting Buildings in a SPEEDLAN 9000 Network

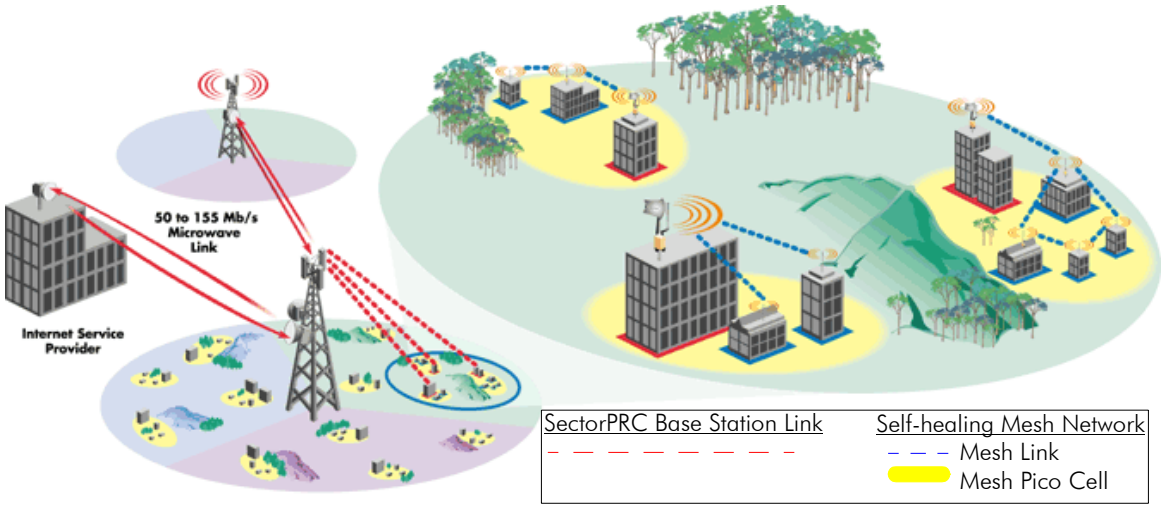


Figure 1-6: Expanding the network

Using a mix of wireless technologies, SPEEDLAN makes it possible to design a Wireless Metropolitan Area Network (WMAN) capable of delivering high-speed Internet services to a variety of buildings. In Figure 1-6 on page 1-12, the ISP has installed three polling base stations, two high-speed microwave links, and several SPEEDLAN 9000 routers.

Broadband Backbone Links

The two-high speed microwave links (50 to 155 Mb/s) provide full-duplex broadband backbone links to other areas of the MAN. These microwave links provide the necessary bandwidth for network expansion and eliminate bottlenecks. Service providers can save money because they will no longer have to depend on backhaul support from the wired telecommunications infrastructures. The three polling base stations (represented by red-dashed links) 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. This effectively gives the ISP base station (e.g., about a 33 Mb/s if using a 100 Mb/s backbone) from which to increase the network penetration and user density. Each remote base station would use directional antennas to achieve maximum distance and to prevent interference from the other base stations. These sectorized base stations then connect to other SPEEDLAN 9000 products, which are located in mesh clouds throughout the sectors. (In Figure 1-6 on page 1-12, the mesh clouds are represented inside the yellow circles; the mesh routers in the cloud are represented with blue-dashed links.) As a provider's network grows, connections may be expanded incrementally to create entire wireless metropolitan area networks.

What's New for Version 3.03

The following fixes apply to Version 3.03:

NAPT Forwarding Rule During Update	If you upgrade from version 2.x to 3.x, verify that your forwarding rules are displayed correctly on the Internal Servers page. If your forwarding rule appears as an "Unknown" service, define the service on the Services page.
Problem with SPEEDView TCP Dump	Fixed a bug that prevented SPEEDVIEW from performing a TCPDUMP on a link that had been encrypted. This only applies to Star mode.
Problem with Address Sharing During Update	Fixed a bug (affecting only Version 3.00) in the update process that prevented the transfer of existing NAPT rules to Address Sharing rules.
Reboot Removed NAT Rules	Fixed a bug (affecting only Version 3.00) that removed NAT rules after a reboot.

What's New for Version 3.0

New Features:

Firewall	The SPEEDLAN 9000 (via the SPEEDLAN 9000 Configurator) allows you to control incoming and outgoing traffic. A firewall prevents unauthorized access to a network. Utilizing the SPEEDLAN 9000 Configurator, SPEEDLAN 9000 routers can increase security and provide additional support to users of the network. The firewall function is located under the Forwarding menu. For more information, see *Firewall, page 3-61*.
SPEEDSignal for Pocket PC PDA	SPEEDSignal can now communicate with SPEEDLAN 9000 routers via their wireless interface. Since this version runs on a Pocket PC Personal Digital Assistant (PDA), installers can easily troubleshoot antenna alignment problems in the field. For more information, see *What is SPEEDSignal?, Appendix F-2*.

Enhancements in the SPEEDLAN 9000 Configurator for Version 3.0:

IP Address Configuration	The "TCP/IP Configuration" page has been renamed "IP Address Configuration". This page is under the Network menu. For more information, see *IP Address Configuration, page 3-20*.
Virtual Addresses	Virtual addresses are IP addresses (usually public) that the SPEEDLAN 9000 router can use in addition to the IP addresses assigned to each of its network interfaces. Virtual addresses are normally used to preserve public IP addresses when a limited number is available. Previously, virtual addresses were implicitly created when referenced in a NAT rule. Version 3.0 requires explicit creation of a virtual address prior to referencing it. This page is under the Network / IP Addresses menu. For more information, see *Virtual Addresses, page 3-24*.

Configuration Summary	The new functions from the Forwarding menu have been added to the Configuration Summary. The Configuration Summary is under the System menu. For more information, see *Configuration Summary, page 3-25*.
DHCP Server	Timestamps are now reported in client time. Timestamps track the date and time for each event in the log. The timestamps are recorded on the Log Messages page under the DHCP Server menu. For more information, see *DHCP Server Menu, page 3-39*.

New Forwarding Menu	Use this menu to control how traffic is forwarded through the router. These features are available under the Forwarding menu: -Services: Use this enhancement to define a network service (e.g., web server, FTP and email server) between the client and server nodes on your network. When you create a service, you will be allowed to forward public services inward to the internal (privately addressed) servers on your network. -Address Sharing: This enhancement allows an administrator to share a public IP address with privately addressed network nodes. -Internal Servers: The enhancement allows an administrator to make a service available from an IP address, even though the owner of the IP address may not be actually providing the service. -1:1 NAT: This enhancement allows an administrator to statically map a public IP address to the private IP address of one of the nodes on your network. This is useful when trying to preserve a limited number of public IP addresses on the WAN network. -IP Sessions: The SPEEDLAN 9000 firewall offers stateful packet filtering. IP Sessions allows you to view sessions whose state is currently active. For more information on these enhancements, see *Forwarding Menu, page 3-48*.

Contacting Technical Support

For more information, contact Wave Wireless Networking at:

7020 Professional Parkway East

Sarasota, FL 34240

941-907-2300 (phone)

941-355-0219 (fax)

www.wavewireless.com

Note: Registered customers should check our web site on a regular basis for updates, router firmware, SPEEDView, and other utility programs. If you haven't registered your products yet, you may do so by visiting the Wave Wireless Website "Support" directory."

Chapter 2
SPEEDLAN 9101, 9102, 9103 & 9104 Hardware

Rooftop and Tower Installations Warning

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

General Safety Requirements for Installation of SPEEDLAN 9000 Models

1. The AC power socket outlet should be installed near the switching power supply and junction box.
2. It is recommended that replacement of the battery which is soldered to the PC board should be done by manufacturer or professional installer.
   CAUTION: THERE IS RISK OF EXPLOSION IF BATTERY IS REPLACED BY INCORRECT TYPE. DISPOSE USED BATTERIES ACCORDING TO INSTRUCTIONS.
3. During installation of SPEEDLAN 9000 on the tower or on the wall, the necessary clearance from the power and lightning conductors should be maintained and proper grounding provided. The installation should be done in accordance with National Electrical Code:
   - NEC Article 725 – CEC Rule 16
   - NEC Article 800 – CEC Section 60 and
   - NEC Article 810 – CEC Section 54.

Hardware Overview

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

- **SPEEDLAN 9101 (for business or residential):** A router used in a non-line-of-sight pico cell (using the Mesh protocol). This router contains an integrated 8 dBi, omni antenna which is directly attached on the top. You do not need an additional external antenna. In addition, the parameters are configured with the Mesh protocol in the SPEEDLAN 9000 Configurator. This router uses an integrated 8 dBi omni-directional antenna.

  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 Mesh Clouds, page 1-8*.

- **SPEEDLAN 9102:** This model can be configured as Customer Premise Equipment (CPE) at one end of the point-to-point or point-to-multipoint link. It could also be configured as a mesh router in a mesh cloud (via an external omni). (This router is also referred to as a "Flexnode" because it is a star (CPE) and mesh topology solution.)

- **SPEEDLAN 9103:** This model is pre-configured as a base station but can be reconfigured to function as a CPE router or as one end of a point-to-point or point-to-multipoint link. The 9103 can also be configured as a mesh node with an external omni.

- **SPEEDLAN 9104 (for residental applications only):** The 9104 contains all of the following features of the 9101 except RIP routing. The 9104 uses an integrated 5 dBi omni and is intended for residential applications. This router also supports one device on the local interface as well.

Tips for Antenna Alignment

You are encouraged to use the transmit power test during installation if you have a spectrum analyzer or power meter to measure the output for the antenna alignment. For more information, see Appendix A - IP Recovery, page 6. The SPEEDSignal application will also help installers align or position antennas on 9000 units. For more information on this application, “What is SPEEDSignal?” on page 2 of Appendix F.

Drawings of Outdoor, Remote-Mounted Components

Indoor Junction Box

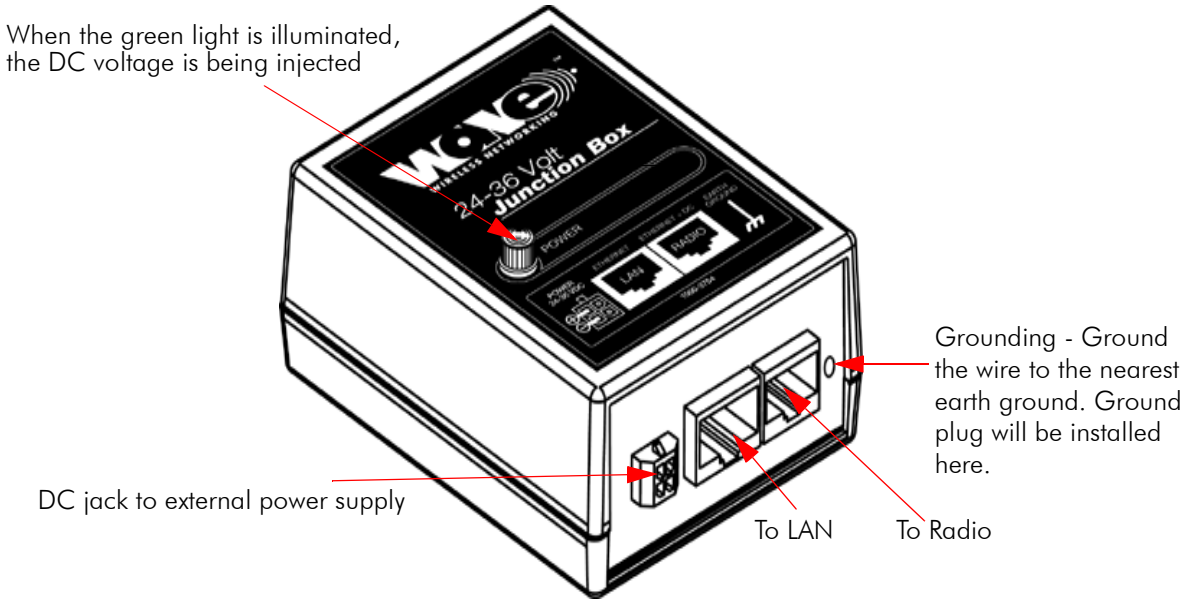


Figure 2-1: Indoor junction box for 9000 series products

The indoor junction box is used with the SPEEDLAN 9000 series routers.

WARNING!: Make sure the network is plugged into the LAN interface, and that the radio is plugged into the radio interface. If you do this procedure wrong, the voltage that is meant to go to the radio can damage a device on the network.

The SPEEDLAN 9101(with an Integrated 8 dBi Omni)

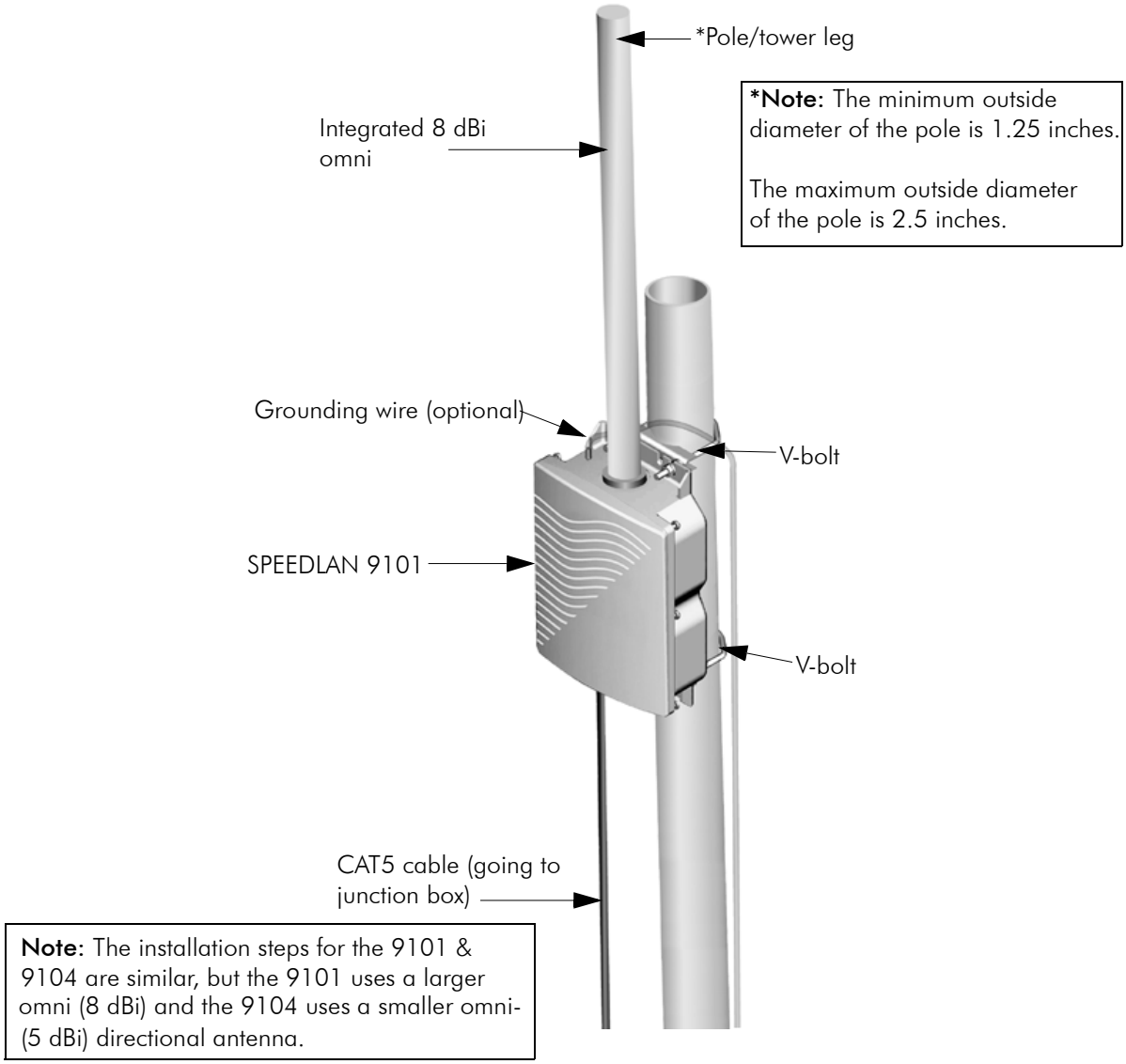
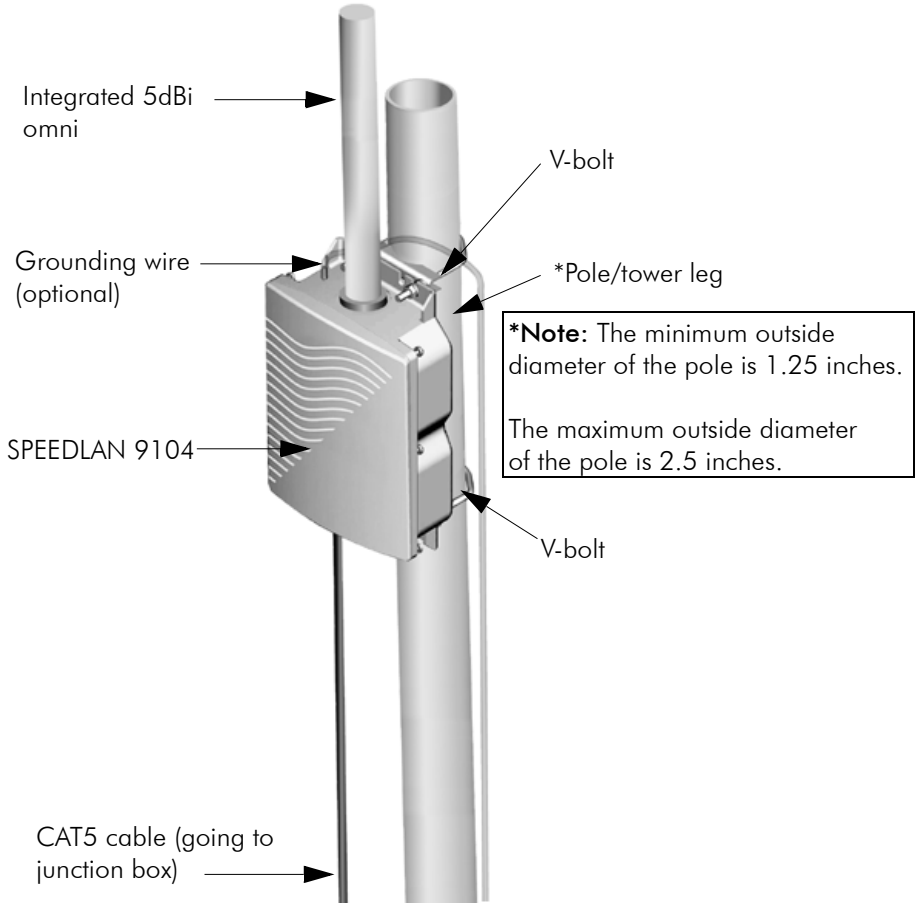


Figure 2-2: SPEEDLAN 9101 installation

SPEEDLAN 9104 (with 5 dBi Omni)



Note: The installation steps for the 9101 & 9104 are similar, but the 9101 uses a larger omni (8 dBi) and the 9104 uses a smaller omni-(5 dBi) directional antenna.

Figure 2-3: SPEEDLAN 9104 installation

Bottom View of SPEEDLAN 9101/9104

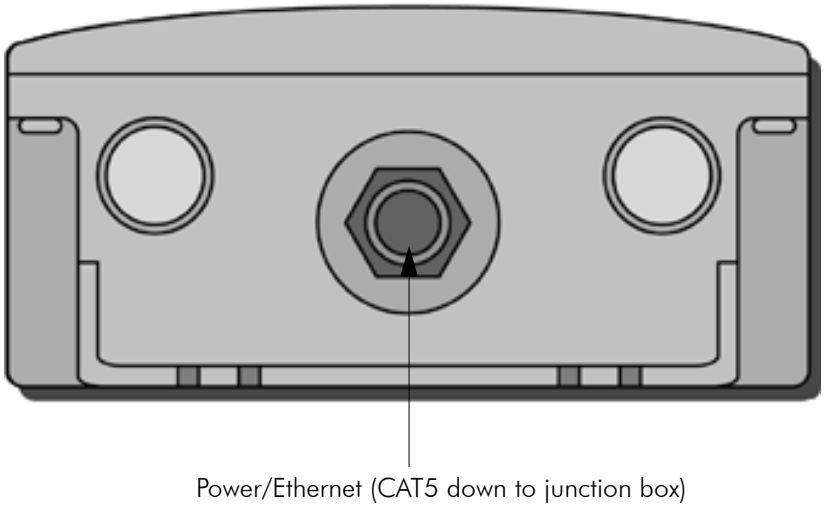


Figure 2-4: Bottom view of 9101/9104 case

System Description

These are high-speed, long range wireless LAN outdoor, remote-mounted units/routers that provide building-to-building connectivity in a mesh cloud.

Package Contents

- SPEEDLAN 9101/9104
- Product registration card
- CD containing: Product manual, SPEEDView management software (including SPEEDSignal and IP Recovery), SPEEDLAN 9000 Installation Diagrams, README.txt file and Adobe Acrobat Reader
- Indoor junction box
- Integrated, omni-directional antenna is attached to the router (8 dBi for 9101 and 5 dBi for 9104)
- V-bolt kit which includes the following
  - Bolt, V, Tower Mount, Stainless Steel (U-bolt) (quantity 2)
  - Nut, 1/4"-20, Serrated Flange, Stainless Steel (quantity 4)
  - V-Bracket, Tower Mount, Aluminum (quantity 2)
- Power supply

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

- Hardware ties
- Specialized CAT5 cable

Customer Sourced / Other

- Combination wrench or socket wrench (7/16") to tighten the nuts on the V-bolts (customer sourced only)
- Other tool accessories that can be purchased separately from Wave Wireless are: cable, connectors, crimpers, spectrum analyzer, shrink wrap, APC 10BaseT putty, aluminum 2" pole, extendable mast, ballast mount, peak roof mount, extra v-bolts, nuts, grounding rod clamps, wall mounts

Installation Steps for the SPEEDLAN 9101/9104

To install your SPEEDLAN 9101, follow the steps below:

Step 1: Mounting the SPEEDLAN 9101/9104

This 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 9101/9104 on the Pole

- **Pole Mount:** 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 nuts for the clamps on the back of the pole mount.

Step 3: Running the Cabling

1. Run outdoor 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. Install the ground plug into the junction box. Install the Ethernet to the radio cable. Install the Ethernet to the router. Install the DC connector to the junction box. Plug the external power supply into the wall outlet.
(The VAC power outlet's input voltage of this universal adapter can vary from 100 to 250 VAC.) Connect the DC output of the adapter to DC jack on the indoor junction box.

4. Connect the wireless SPEEDLAN 9101/9104 to the customer's Ethernet LAN or PC by connecting the RJ-45 plug on a standard Ethernet CAT5 cable to the RJ-45 port connector, marked as "radio" on indoor junction box. Connect the other end of the Ethernet CAT5 cable to your Ethernet hub, switch or router.

Important Note: Waterproofing the Connectors!

Make sure you waterproof all the connectors, as follows: Apply two layers of electrical tape to the connector (covering three inches of cable past 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 9101/9104

The diagram below displays where the main components are located for the SPEEDLAN 9101/9104 with an integrated omni.

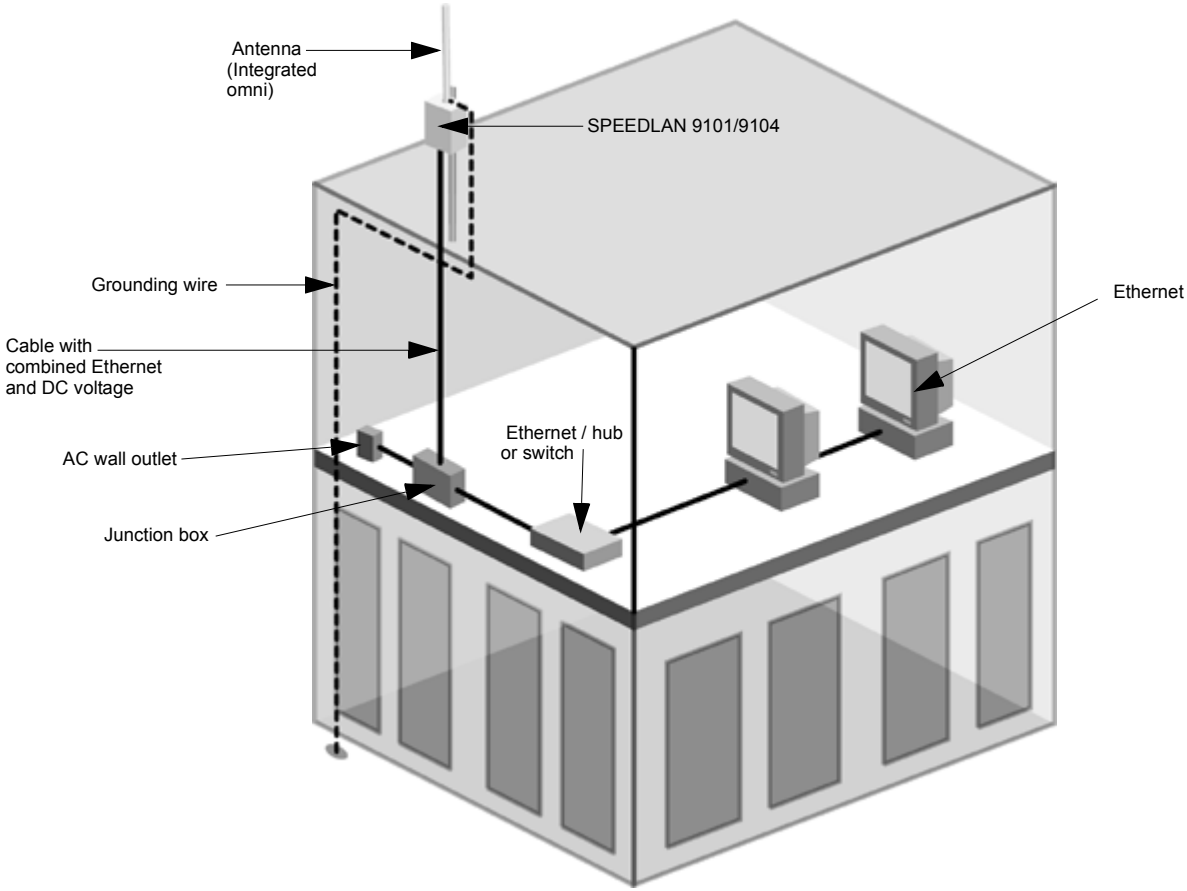
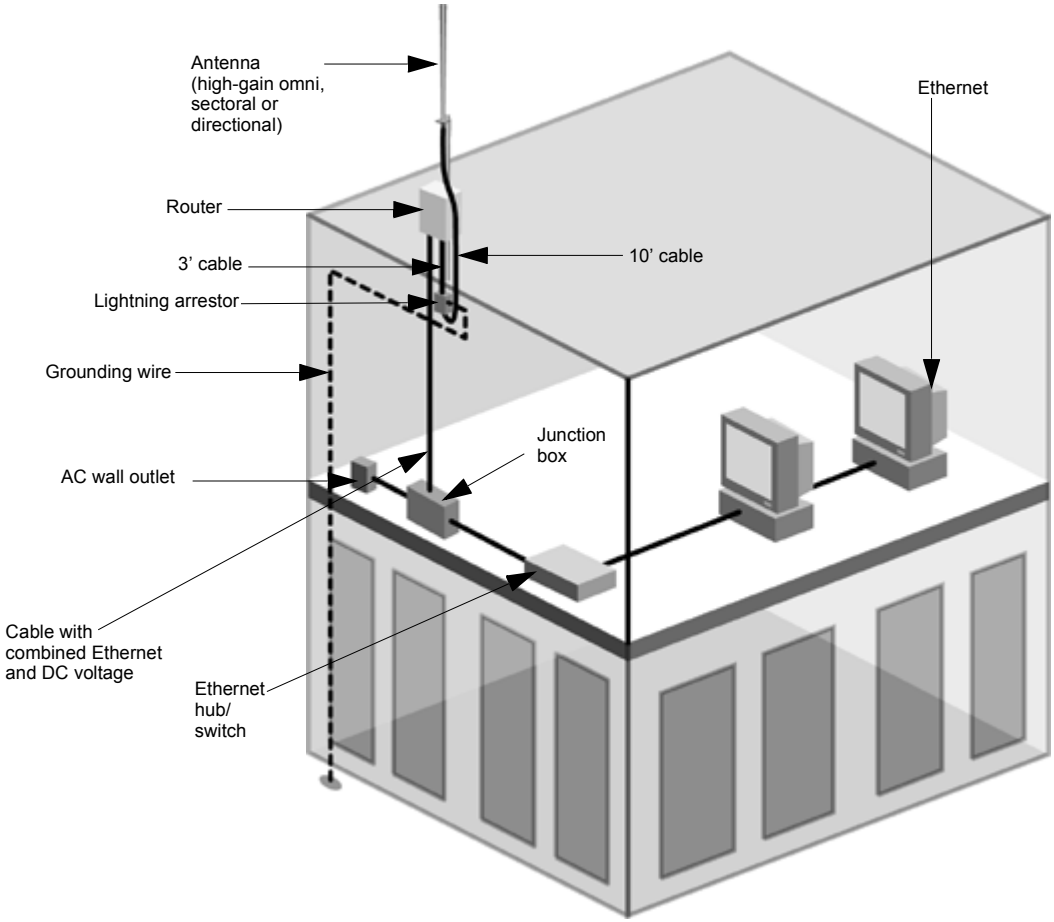


Figure 2-5: 9101/9104 installation diagram

Note: Most users needing the mesh topology solution will use the SPEEDLAN 9101/9104. However, there is the option of using an external antenna for mesh use (e.g., high-gain omni antenna, sectoral or even directional). Contact Wave Wireless for more information. On the next page is an example of this solution:

SPEEDLAN 9102 (acting as mesh router) with High-Gain Omni External Antenna (e.g., High-Gain Omni)



Note: Ground the case to the closest building ground. This will create a short conduction path for lightning strikes to dissipate properly.

Figure 2-6: 9102 installation diagram

To install an external antenna (e.g., high-gain omni), see *Installation Steps for the SPEEDLAN 9102 and 9103, page 2-16*.

The SPEEDLAN 9102 and 9103 (CPE and Base Station Use)

As a 9102 CPE/Point-to-Point with Grid or Directional Antenna

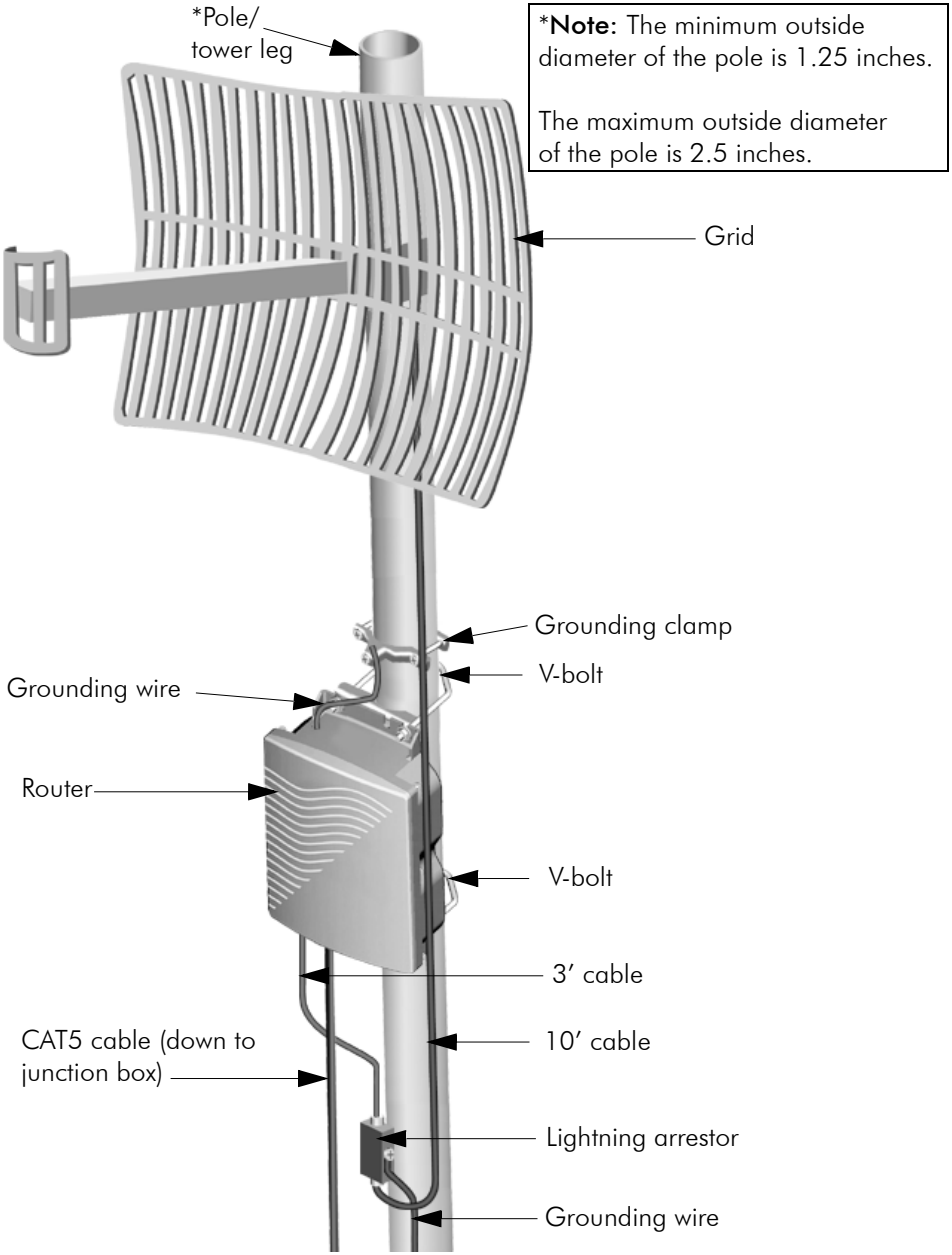


Figure 2-7: CPE with grid

As a Base Station with Sectoral Antenna

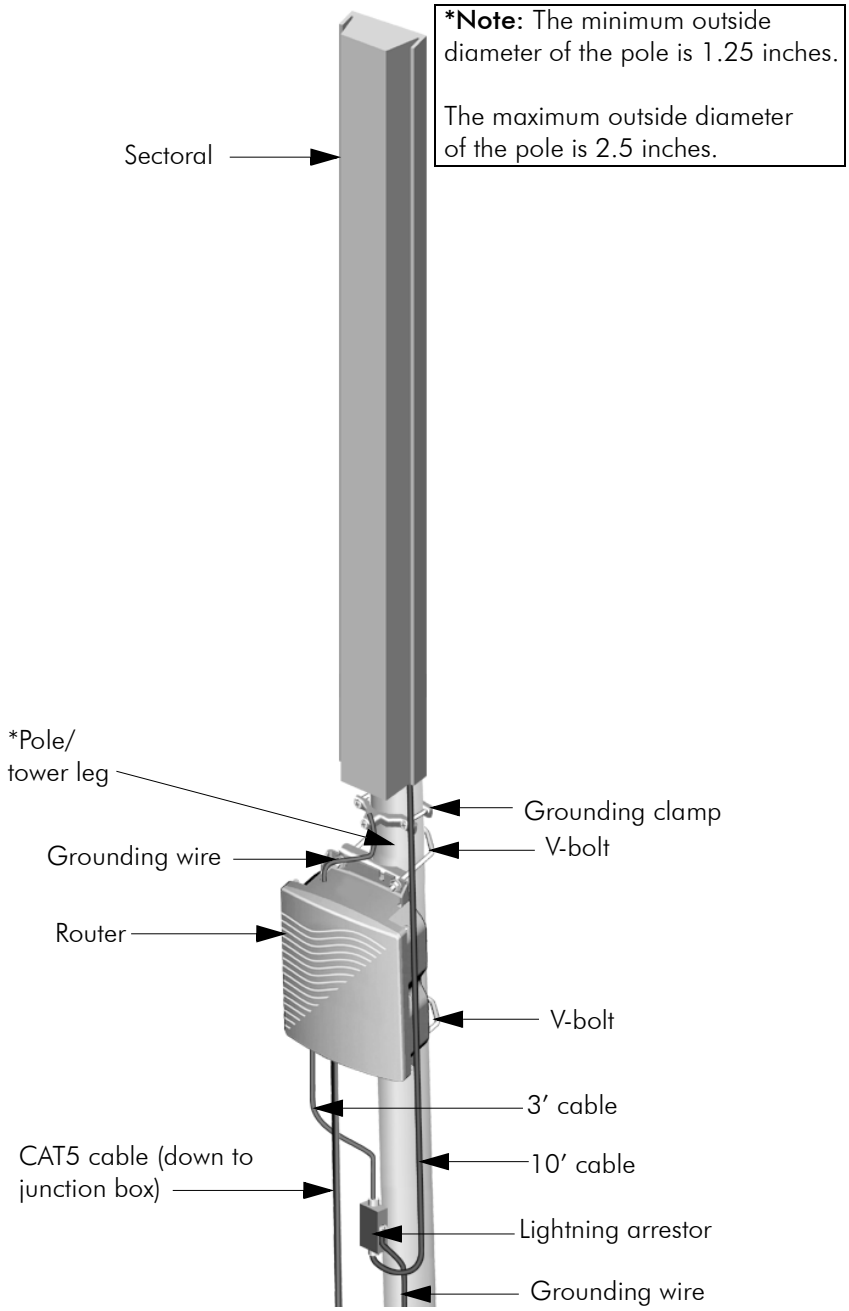


Figure 2-8: Base station with sectoral

As a Base Station with High-Gain Omni Antenna

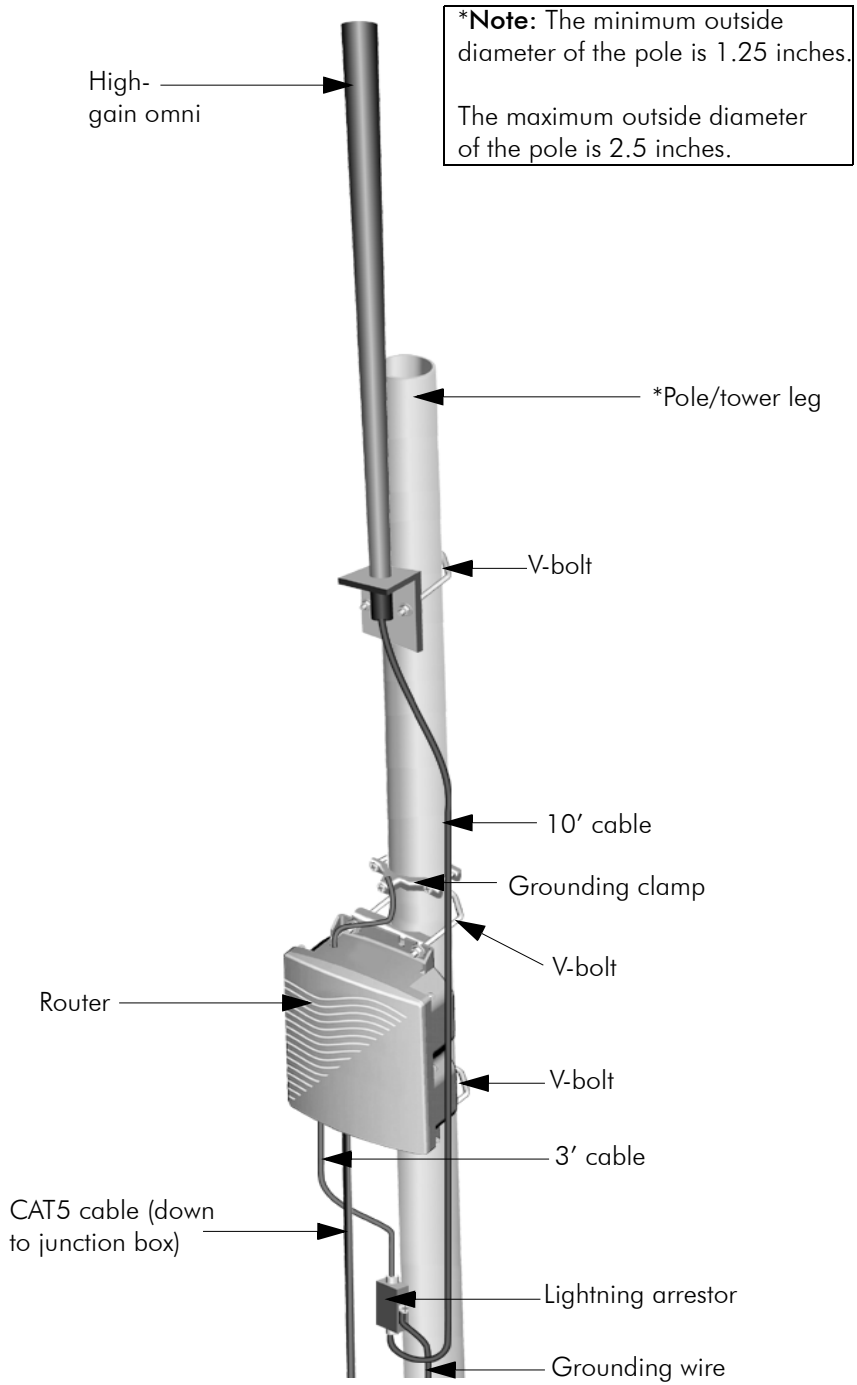


Figure 2-9: Base station with high-gain omni

Bottom View of SPEEDLAN 9102 and 9103

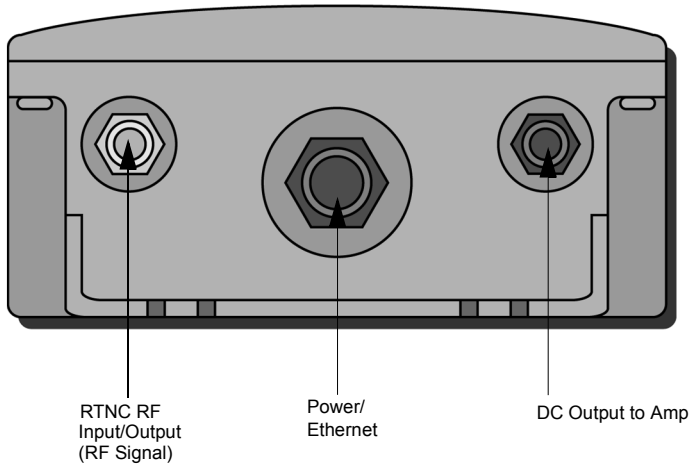


Figure 2-10: Bottom view of SPEEDLAN 9102/9103 case

System Description

The SPEEDLAN 9102 and 9103 routers are high speed, long range wireless LAN routers that provide connectivity to remote Ethernet networks. For single point-to-point links, a SPEEDLAN 9102 router can be used in each building to create a wireless communication link. For multipoint links, a SPEEDLAN 9103 router acts as the central base station, which controls the communication between multiple SPEEDLAN 9102 routers acting as CPE. The local router communicates with a remote router on another LAN. This effectively creates an extended wireless network, spanning sites can be 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

The following items are included in the package contents:

- SPEEDLAN 9102 or SPEEDLAN 9103 router
- Product registration card
- CD containing: Product manual, SPEEDView management software (including SPEEDSignal and IP Recovery), SPEEDLAN 9000 Installation Diagrams, README.txt file and Adobe Acrobat Reader
- Indoor junction box
- 3’ RF cable

- V-bolt kit which includes the following
  - Bolt, V, Tower Mount, Stainless Steel (U-bolt) (quantity 2)
  - Nut, 1/4"-20, Serrated Flange, Stainless Steel (quantity 4)
  - V-Bracket, Tower Mount, Stainless Steel (quantity 2)
- Power supply

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

- Hardware ties
- Lightning arrestor
- Electrical tape
- Waterproof putty tape
- Specialized CAT5 cable
- 10′ RF cable
- Grounding rod clamps

*Note: Antenna for the SPEEDLAN 9102 or 9103 can be purchased separately.

Customer Sourced / Other

- Combination wrench or socket wrench (7/16") to tighten the nuts on the V-bolts (customer sourced only)
- Other tool accessories that can be purchased separately from Wave Wireless are: cable, connectors, crimpers, spectrum analyzer, shrink wrap, APC 10BaseT putty, aluminum 2" pole, extendable mast, ballast mount, peak roof mount, extra v-bolts, nuts, grounding rod clamps, wall mounts

Installation Steps for the SPEEDLAN 9102 and 9103

Both SPEEDLAN 9102 and 9103 routers follow the same general installation steps. Some installation instructions are specific to customers who purchased Installation Kits from Wave Wireless. To view a diagram of the installation listed below, see Figure 2-13 on page 2-22.

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

Antenna Selection Tip: Use a high-gain omni or sectoral antenna for a base station (9103), and use a grid or directional antenna for a CPE or point-to-point router (9102).

To install your SPEEDLAN 9102 or 9103 router with an external antenna, do the following:

Step 1.Verifying Line-of-Sight

Before installing the antenna and router, make sure a clear line-of-sight exists between the two points. 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 at 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. Make sure at least 60 percent of the RF signal is unobstructed by any path blockages.

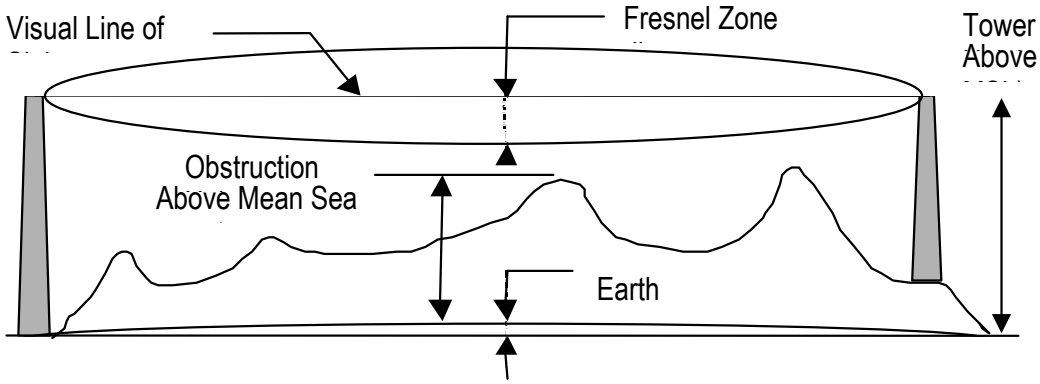


Figure 2-11: Line-of-sight (LOS) diagram

Note: For long distances, additional antenna height is often required to overcome signal diffraction and to provide clear Radio LOS. For Radio LOS, a clear Fresnel (Freh-nel) zone is required to minimize diffraction effects. The Fresnel zone is shaped like an elongated football. The most clearance is required at the mid-point between the two sites.

Beyond approximately 10 miles, the curvature of the earth can also become significant. At these longer distances, visually sighting the remote site can be difficult or impossible due to atmospheric haze. Terrain data (map or differential GPS) must be relied upon for determining path clearance. Elevation data determined with these methods is above Mean Sea Level; and does not account for curvature of the earth. Both the curvature of the earth and the Fresnel clearance numbers can be combined to determine the additional clearance required above any natural or man-made obstructions along the path.

Obtaining this clearance can be accomplished by raising the antenna height at one or both sites. If this is not practical, then consider relocating one or both sites to locations with higher elevations. Another option is to add a third site to go over or around the obstacle.

If you see any obstructions between two antennas, move one or both antennas to another location.

Step 2. Mounting the Antenna

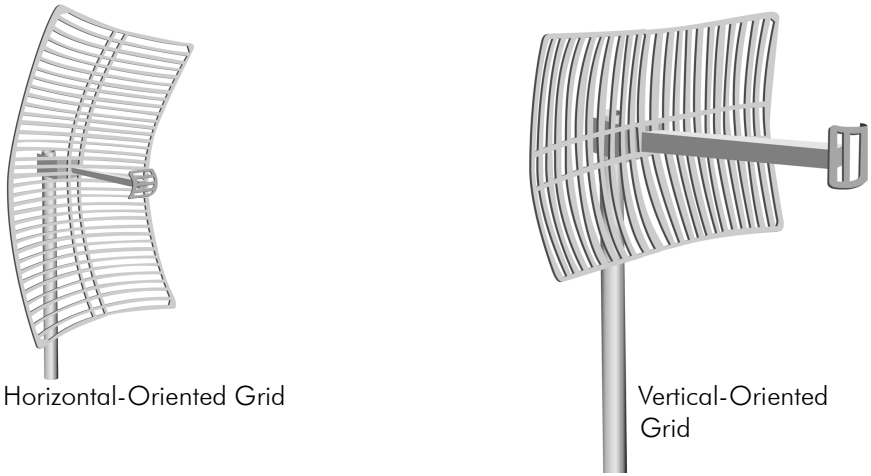
Follow the instructions below to mount the antenna.

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. A horizontal grid should be horizontal (or parallel to the ground). A vertical grid should be perpendicular to the ground. Make sure all bolts and screws are fastened tightly.



See also *Tips for Antenna Alignment, page 2-3*.

Figure 2-12: Grid antennas

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 horizontal and vertical-oriented 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 and 9103

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 router and the other on the bottom. Make sure you tighten the nuts for the clamps 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 SPEEDLAN router to the wall or concrete by using the concrete or wood mounting screws. Make sure it is securely mounted on the wall.

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 or 9103 router.

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 outdoor Ethernet cable from the router to the indoor junction box located inside the building.

e) Secure the cable (i.e., to the pole) 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 the opening 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 2-21*.

g) Next, ground the lightning arrestor. For more information, see *Grounding the Lightning Arrestor, page 2-21*. You can also ground the router case to the ground, as shown in the installation diagrams in this chapter.

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. The next series of steps will show you how to effectively seal the lightning arrestor and its cables.

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 the bottom, below the bottom connector over the lightning arrestor and beyond the upper connector, 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 Router to Customer's Ethernet LAN

a) Connect the RJ-45 connector on a standard Ethernet CAT5 cable to the Radio RJ-45 port on the indoor junction box.

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

Step 8. Connect the Wireless Router to the Power Supply

a) Connect the DC output of the adapter (24-36 Vdc) to DC jack on the indoor junction box.

b) Connect power cord of AC-DC 24-36 Vdc adapter to 110 or 220 VAC power outlet (the input voltage of this universal adapter can vary from 100 to 250 VAC).

Step 9. Adding Additional Routers

Repeat the steps above for all SPEEDLAN 9102 and 9103 routers that will be communicating with this one.

9102/9103 Installation Diagram

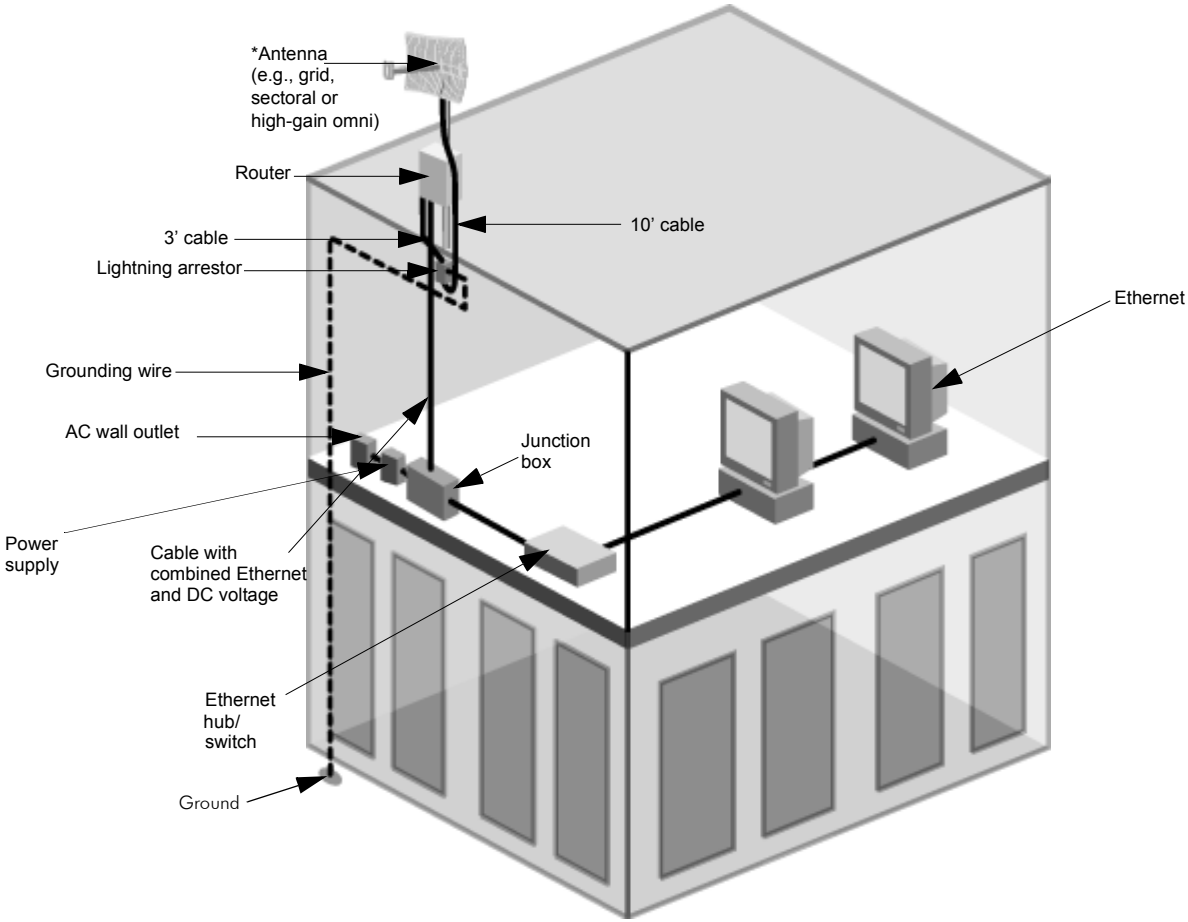


Figure 2-13: Base/CPE complete installation diagram

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

You can ground the router case to the ground. You can ground the lightning arrestor as well.

Notes:

Chapter 3
General Functions of the Configurator

This chapter covers general functions when configuring any 9000 router, such as:

- General Information: *Manual Initial Configuration of the SPEEDLAN 9000, page 3-2*, *Logging on the SPEEDLAN 9000 Configurator, page 3-10* and *Logging Off, page 3-13*
- Network menu: *IP Address Configuration, page 3-20* and *Virtual Addresses, page 3-24*
- System menu: *Configuration Summary, page 3-25 Version, page 3-28*; *Host Name, page 3-29*; *Password, page 3-30* and *Reboot, page 3-31*
- Routing menu: *Def Gateway, page 3-32*; *RIP2 Setup, page 3-33* and *RIP Settings, page 3-34*; *Route Table, page 3-36* and *Static Route, page 3-37*
- DHCP Server menu: *Basic Instructions for Setting Up DHCP on an Interface, page 3-40*; *Viewing Log Messages, page 3-47* and *Status, page 3-47*
- DHCP Relay menu: *DHCP Relay Menu, page 3-47*
- Forwarding menu: *Services, page 3-49*, *Three Features of NAT, page 3-54*, *Firewall, page 3-61* and *IP Sessions, page 3-66*.

- Diagnostics menu: *Interface Statistics, page 3-68*; *ARP Table, page 3-70* and *ICMP Statistics, page 3-71*
- Admin menu: *User Configuration, page 3-74*; *Permissions, page 3-74*; *Software Update, page 3-76 Support, page 3-77* and *Current Sessions, page 3-79*.

Note: For more information on how the Configurator menu is structured, see *Overview of the SPEEDLAN 9000 Configurator General Main Menu, page 3-7*.

Warning! Do not forget your password. Keep it in a safe place. If you lose your full access password, there is no way to recover it without returning the router to Wave Wireless Networking.

Manual Initial Configuration of the SPEEDLAN 9000

Each SPEEDLAN 9000 is produced with a default configuration that renders it usable in many applications. However, if you need to manually configure your 9000 router, follow the directions below.

Prerequisites

Configuration of the SPEEDLAN 9000 is done through the SPEEDLAN 9000 Configurator. In order to access the SPEEDLAN 9000 Configurator, you must have:

- a client workstation (e.g., PC, Mac, Sun),
- a compatible browser (Netscape Navigator 4+ or Internet Explorer 5+), and
- a TCP/IP connection to the SPEEDLAN 9000.

A TCP/IP connection to the SPEEDLAN 9000 can be made through its wireless interface or through its wired interface. If the default configuration creates a wireless LAN that is compatible with the target inter-network, the network administrator can connect to the individual SPEEDLAN 9000 router through that wireless LAN. The following section assumes that a SPEEDLAN 9000 router is being configured via its wired interface, possibly before it is installed at its intended physical location.

Connecting a SPEEDLAN 9000 and a Client PC

A connection between a SPEEDLAN 9000 and a client PC may be established using either:

1. one crossover cable, or
2. two straight-through cables (also called patch cables) and a hub or a switch.

- If you select option # 1, connect one end of the crossover cable to the client PC and the other end to the junction box.

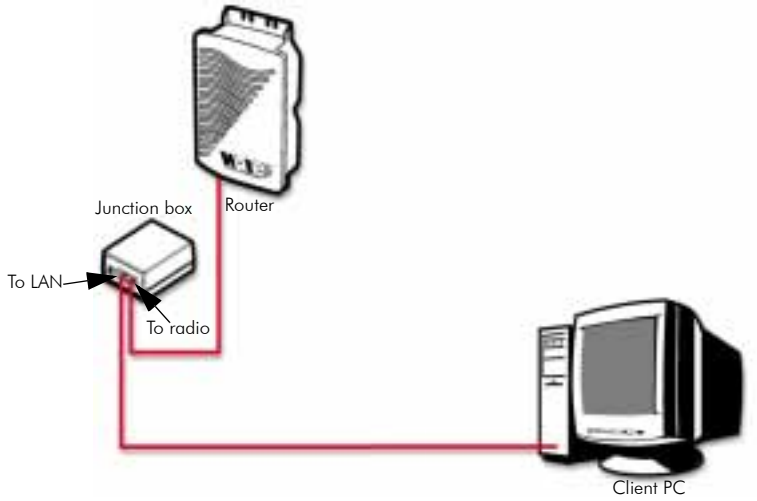


Figure 3-1: Using one crossover RJ-45 Ethernet cable

Either end of the crossover cable can connect to the client PC or junction box.

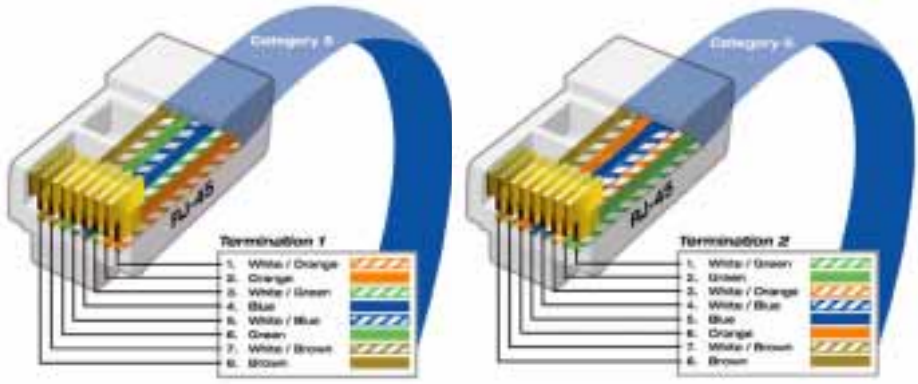


Figure 3-2: Crossover cable and pin out diagram

Note: The crossover cable actually crosses the transmit and receive pairs of wires so that direct communications can take place between devices. Use a crossover cable anytime you need to interconnect two computers or two devices in the same location when a hub or a switch is either unavailable or not practical.

- If you select option # 2, connect a straight-through cable from both the client PC and the junction box to the hub or a switch.

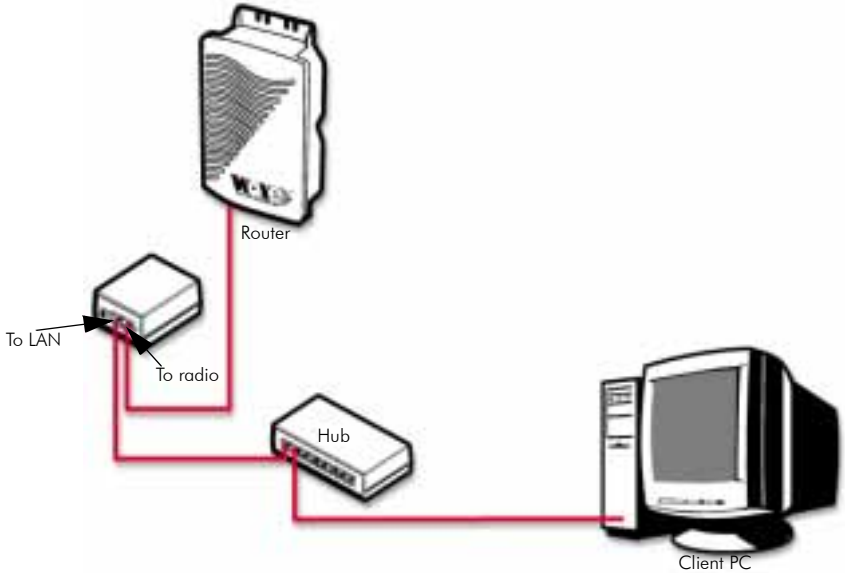


Figure 3-3: Using two straight-through RJ-45 Ethernet cables

Upon power up, a SPEEDLAN 9000 router that is not configured attempts to obtain an IP address for its Ethernet LAN interface from a DHCP server. This is done by broadcasting a "DHCPDISCOVER" message on that interface. If a suitably configured and reachable DHCP server replies within 30 seconds, the SPEEDLAN 9000 will use the IP address, netmask, (etc.) that the DHCP server provides. Otherwise, the unconfigured SPEEDLAN 9000 will adopt a private network IP address 192.168.69.1 and a /24 netmask (255.255.255.0).

If a DHCP server is not used, it is recommended that the SPEEDLAN 9000 router and the client PC be on the same subnet. Otherwise, the ability to configure intervening routers may be required.

If the SPEEDLAN 9000 that is not configured and the client PC are on the same LAN, their IP address should be configured compatibly (same IP network and netmask). This can be accomplished by either:

1. The client PC obtaining its IP address from the same DHCP server as the SPEEDLAN 9000.
2. Statically set the client's PC IP address to 192.168.69.x (x is in the range of 2 - 254) and its netmask to /24 (255.255.255.0).

- If you selected option #1 above, follow these general directions:
  Open the **Control Panel**, and then double-click the **Network and Dial-up Connections** icon. Go to **TCP/IP Protocol Properties** to select the **Obtain an IP address from a DHCP server** option. Then, accept changes and close this dialog box. Then, restart your computer.

- If you selected option #2 above, follow these general directions:
  Open the **Control Panel**, and then double-click the **Network and Dial-up Connections** icon. Go to **TCP/IP Protocol Properties** to verify that your PC is on the same network as the router 192.168.69.x (x is in the range of 2 - 254), and the subnet mask should be /24 (255.255.255.0). If you made changes, accept the changes and close this dialog box. Then, restart your computer.

Before continuing you should verify that the client 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 the DHCP assigned address) at a command-line prompt. This ping 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, you can open the client's browser and enter the IP address of the SPEEDLAN 9000 router. If using DHCP and DNS, it may be possible to refer to the SPEEDLAN 9000 router by its name.

Note: SPEEDView gives you a "management" view of the network. You will use the SPEEDLAN 9000 Configurator (web browser) to configure the 9000 routers. If you want to configure a router in SPEEDView, just double-click any router and it will open the SPEEDLAN 9000 Configurator. For more information about SPEEDView, see *Using SPEEDView, page 8-1*.

Wireless Interface IP Address Assignment

If the wireless interface does not already have a statically configured IP address, it will assume the 10.x.y.z/8 address, where x, y, and z are the decimal representations of the least significant three octets of the IEEE 802 MAC address of the SPEEDLAN 9000's wireless interface. This method is used to ensure uniqueness. Because the last three octets of the IP address are variable, a /8 netmask (255.0.0.0) is used in order for the SPEEDLAN 9000s to communicate on this network.

Automating the Configuration of Multiple SPEEDLAN 9000s

In mesh mode, some of the configuration parameters for the SPEEDLAN 9000 are common to all SPEEDLAN 9000s in the same network, for instance the channel and signaling rate of the wireless interface.

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 the SPEEDLAN 9000 Configurator, choose **Reboot** from the **System** menu (see *Reboot, page 3-31*).

Adding Additional SPEEDLAN 9000s to the Wired Network

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

- Connect the additional SPEEDLAN 9000 routers to a hub or switch on the network and have DHCP assign IP addresses dynamically.
- 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 General Main Menu

How the Configurator Menu is Structured

Base stations, CPE routers, point-to-point routers and mesh routers all use the same main menu, as shown in *Main menu, page 3-10*. However, some of the submenus are limited depending on which mode you are operating, such as base station mode, CPE mode, point-to-point (primary and secondary), and mesh mode. Any content that is common for the base station, CPE, point-to-point, and mesh router is located in this chapter. Any content that is exclusively used for base station mode is in *Using the Configurator to Set Up Special Parameters for a Base Station, page 4-1*. Any content that is exclusively used for CPE mode is in *Using the Configurator to Set Up Special Parameters for CPE Routers, page 5-1*. Any content that is exclusively used for point-to-point mode is in *Using the Configurator to Set Up Special Parameters for Point-to-Point Routers, page 6-1*. Any content that is exclusively used for mesh mode is in *Using the Configurator to Set Up Special Parameters for Mesh Routers, page 7-1*.

This menu lists the pages that are common to a SPEEDLAN 9000 base station, CPE, point-to-point, and mesh routers.

- Network
  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 router. You will also be able to define the display name for the wireless or fixed device. For more information, see *IP Address Configuration, page 3-20*.
  - If you need to set up the interfaces from a base station, see *Interfaces for Base Mode, page 4-2*.
  - If you need to set up the interfaces from a CPE router, see *Interfaces for CPE Mode, page 5-2*.
  - If you need to set up the interfaces from a point-to-point router, see *Interfaces for Point-to-Point Mode, page 6-2*.
  - If you need to set up the interfaces from a mesh router, see *Interfaces for Mesh Mode, page 7-2*.
  - If you need to set up authentication and encryption between a base station and CPE routers, see *Authentication Section, page 4-4* and *Turning on Encryption, page 4-8*.

Other specialized parameters not common under the Network menu for the base, CPE, point-to-point and mesh routers:

- If you need to set the start timing parameters (polling) for controlling how a base station treats a CPE router that has no traffic to send but still respond to polls, see *Star Timing Parameters Section, page 4-7*.
- If you need to see what CPE routers are connected to the base station, see *Base Station Information, page 5-3*.
- If you need to set up pass phrase authentication from a CPE router, see *Authentication, page 5-4*.
- If you need to set up encryption or specialized settings for a point-to-point router, see *Point-to-Point Settings, page 6-3*. If you need to see what secondary point-to-point routers are connected to the primary point-to-point router(s), see *Primary Station Information, page 6-6*. See also *Authenticating a Point-to-Point Secondary Router Only, page 6-6*.
- If you need to view mesh routers currently on the network, *Mesh Nodes, page 7-3*. If you need to set up security parameters for mesh routers, see *Security, page 7-3*.

- **System**
  Use this menu to define information about the host, view information about the SPEEDLAN 9000 Configurator, set the current password and reboot the 9000 router. For more information see, *System Menu, page 3-25*. To view a configuration summary of the units on the network, see *Configuration Summary, page 3-25*.
- **Routing**
  Use this menu to view and set routing configuration. For more information, see *Routing Menu, page 3-31*.
- **Wireless**
  Use this menu to select the frequency and signaling rate of the wireless device. You can also set up the Tx Retry, Max Tx Rate, and Signaling Rate Fallback on a base station, CPE, point-to-point or mesh router. To do these options, choose **Wireless** from the main menu. You can also block or unblock mesh routers. In mesh mode, you can also set the receive threshold.
- **DHCP Server**
  Use this menu to configure a DHCP server on one or more of the wired interfaces. You can also view log messages and view the interfaces being serviced with DHCP. For more information see, *DHCP Server Menu, page 3-39*.

- **DHCP Relay**
  Click this menu to enable DHCP Relay and set the parameters it requires. For more information, see *DHCP Relay Menu, page 3-47*.
- **Forwarding**
  Use this menu to control how traffic is forwarded through this router. For more information, see *Forwarding Menu, page 3-48*.
- **Diagnostics**
  Use this menu to troubleshoot your SPEEDLAN 9000 network. For more information, see *Diagnostics Menu (Troubleshooting the Network), page 3-67*.
- **Admin**
  Use this menu to perform administrative tasks, such as setting up user password and permission information. You can also remotely control the 9000 routers on the network, update software, reset all configuration to the factory default, enable or disable SPEEDSignal, and enable manufacturer access to the router for advanced troubleshooting. For more information, see *Admin Menu, page 3-73*.

Other specialized parameters not common under the Admin menu for the base, CPE, point-to-point and mesh routers:

- If you need to remotely reboot a 9000 router (base station mode), see *Remote Control, page 4-15*.
- If you need to update software on a 9000 base station, see *Software Update, page 4-16*. If you need to update software for a base station and a CPE, see *Updating the Software on a Base Station and CPE, page 4-17*.
- If you need to remotely reboot or turn off the SPEEDLAN 9000 point-to point routers, see *Remote Control for Point-to-Point Primary Routers, page 6-13*.
- If you need to remotely reboot or turn off the SPEEDLAN 9000 mesh routers, see *Remote Control, page 7-13*.
- If you need to update the software on the point-to-point routers, see *Software Update for Point-to-Point Primary or Secondary Routers, page 6-13*.
- If you need to update the software on the mesh routers, see *Software Update, page 7-14*.

Diagram of SPEEDLAN 9000 Configurator Main Menu

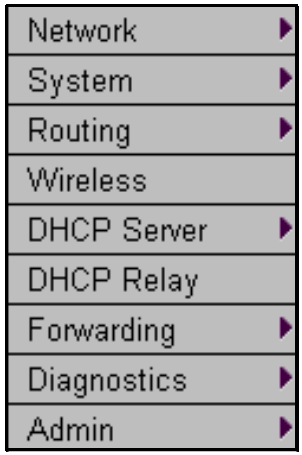


Figure 3-4: Main menu

Note: If you want to learn more about IP addressing, see *Basics of IP Addressing, page 9-2*.

Logging on the SPEEDLAN 9000 Configurator

To access the SPEEDLAN 9000 Configurator, open your web browser and enter the URL (http://) or IP address of the router you want to configure. The factory default IP address is 192.168.69.1.

Note: The SPEEDLAN 9000 Configurator can be accessed at the standard web (HTTP, port 80) and secure web (HTTPS, port 443) locations. If you have forwarded either of those ports to internal network nodes, you can still reach the configurator at an alternate location:

- port 6590 - server alternate HTTPS (for example, type "https://192.168.69.1:6590/")

Classes of Users (and Passwords)

All software including the SPEEDLAN 9000 Configurator, SPEEDView, SPEEDSignal and IP Recovery share the same password(s). The only place where you change the password for all of these is in the SPEEDLAN 9000 Configurator.

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_full" (this is also the only access password for IP Recovery).
  Note: "Full Access" does not show up in "Admin/Users" because the user will not be able to change its permissions and it has write permission on everything.
- **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_ad" (account for the wireless SPEEDLAN 9000 network)
- **Wireless Read**: "wave_wireless" (account for the wireless SPEEDLAN 9000 network)

Notes:

The minimum password length is 8 characters. The maximum password length is 16 characters (including the underscore character or spacebar). Any characters over the maximum length (16) will be truncated. This rule applies for the Configurator, SPEEDView, SPEEDSignal and IP Recovery.

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 *Admin Menu, page 3-73*.

Logging On

Follow these steps (starting on the following page) to log on to the SPEEDLAN 9000 Configurator.

1 Make sure you entered the correct URL or IP address of the router. For more information, see *Logging on the SPEEDLAN 9000 Configurator, page 3-10*.

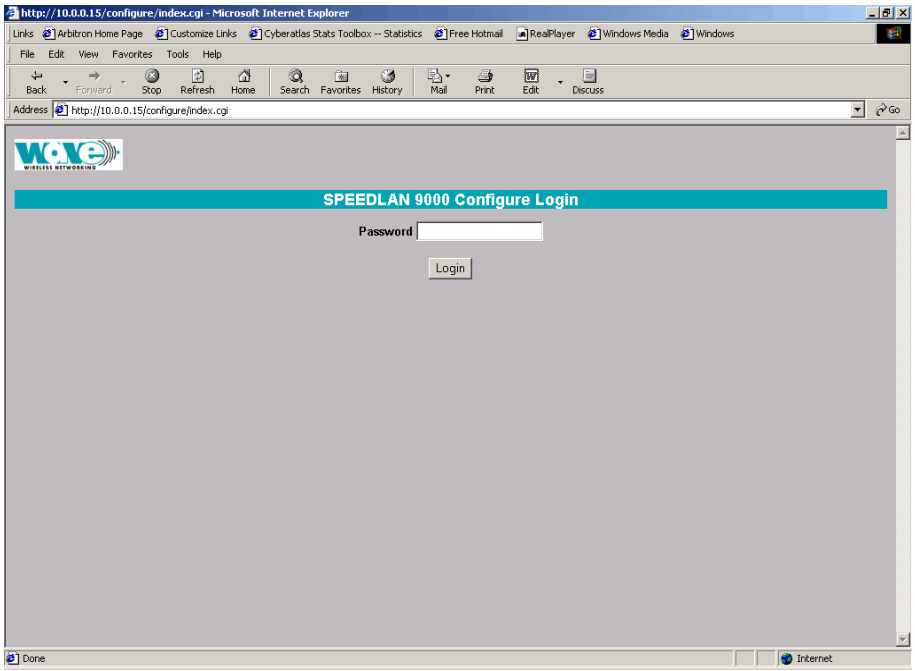


Figure 3-5: Login page

2 Enter the password in the **Password** text box. To know which password (from 8 to 16 characters) you should enter, see *Classes of Users (and Passwords), page 3-10*.

3 Login by clicking **Login**.

4 When you login for the first time, the Security Alert dialog box will appear. Follow the directions under *Understanding the Security Alert Screens, page 3-13*.

Logging Off

If you need to log off the Configurator, click the **Log Off** link (as circled in the figure below).

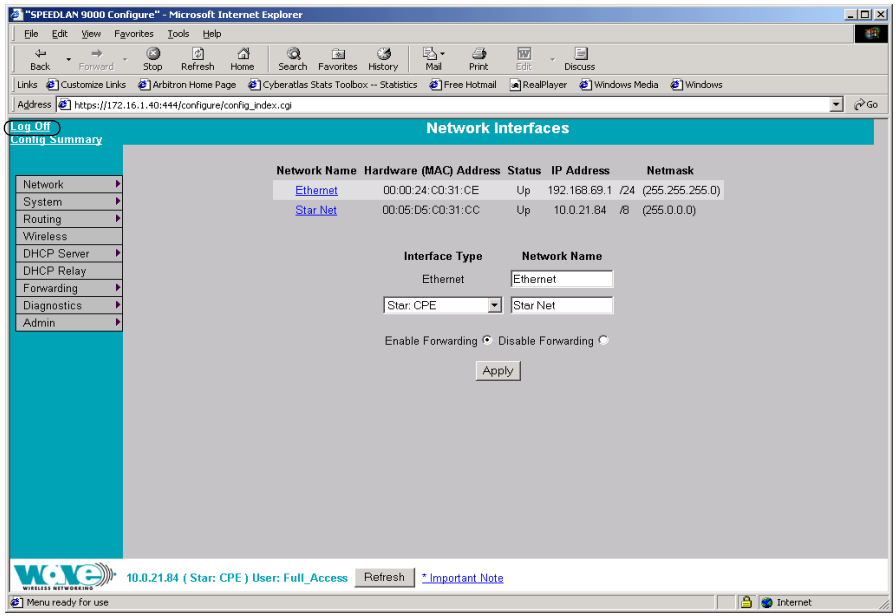


Figure 3-6: Logging Off

Understanding the Security Alert Screens

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

Follow the steps beginning on the next page:

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.

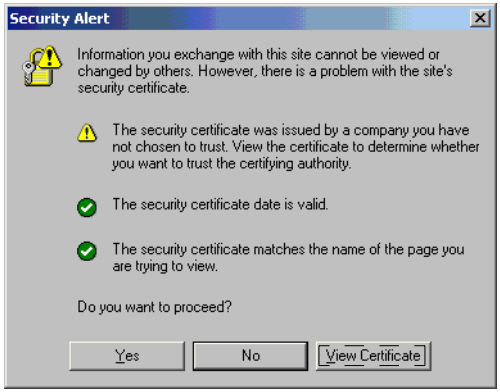


Figure 3-7: Security Alert screen

2 Click **Install Certificate**.

Figure 3-8: Certificate screen

3 The Certificate Import Wizard will appear.

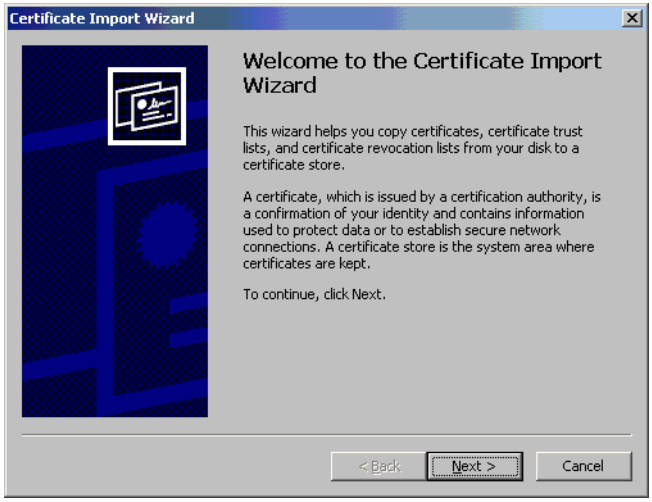


Figure 3-9: Certificate Import Wizard screen 1

4 Click **Next**.

5 The following dialog box will appear.

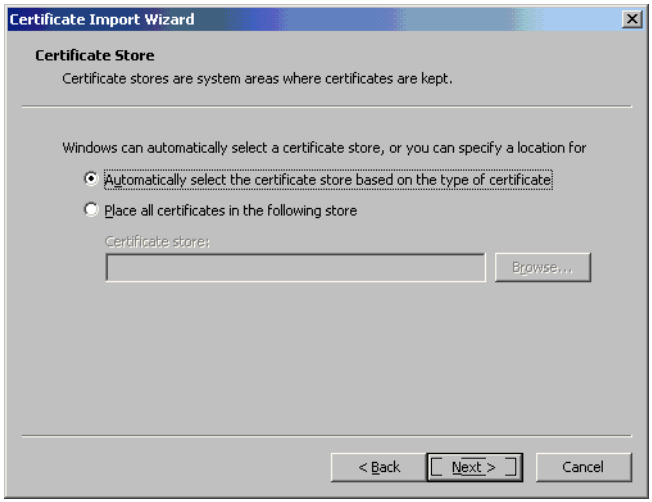


Figure 3-10: Certificate Import Wizard screen 2

6 Click **Next** again.

7 The following dialog box will appear.

Figure 3-11: Certificate Import Wizard screen 3

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

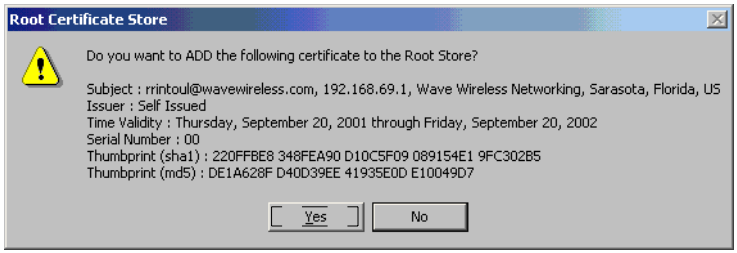


Figure 3-12: Root Certificate Store screen

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**.

Figure 3-13: Certificate Import Wizard message box

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

After Logging On

After you log on, you will see the Network Interfaces page, as displayed below.

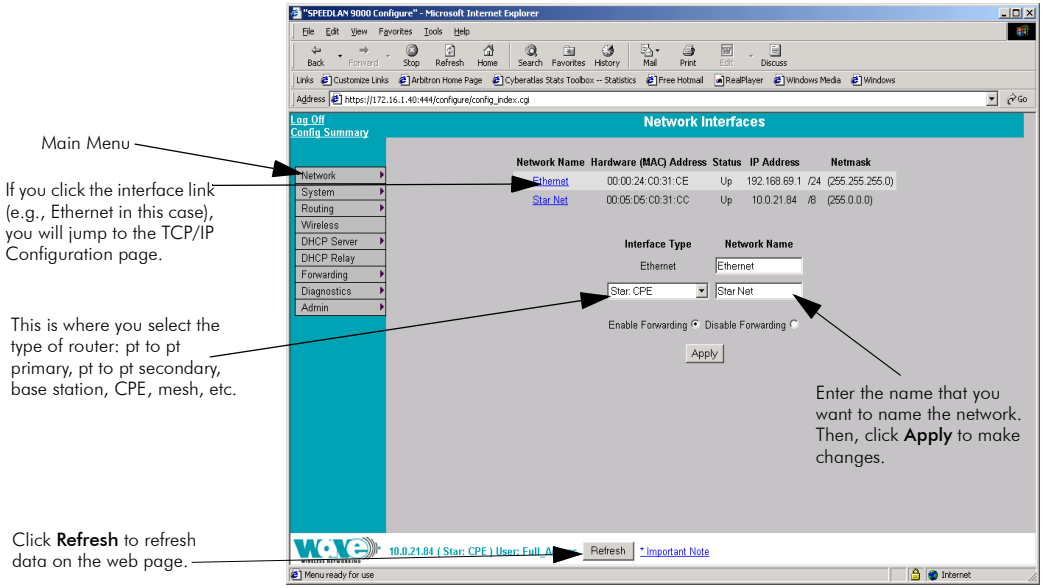


Figure 3-14: 1st screen after logging on

Note: The name you enter in the **Network Name** text box (shown in Figure 3-14 on page 3-17) determines what the interfaces are called on the network. For instance, you can enter, "Star Net" in the **Network Name** text box to represent the "Star CPE" interface. This option just gives the user control over the name of the interface. Therefore, Star Net would be the new name of the Star CPE interface and would be located under the menu headings (e.g., TCP/IP, RIP2, DHCP Server and NAT).

What are enable and disable forwarding?

- **Enable Forwarding**: Select the **Enable Forwarding** option to enable the forwarding of IP packets from the wired interface to the wireless interface and vice-versa.
- **Disable Forwarding**: Select the **Disable Forwarding** option to disable the forwarding of IP packets from the wired interface to the wireless interface and vice-versa.

Helpful Information to Know...

How do you select the router?

As shown in Figure 3-14 on page 3-17, select the type of router (point-to-point, CPE, base station, or mesh) from the **Interface Type** drop-down list. Then, click **Apply**. The SPEEDLAN 9000 Configurator will then recognize the router you selected and allow you to make modifications as needed.

Note: If you need to change the router's topology mode (base station, CPE, point-to-point or mesh) from or to another topology mode (base station, CPE, point-to-point or mesh), see *Changing the Router's Topology Mode, Change Topology Mode, Appendix A-2*.

References on Setting Up the Router

The next step is to set up your router. Follow this chapter to set up the IP address, set routing information, set DHCP, set NAT information, troubleshoot network errors (diagnostic information), and enter basic Administrative information. Make sure you see the section called, *Overview of the SPEEDLAN 9000 Configurator General Main Menu, page 3-7*. This section will tell you which functions are common to all routers and which functions are specialized. This will help you locate the proper section in the manual more quickly.

Caching - viewing the most recent version of a page

Important Note: If you do not see the changes you made on a configurator page, click the **Refresh** button, as shown in Figure 3-14 on page 3-17. Then, the changes will appear.

If the above procedure does not work, follow these steps below:

1. Go to your Internet browser. (These directions are for Internet Explorer.)
2. From the **Tools** menu, choose **Internet Options**. The Internet Options dialog box appears. Click the **Delete Files** button. Then, click **OK**.
3. On the Internet Options dialog box, click the **Settings** button. The Settings dialog box appears. Select the **Every visit to the page** option. This makes sure that the new information is displayed the next time you visit the configurator web page, and the new information will also be added on the SPEEDLAN router.

Session Activity

If you receive this message during your configuration session, "Sorry, the maximum number of sessions has been reached. Try to login later," this is because the maximum log on is 32 consecutive sessions.

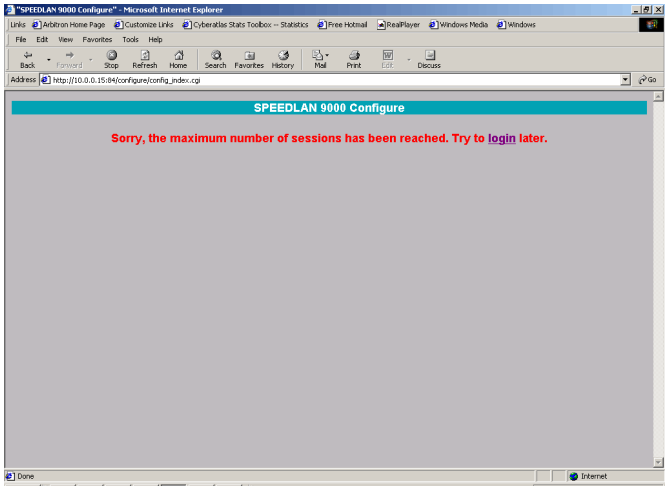


Figure 3-15: Session Activity message 1

If you receive this message during your configuration session, "Your session has expired due to inactivity or because another user has made configuration changes that affect your session, " this is because the configuration session's default time is 30 minutes.

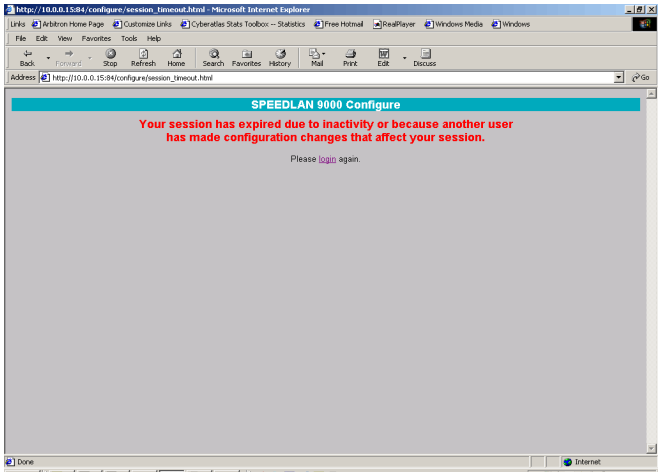


Figure 3-16: Session Activity message 2

9000 Firmware Updates, SPEEDView or Other Utility Programs

Registered customers should check our web site on a regular basis for updates to router firmware, SPEEDView, and other utility programs. If you haven't registered your products yet, you may do so by visiting the Wave Wireless Web site "Support" directory.

If You Need a Temporary IP Address

See the section called, *What is IP Recovery?, IP Recovery, Appendix A-2*:

- If you changed the IP address on the router and forgot it, you can find the configured IP address of the Ethernet interface using IP Recovery.

OR

- If after learning the IP address of the Ethernet interface, you cannot log on to the router using the HTML Configurator (SPEEDLAN 9000 Configurator), then you will be able set a temporary Ethernet IP address so that a connection can made.

The Configuration Menu

Network Menu

- Choose **Interfaces** to select the router you need.
- Choose **IP Addresses** from the **Network** menu to assign an IP address (manually or dynamically via DHCP).
- Choose **Virtual Addresses** from the **IP Addresses** submenu (under the Network menu) to create a public IP address that can be mapped to a private IP address.

Network Interfaces

Choose the type of router as shown in Figure 3-14 on page 3-17. Then, click **Apply**.

IP Address Configuration

This is where you would assign IP Addresses either Manually (static) or via DHCP (dynamic). For DHCP, you may also enter the hostname of the client.
Note: DHCP is not available on the wireless interface.

To activate this page, choose **IP Addresses** and then the name of the interface (i.e., Ethernet, Star Net, Mesh Net) from the **Network** menu. The following page will appear.

The following page will appear.

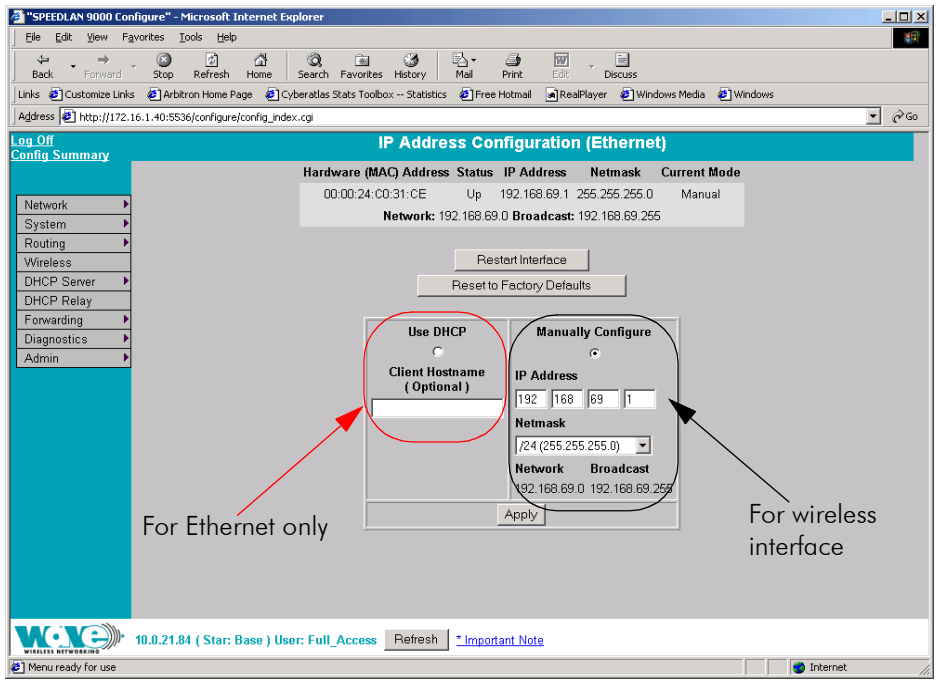


Figure 3-17: IP Addresses page

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

- **Hardware (MAC) 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.
- **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

Figure 3-18: CIDR information page

- **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. The 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 **Apply**.
Optional: If you prefer, you can enter the client name of the host in the **Client Hostname** text box (under "Use DHCP"). The limit of the Client Hostname is 16 characters.

- **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 **Apply**.

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.

After you change the Internet address for an Ethernet or directly connected interface, you must close the SPEEDLAN 9000 Configurator every interface. Otherwise, the information will not be updated. If you follow this step correctly, the next time you open the SPEEDLAN 9000 Configurator, these changes will be updated.

Virtual Addresses

Choose **Virtual Addresses** from the **IP Addresses** submenu (under the Network menu) to create a public IP address that can be mapped to a private IP address. Virtual addresses are IP addresses (usually public) that the SPEEDLAN 9000 router can use in addition to the IP addresses assigned to each of its network interfaces. Virtual addresses are normally used to preserve public IP addresses when a limited number is available. Previously, virtual addresses were implicitly created when referenced in a NAT rule. Version 3.0 requires explicit creation of a virtual address prior to referencing it. Virtual addresses can be used to access the SPEEDLAN 9000 router for configuration, or in NAT functions like Address Sharing, Internal Servers, and 1:1 NAT. Virtual addresses are particularly useful when using 1:1 NAT, where you need more than one public IP address. The virtual addresses do not need to belong to a network assigned to one of the SPEEDLAN 9000's interfaces.

The existence of these addresses will be advertised with RIP, providing that the RIP filters allow it. The Virtual Address page will appear when you choose the Virtual Addresses feature.

The elements on this page are explained below:

- **IP Address:** In this text box, enter the virtual address you want to add. Click **Add** to add the new virtual address. (In the next figure, the user entered "13.13.13.16" in the **IP Address** text box. Next, the user will click **Add**.)

Notes: You cannot apply an IP address from the Ethernet port's subnet.
All virtual addresses have a netmask of /32 (255.255.255.255).

Existing Virtual Addresses

This list contains all defined virtual addresses.

- To remove a virtual address, select it and click **Delete Selected**. (In the next figure, if the user wants to remove virtual address "13.13.13.14". Then, the user would select the check box next to it and click **Delete Selected**.)
- To select all addresses, click **All**. To clear all selections, click **None**.

If an entry has "(In Use)" instead of a check box (as shown in the next figure to the right of virtual address "13.13.13.13"), this means the virtual address is "in use" and cannot be removed.

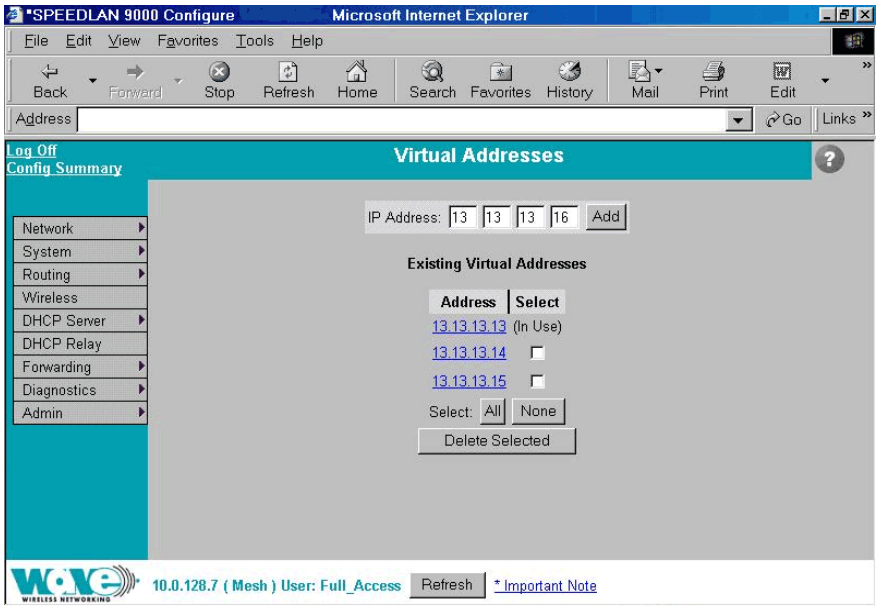


Figure 3-19: Virtual address

Note: If you want to distribute virtual routes, make sure the **Static Routes** check box is selected on the RIP Global Settings page under the Routing / RIP2 Setup / Global Settings menu.

System Menu

- Choose **Config Summary** to view a summarized configuration of the units.
- Choose **Version** to view the current version information.
- Choose **Host Name** to enter a name of the host.
- Choose **Password** to modify the password entries.
- Choose **Reboot** to reboot the system.

Configuration Summary

To view a summarized list of the configuration on the units, choose **Config Summary** from the **System** menu. This is very useful tool for technical support. The Configuration Summary for the Host page will appear displaying a summary which includes the following information:

- **System Version**: Displays the firmware version and uptime for the unit.
- **Network Interfaces**: Displays the interfaces on the network.
- **Route Table**: Displays the routing information between destinations.
- **Wireless Configuration**: Displays the channel, signaling rates, Max Tx Retries, Signaling Rate Fallback and Max Throughput.
- **Blocked Wireless Links**: Displays blocked links. For more information, see *Receive (Rx) Threshold Parameter, page 7-11*.
- **RIP Configuration**: Indicates if RIP is on or off.
- **DHCP Server Configuration**: Indicates if DHCP Server Configuration is on or off.
- **DHCP Relay Configuration**: Indicates if DHCP Relay Configuration is on or off.
- **Virtual Addresses**: Displays virtual addresses.
- **NAT**: Displays types of NAT.
- **Firewall**: Displays if the firewall is enabled or disabled.
- **ARP Table**: Displays Address Resolution Protocol statistics.
- **Statistics**: Displays statistics about the wireless inbound and outbound traffic.

Note: Select the appropriate feature (noted via blue-underlined hyperlink) to jump to the proper feature page. For example, if you click the **DHCP Relay Configuration** link on the Configuration Summary page, it will bring up the DHCP Relay Configuration page where you can modify further information.

There is a short-cut link to the Configuration Summary by clicking the **Config Summary** Link as circled in the figure below.

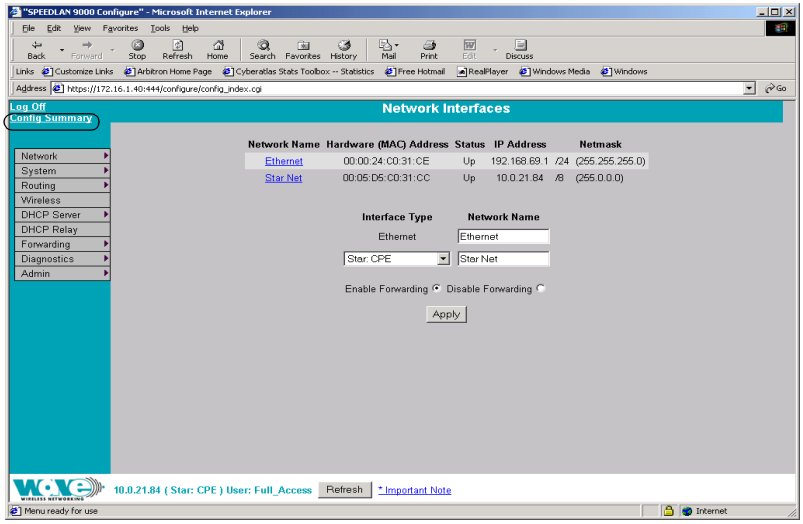


Figure 3-20: Config Summary Link

Version

This page displays information about the current version. When you choose **Version** under **System** menu, the System Version page appears displaying the following information.

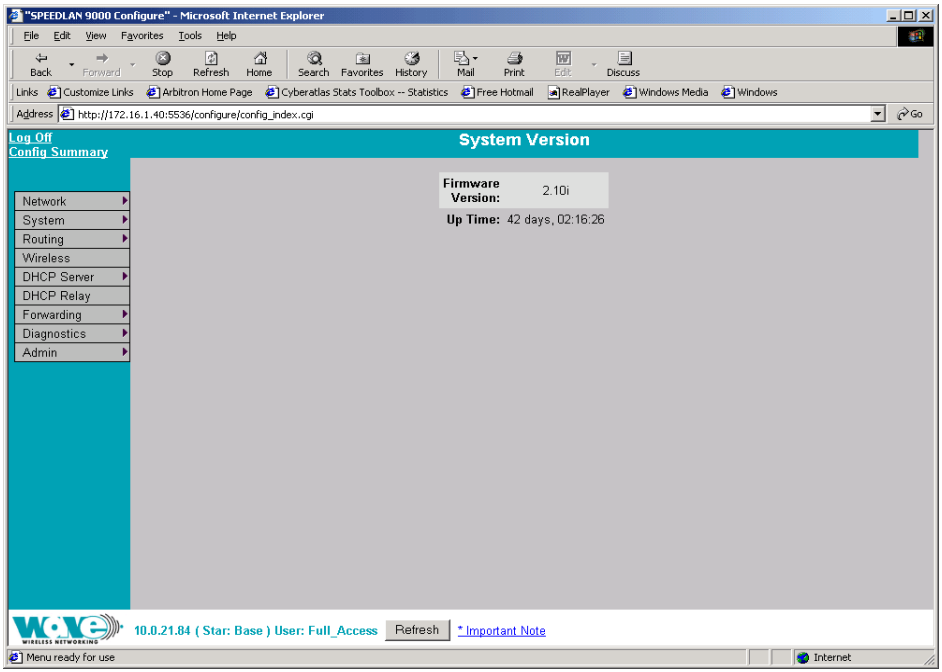


Figure 3-21: Version page

- **Firmware Version:** The version of the firmware.
- **Up Time:** The time since the network-management portion of the system was last re-initialized.

Host Name

To enter the host name of a 9000 router, choose **Host Name** from the **System** menu. The following page will appear.

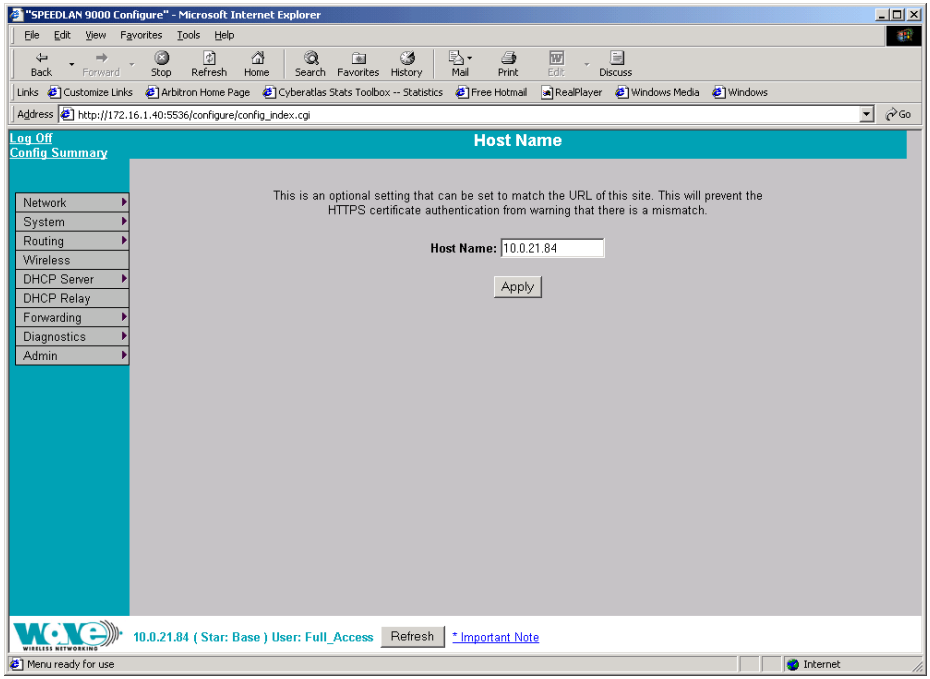


Figure 3-22: Host Name page

The hostname should contain the administratively assigned name for this managed host.

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.

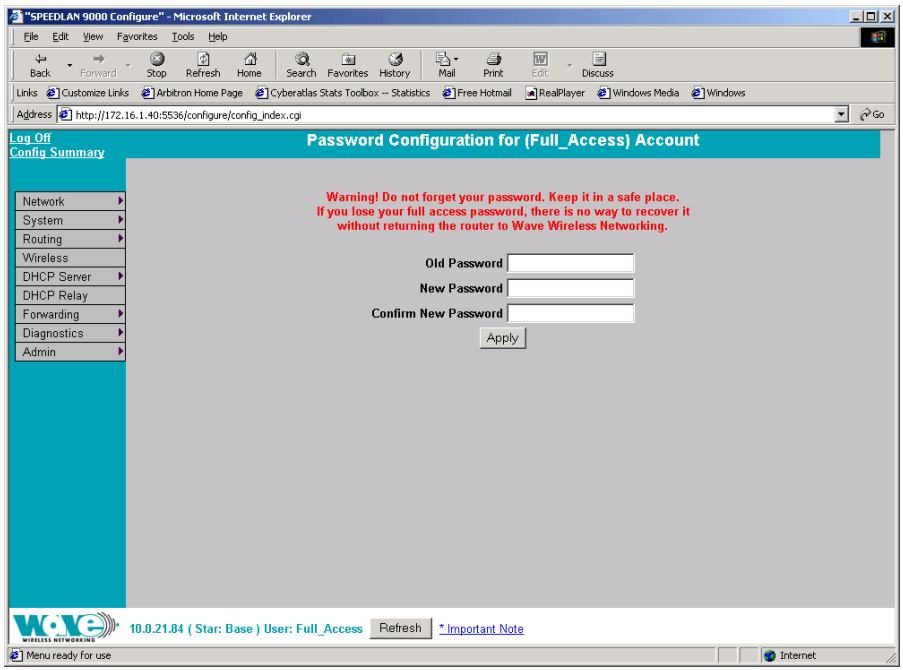


Figure 3-23: Password page

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.
   The minimum password length is 8 characters. The maximum password length is 16 characters (including the underscore character or spacebar).
3. Finally, confirm the new password in the **Confirm New Password** text box and click **Apply**.

Warning! Do not forget your password. Keep it in a safe place. If you lose your full access password, there is no way to recover it without returning the router to Wave Wireless Networking.

Reboot

To reboot the system, choose **Reboot** from the **System** menu. Then, click the **Reboot** button. After clicking **Reboot**, it could take a minute for the 9000 to become fully operational following a reboot.

Routing Menu

Note that full interoperability with RIP1 domains requires that the RIP2 domain be describable as a collection of classfull networks. This requirement can artificially limit the use of Variable Length Subnet Mask (VLSM) to support Classless Inter-Domain Routing (CIDR).

Summary Table of Differences Between RIP 1 and RIP2

	RIP Version 1	RIP Version 2
Status	Obsolete	Current
Acronyms	RIP, RIP1, RIP-1, RIPv1	RIP2, RIP-2, RIPv2
Internet Standards	STD 34 (deprecated)	STDs 56 and 57
Defining RFCs	1058	2453 and 1722
Routing	Classfull	Classless
Subnet Mask	Implicit, fixed length	Explicit, variable length
Route Summarizing	No	Yes
Authentication	None	Optional
Updates Distribution	Broadcast	Multicast

Figure 3-24: Summary Table

The submenus for general routing are specified below:

- Choose **Default Gateway** to modify the IP address of the default gateway.
- Choose **RIP2** to enter settings for RIP.
- Choose **Route Table** to view the information in the routing table.
- Choose **Static Routes** to add static routes as additional routes, default routes or routes that the SPEEDLAN 9000 routers do not contain in their routing table.

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.

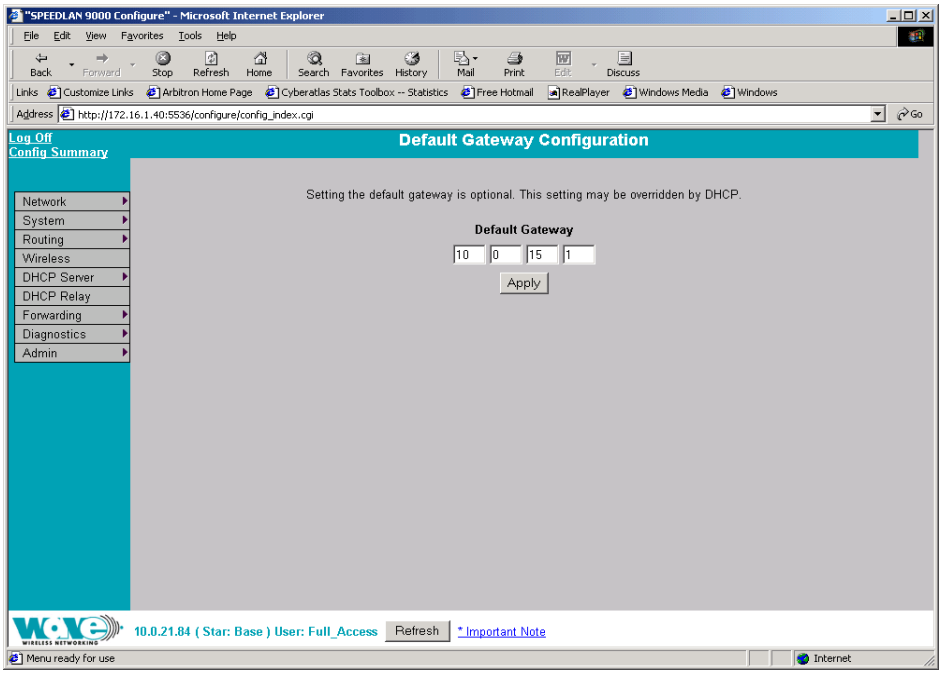


Figure 3-25: Default Gateway page

Default Gateway: Enter the IP address of the default gateway. This is the "door" (usually a base station) where you want the data to travel. Then, click **Apply** after modifying information.

Note: Setting the default gateway is optional. This setting may be overridden by DHCP.

RIP2 Setup

To set up global settings for RIP, from the **Routing** menu, choose **RIP2 Setup** + **Global Settings**. The following page will appear.

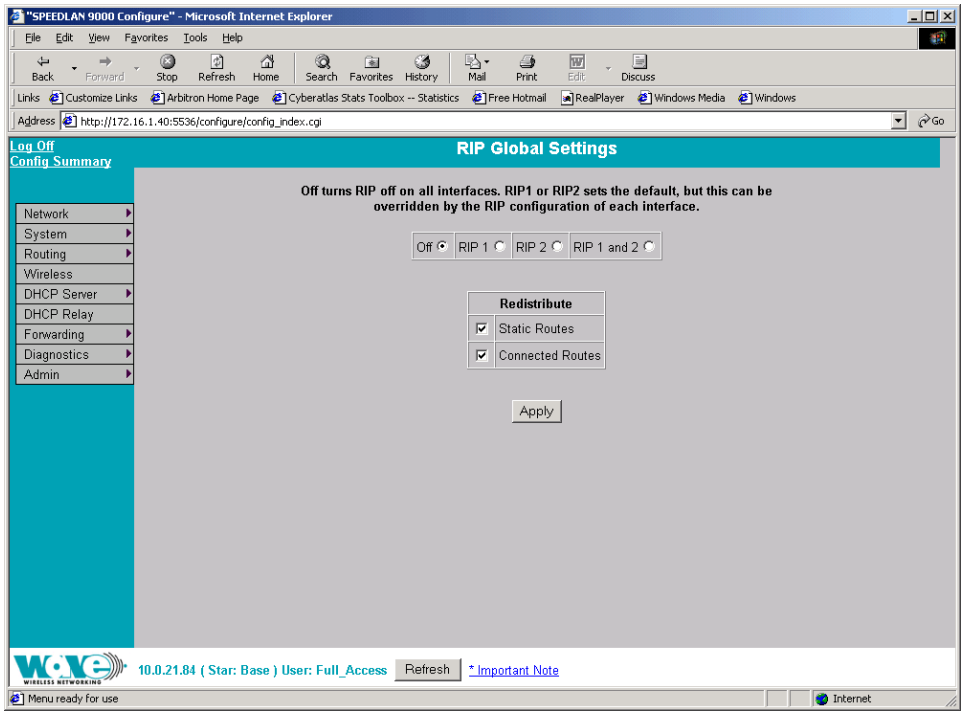


Figure 3-26: RIP Global Settings page

The following RIP Global Settings parameters are described below:

- **Off**: Select to disable RIP.
- **RIP 1**: Select to enable RIP 1.
- **RIP 2**: Select to enable RIP 2.
- **RIP 1 and RIP 2**: Select to enable RIP 1 and RIP 2.

Redistribute section:

- **Static routes:** Select this check box to redistribute static routes so all routers know who it has to pass through to get to the destination. Do not select this check box if you do not want other devices on the network to learn its static route. A static route is an IP path from one point on the network to another point on the network.
- **Connected routes:** Select this check box to redistribute connected routes, which tells the network where it is connected. Do not select this check box if you do not want other devices on the network to know who the router is connected.

Click **Apply** when you are finished making changes.

RIP Settings

To set up RIP 2 settings, from the **Routing** menu, choose **RIP2 Setup** + the interface (e.g., Ethernet or StarNet). The following page will appear.

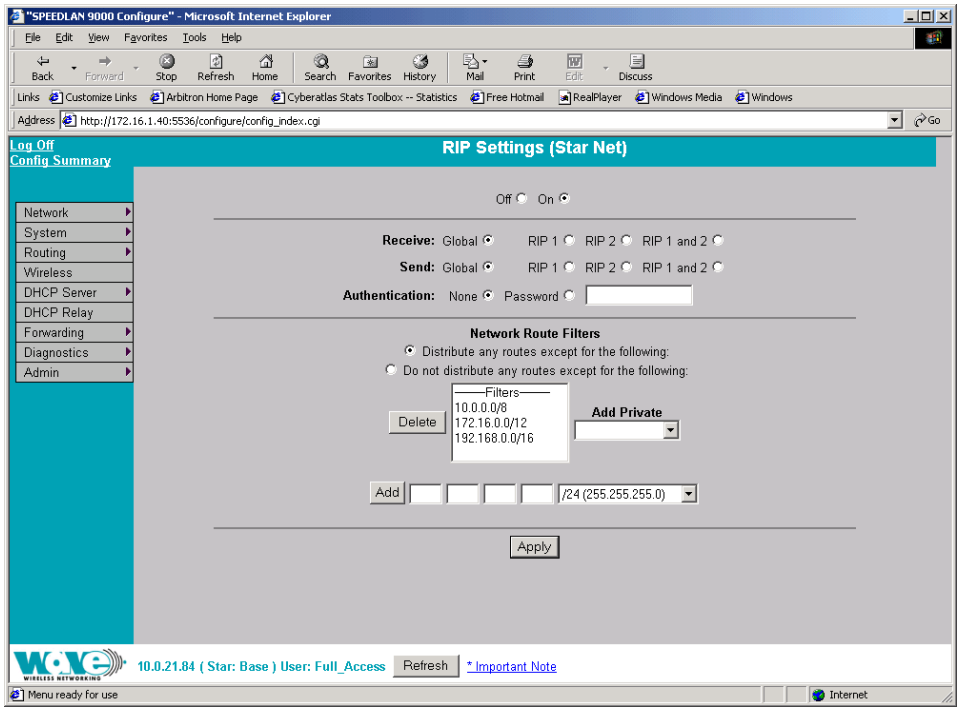


Figure 3-27: RIP Settings page

The following RIP Settings parameters are described below:

- **Off**: Select this option to disable RIP.
- **On**: Select this option to enable RIP.
- **RIP 1 and RIP 2**: Select to enable RIP 1 and RIP 2.
- **Receive**: This is from the incoming location.
- **Send**: This is from the outgoing location.

Receive and Send options:

- **Global**: Click this option to receive/send RIP 1, RIP 2 or RIP 1 & 2 throughout the entire network.
- **RIP 1**: Click this option to receive/send RIP1 from/to the interface.
- **RIP 2**: Click this option to receive/send RIP2 from/to the interface.
- **RIP 1 and 2**: Click this option to receive/send RIP 1 & 2 from/to the interface.

Authentication:

- **None**: Select this option when no authentication is needed.
- **Password**: Select this option when authentication is needed and then enter the password to the right of this option. (Authentication password has a minimum of 8 characters and a maximum of 32 characters.)

Click **Apply** when you are finished making changes.

Network Route Filters:

- **Distribute any routes except for the following**: Select this option to distribute all the network route routes except those which are selected in the Filters box.
- **Do not distribute any routes except for the following**: Select this option to only distribute the selected network route filters in the Filters box.
- **Filters box**: Select those filters needed for option 1 or 2 as explained above.
- **Add**: Click this button to add a network route filter to the Filters box.
- **Delete**: Click this button to remove a network filter from the Filters box.
- **Add Private**: Select the private address from this drop-down list if you want to include a private address in the Network Route Filters list.

Note: If you want to create your own network route filter IP address, type them in the four boxes provided below (each box represents the first, second, third and forth octet in the IP address). Then, click the **Add** button to add the new IP address to the Filters box.

Click **Apply** when you are finished making changes.

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.

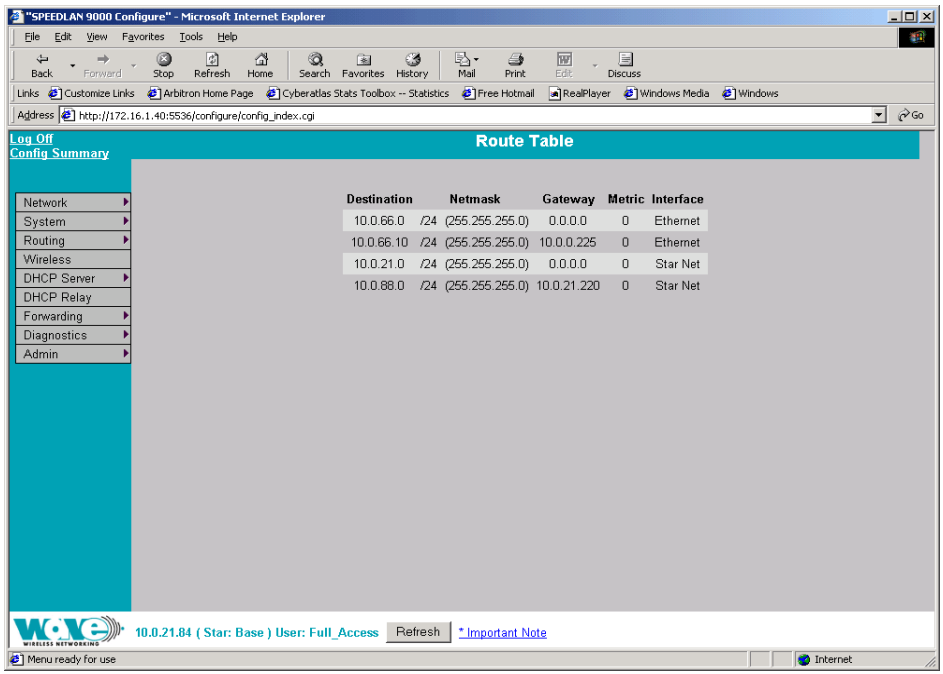


Figure 3-28: Route Table page

Each statistic is defined below:

- **Destination:** This is 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).

- **Mask (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.
- **Metric:** Metric is a number indicating the preference of one route link over another. A route link with a lower number will be chosen over one with a higher number.
- **Interface:** This 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 Routes:** A local route is a route that is not shared between neighboring routers. (Local static routes only apply to the current system.)
- **Common Static Routes:** A common route is a route that is shared between neighboring routers.

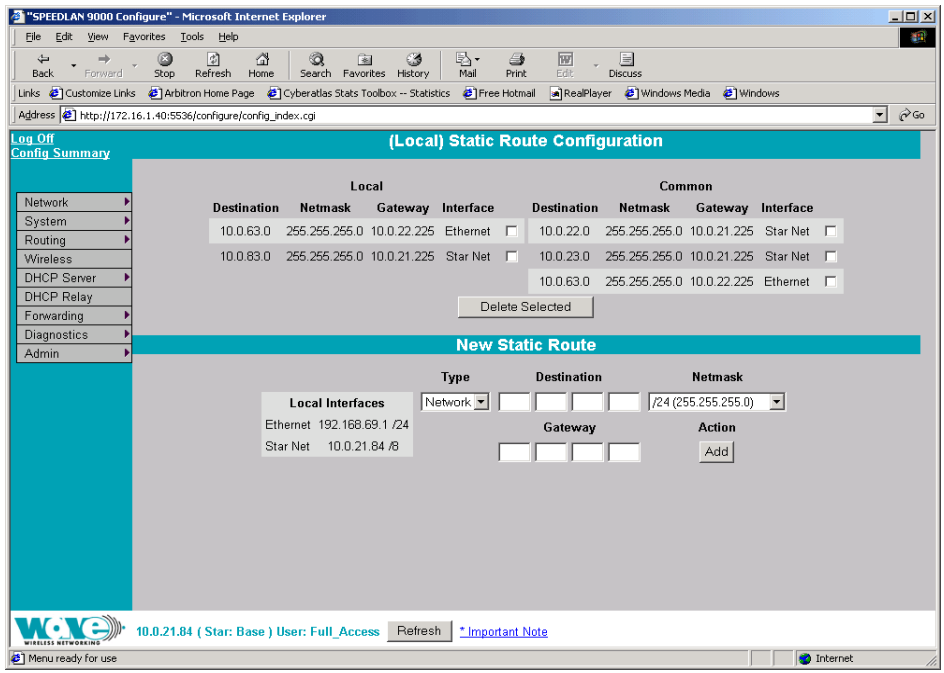


Figure 3-29: Local Static Route page

(Common static routes apply to multiple routers and propagate updates to other routers.)

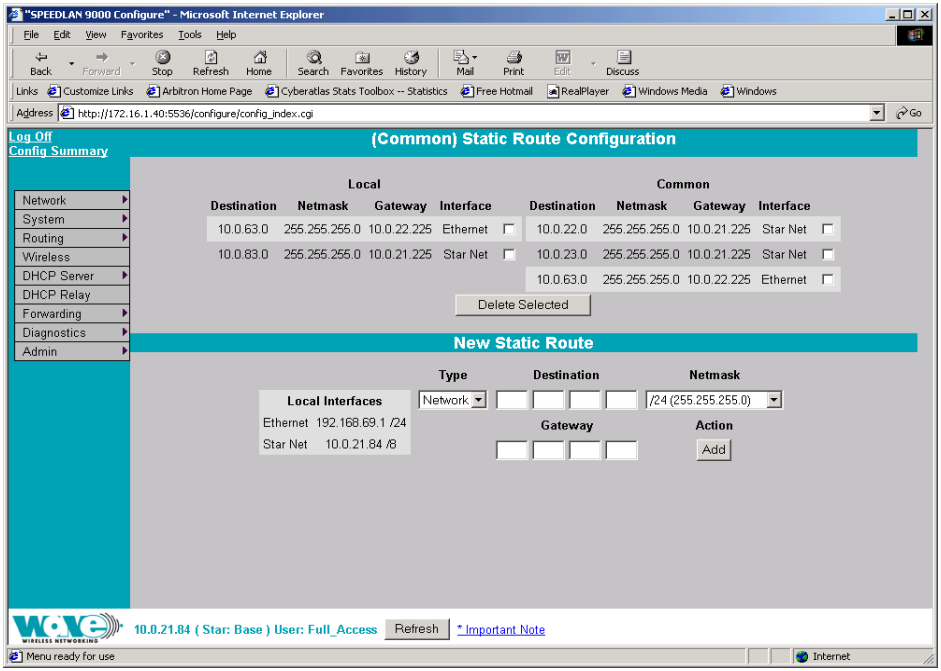


Figure 3-30: Common Static Route page

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

Near the top of the page you will see a dynamic list about local and common static routes.

Near the middle of the page 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 CIDR 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 3-22*.
- **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 **Network** 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.

  Note: If you do not want to use a current static route, select the routes you want to remove and click **Delete Selected**. To add a new static route, click **Add.**

DHCP Server Menu

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 the 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.

Servers that utilize DHCP resolve security issues, costly IP addressing services, and compatibility problems. DHCP is a superset 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 3-40*.

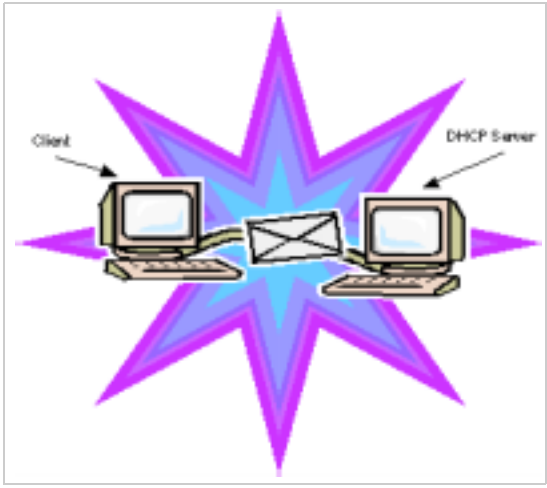


Figure 3-31: DHCP client and server

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 the client.
3 The client takes the IP address from DHCP server and requests for additional configuration that is 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

Important Notes:

- The DHCP server and DHCP client are only available for Ethernet (wired) interfaces.
- The DHCP server can only be configured to serve IP addresses on the subnet where its Ethernet IP address resides.

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. (For definitions, see *General DHCP Elements Defined, page 3-44*.)

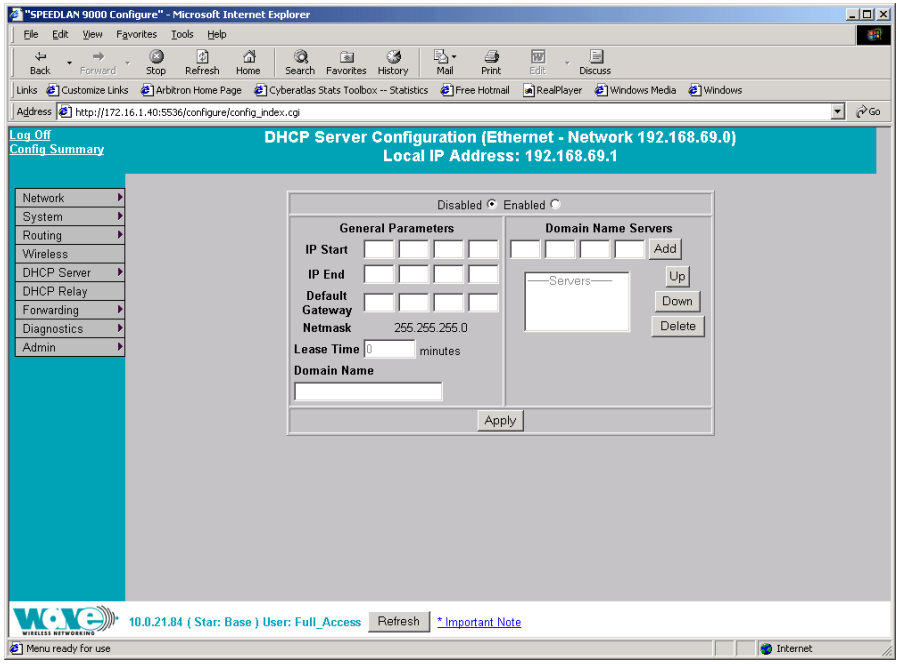


Figure 3-32: DHCP General Clients

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 (screen shot located after this step). This page is shown in Figure 3-33 on page 3-42 (for definitions, see *Known Clients Elements Defined, page 3-46*).

b) This is where you can then specify the computer name or MAC address and the corresponding IP address that should be assigned to that device at all times.

DHCP can be configured on only the Ethernet interface, easing the administrator overhead when adding new computers or SPEEDLAN 9000 routers.

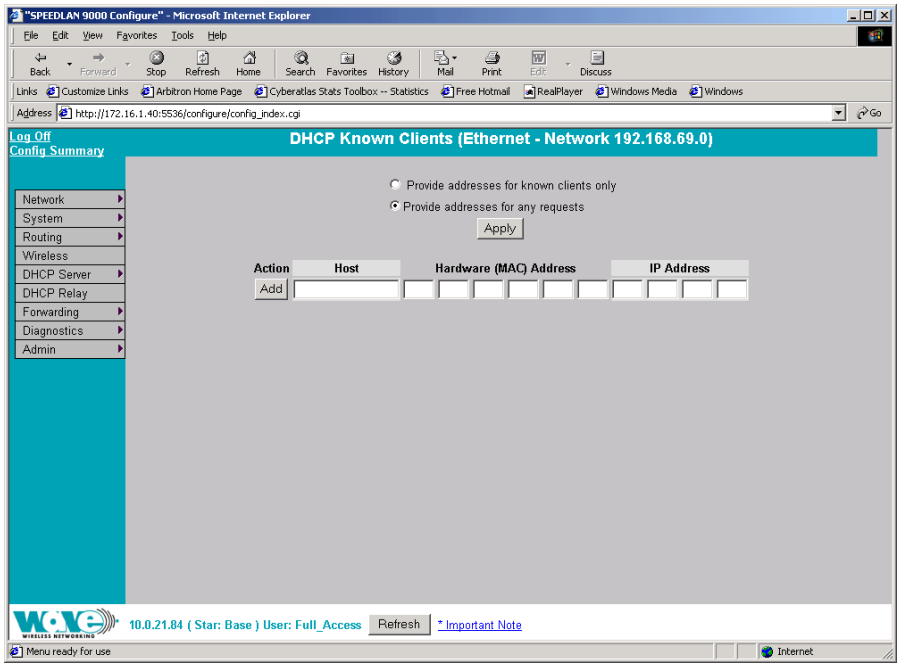


Figure 3-33: DHCP Known Clients page

c) If your DHCP server is a machine separate from the SPEEDLAN 9000 routers, you will need to set up DHCP Relay (by choosing **DHCP Relay** from the main menu). This page is shown in *DHCP Relay Configuration page, page 3-43* (for definitions, see *DHCP Relay Menu, page 3-47*).

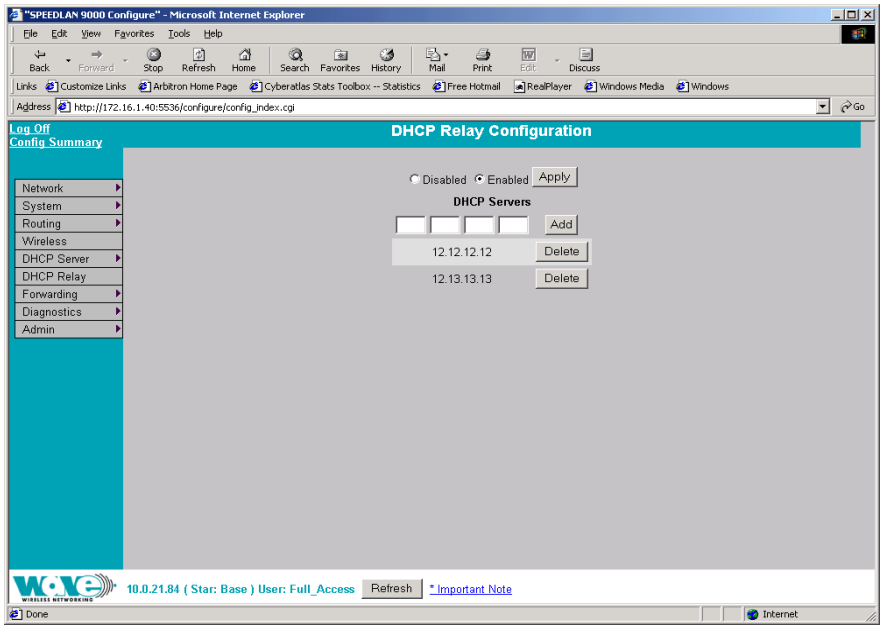


Figure 3-34: DHCP Relay Configuration page

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

e) Next, you need to enable the Ethernet interface. Next, enter the IP address of the DHCP server that is offering IPs to clients.

f) Once you have set up the SPEEDLAN 9000 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 routers, 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 3-40*.

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.

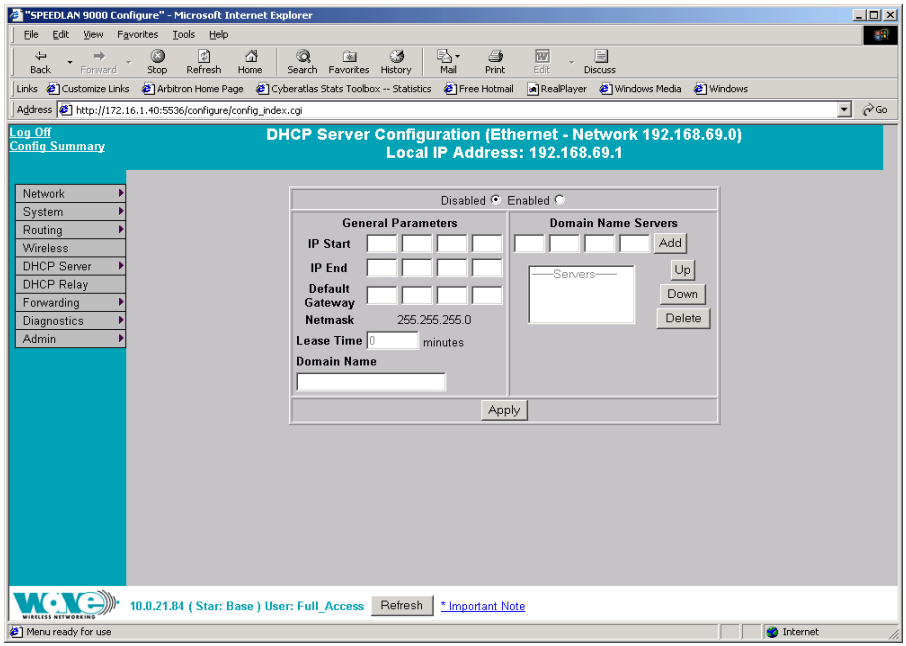


Figure 3-35: DHCP General page

- **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 addresses.
- **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. (Entering "0" means the lease time never expires.)
- **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 it (from highest to lowest).
  - If you want to remove any of the DNS parameters, click **Delete**.

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 **Apply**.

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.

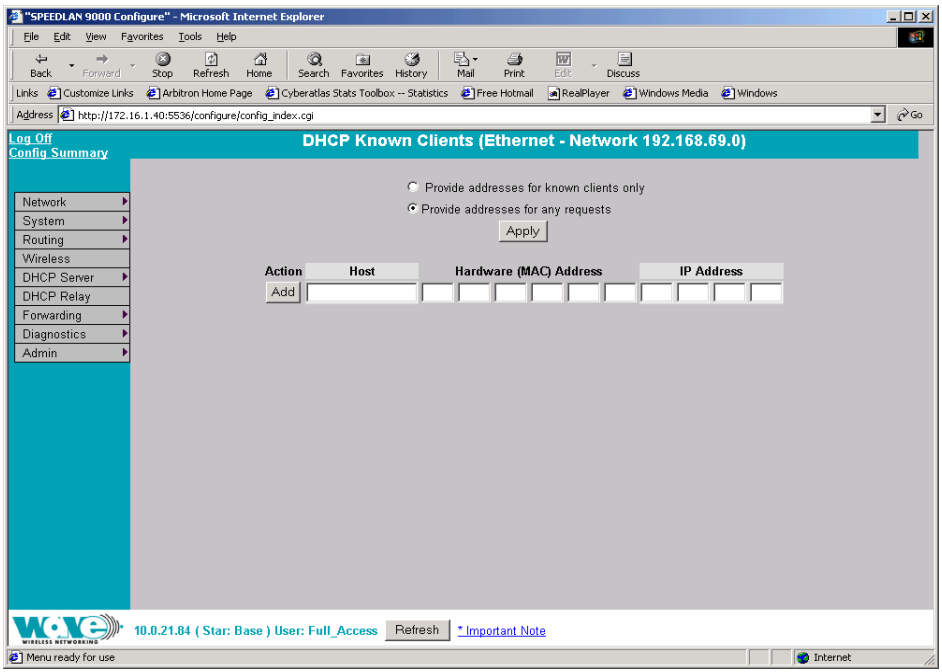


Figure 3-36: DHCP Known Clients page

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 **Apply** 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. Timestamps are also reported in client time. Timestamps track the date and time for each event in the log.

Status

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

DHCP Relay Menu

This section defines the elements described a few pages back in the section, called *Basic Instructions for Setting Up DHCP on an Interface, page 3-40*.

DHCP Relay allows you to configure the SPEEDLAN 9000 to relay (forward) any DHCP requests originating on the Ethernet 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 interface address. If this service is enabled and the SPEEDLAN 9000 did not use DHCP to get an address for its 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.

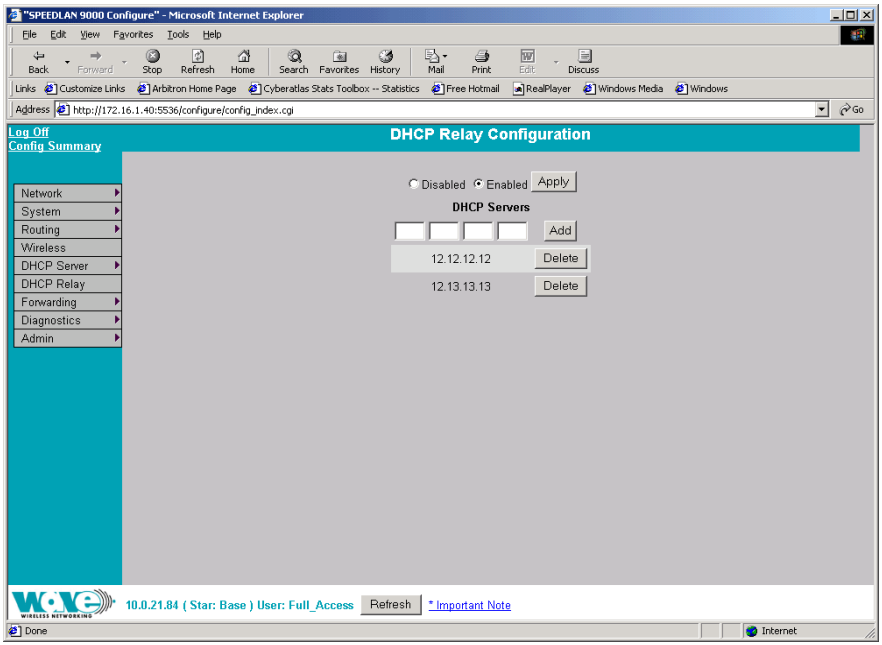


Figure 3-37: DHCP Relay Configuration page

1 To enter a new DHCP server, enter the appropriate IP address and click **Add**.

2 Click **Apply** when making changes. Click **Delete** to remove information.

Forwarding Menu

Use this menu to control how traffic is forwarded through this router. These features are available under the Forwarding menu:

- **Services** - Defines a network service (e.g., web server, FTP and email server) between the client and server nodes on your network. When you create a service, you will be allowed to forward public services inward to the internal (privately addressed) servers on your network. See *Services, page 3-49*.
- **Address Sharing** - Address Sharing uses Network Address Translation (NAT) to allow you to share public IP addresses with privately addressed network nodes in order for them to access the Internet. See *Address Sharing, page 3-56*.

- **Internal Servers** - Allows an administrator to make a service available from an IP address, even though the owner of the IP address may not be actually providing the service. See *Internal Servers, page 3-58*.
- **1:1 NAT** - Allows an administrator to statically map a public IP address to the private IP address of one of the nodes on your network. This is useful when trying to preserve a limited number of IP addresses on the WAN network. See *1:1 NAT, page 3-60*.
- **Firewall** - The SPEEDLAN 9000 (via the SPEEDLAN 9000 Configurator) allows you to control incoming and outgoing traffic. A firewall prevents unauthorized access to a network. Utilizing the SPEEDLAN 9000 Configurator, SPEEDLAN 9000 routers can increase security and provide additional support to users of the network. See *Firewall, page 3-61*.
- **IP Sessions** - The SPEEDLAN 9000 firewall offers stateful packet filtering. IP Sessions allows you to view sessions whose state is currently active. See *IP Sessions, page 3-66*.

Services

Network "Services" describe specific sessions between clients and servers, servers and servers, or clients and clients on your network. Examples of servers that provide services are web servers, FTP servers and email servers. Service definitions allow you to forward public services inward to the internal (privately addressed) servers on your network.

Note: You can also choose to allow or deny such services between networks or individual nodes in the firewall section. For more information, see *Firewall, page 3-61*.

To use the Services feature, choose **Services** from the **Forwarding** menu. The following page will appear:

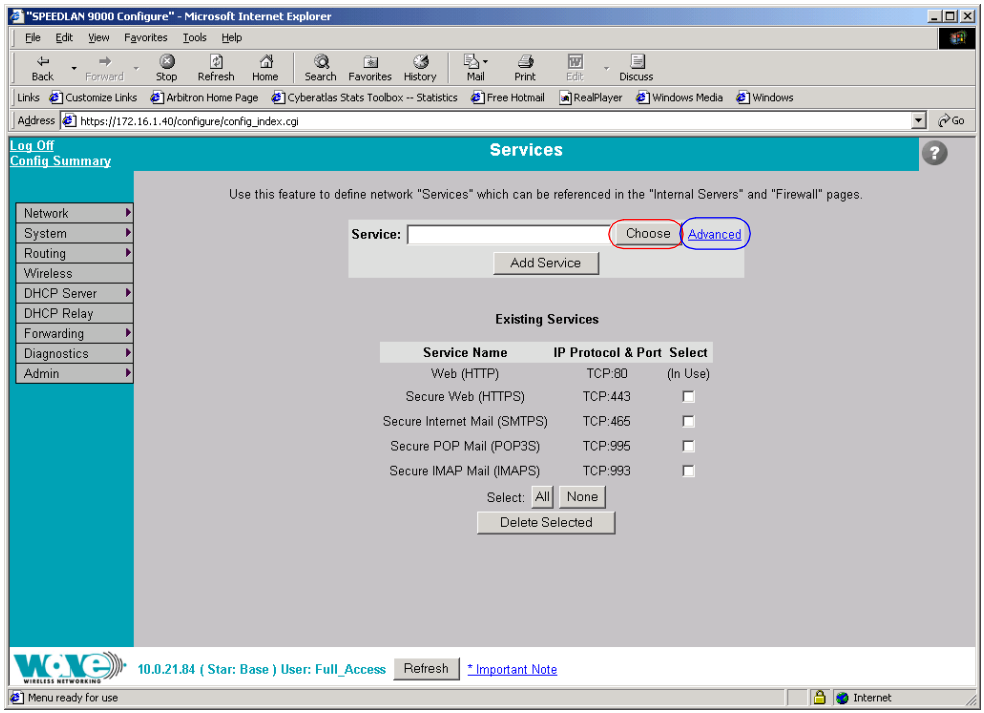


Figure 3-38: Services page

To enter a service, do the following:

1 To display a service in the Service text box, you must click the **Choose** button to select a service (circled in red in the previous figure). The service describes the specific sessions between client and server nodes on your network (e.g., web servers, FTP servers and email servers).

2 The following pop-up will appear, which lists the known services.

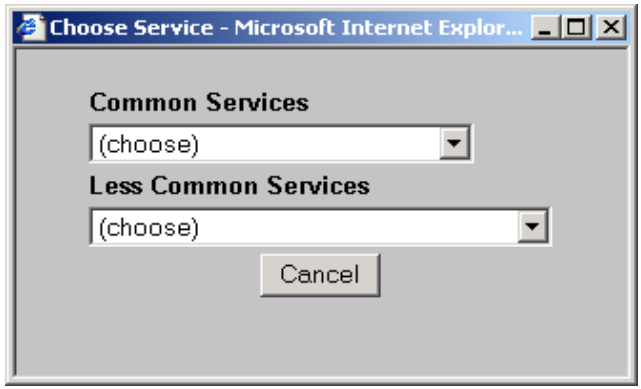


Figure 3-39: Choose Service

3 Select one of the following:

- **Common Services:** This list contains the most common type of network services. (Note: SPEEDView is also listed under this list. It simply lets the user allow SPEEDView access when the firewall is enabled.) Select the appropriate service from this drop-down list. Then, click the **Add Service** button on the Services page.
- **Less Common Services:** This list contains less common types of network services. Select the appropriate service from this drop-down list. Your selection will be added to the Services page. Then, click the **Add Service** button on the Services page.

Creating an Advanced Service

If you cannot locate the service you want to add, you can define an advanced service by clicking the **Advanced** link to the right of the Choose button (as circled in blue in Figure 3-38 on page 50). The following pop-up will appear:

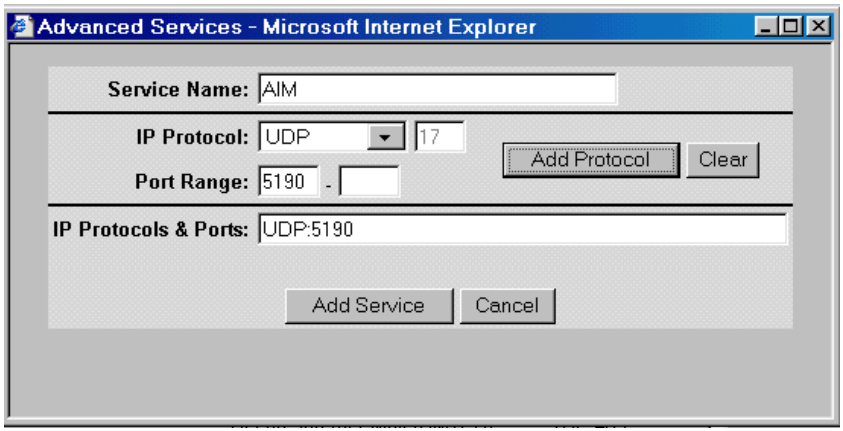


Figure 3-40: Advanced Services (adding AIM)

Advanced services can have one or more IP protocols. **Under Advanced Services, you will need to know the name of the service (or it can be unique), the protocol(s) used and the ports needed to operate the service.** For the TCP and UDP protocols, you can define specific ports, or a range of ports. Enter the following information:

1. **Service Name**: Enter a new name for the service. (In the previous figure, the user entered "AIM" because the user wanted to add AOL Instant Messenger.)
2. **IP Protocol**: Select an IP protocol for your service. If you select any protocol other than TCP or UDP, the protocol will be immediately added to the list of protocols for this service. (In previous figure, the user selected "UDP" because it is the protocol for AIM.)
3. **Port range**: If you select TCP or UDP, you can specify a port or a port range. Then, click **Add Protocol** to add that protocol and port to the list. Click **Clear** to remove the IP protocol list if you need to start over. (In the previous figure, the user entered port "5190".) If you are only entering a single port, enter it in the left **Port Range** text box.
4. **IP Protocols and Ports**: After clicking **Add Protocol**, this text box will be populated with the data, based on what you entered in the IP Protocol, Port number and Port range text boxes.

5 Click **Add Service** to add the service to the Existing Services list on the Services page. (In the next figure, you can see the user's new service, "AIM", circled in red.)

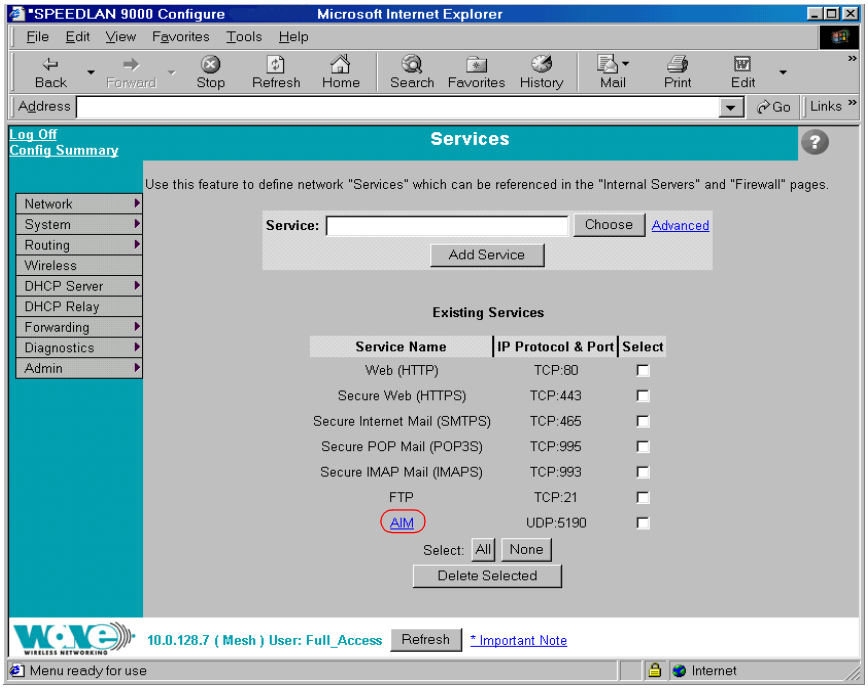


Figure 3-41: New service added to existing services list

Existing Services

The Existing Services list shows all defined services.

- **Service Name:** The name of the service.
- **IP Protocol:** The IP protocol by which data sent from one network node to another is classified (e.g., TCP, UDP, ICMP, OSPF).
- **Port:** A number used in the TCP and UDP protocols to differentiate streams. The number is included in the transmitted packets to link the incoming data to the correct service (e.g., port 80 is used for HTTP).

Note: To remove a service, select its check box and click **Delete Selected**. Click **All** to select all of the existing services. Click **None** to clear all selections. If an entry has (In Use) instead of a check box, this means the service is in use and cannot be removed.

Three Features of NAT

NAT Background Info

Network Address Translation (NAT) occurs when there is a translation from one IP address to another. There are several implementations of NAT - each with their own purpose. One would choose the type of NAT that suits the task.

The SPEEDLAN 9000 offers 3 features that use NAT: Address Sharing, Internal Servers and 1:1 NAT. Each is described below.

1. **Address Sharing:** This feature allows an administrator to share a public IP address with privately addressed nodes. Typically, this is used to allow outbound connections to the Internet from hosts who do not have IP addresses that can be reached from the Internet. In implementing Address Sharing, requests to the Internet would be directed to the SPEEDLAN 9000. The SPEEDLAN 9000 would then translate the source address and port to one of its own, and then forward the request on to its destination. The destination server would return the request to the SPEEDLAN 9000, which would consult its NAT table, determine which host made the request, change the destination address and port, and return the completed request. Similar to Internal Servers, this process also creates the Network Address and Port Translations (NAPT). Address sharing is possible when units need to act only as clients and do not need to respond to requests. This is a useful feature if you have a limited number of public IP addresses. You can use this feature to connect the whole LAN to the Internet using just one public IP address. Here are some other benefits of address sharing:

- reduce costs by using only one Internet account.
- protect your information by hiding your workstations IP addresses.
- restrict those users you want to access Internet services and resources.

The main Address Sharing page allows you to share the IP addresses assigned to the SPEEDLAN 9000's network interfaces with all nodes connected to a different network interface.

2. **Internal Servers:** This feature allows an administrator to make a service available from an IP address, even though the owner of the IP address may not be actually providing the service. Typically, this is used to allow access through a firewall to a protected server. In implementing "Internal Servers," static NAT rules are established that forward requests on a given port to a port on a server. For example, a client request to port 80 on the SPEEDLAN 9000 would be forwarded to an internal web server on port 80. The web server would then handle the request and return to the client via the SPEEDLAN 9000 router. To the client, it would appear that the reply came from the external address.

3. **1:1 NAT:** This feature allows an administrator to statically map a public IP address to the private IP address of one of the nodes on the network. This is useful when trying to preserve a limited number of public IP addresses on the WAN network. Otherwise, you may be forced to split a public network into two smaller networks and incur the penalty of network and broadcast IP address for both of the new networks. All traffic, regardless of protocol or port, is translated from the external address to the internal address.

For example, a client request to any port on the "advertised" IP address would be forwarded to the IP address of the server. The server would then handle the request and return to the client the requested data. To the client, it would appear that the reply came from the external address. This is also referred to as Static NAT.

Address Sharing

To share a public IP address with other computers, choose **Address Sharing** from the **Forwarding** menu. The following page will appear:

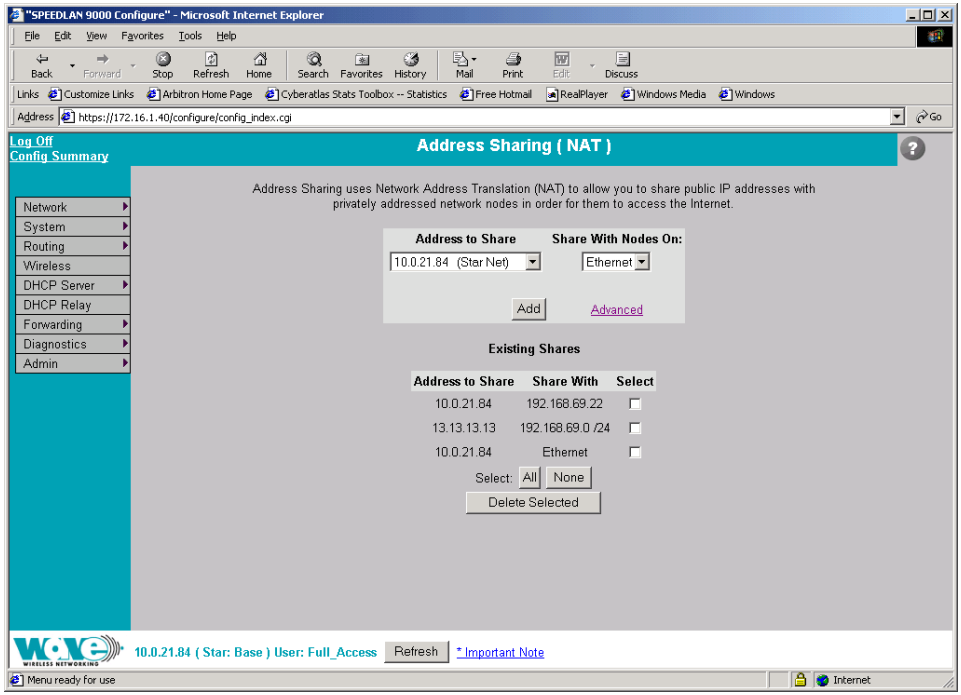


Figure 3-42: Address Sharing page

The elements on this page are described below:

If you want to share an IP address assigned to the wireless or wired network interfaces, select the address from the **Address to Share** list. (In the previous figure, the user entered "10.0.21.84"). The "Share With Nodes" will automatically be selected (for the Ethernet interface in this example).

Note 1: Addressing Sharing works for connections originating from a host on the "address to share" interface/network. Connections to actual IP addresses can still be made from the outside network; those connections will not use the shared address. To prevent this issue, make sure the firewall is enabled.

Note 2: If changes are made to "address sharing," connections that originated prior to these changes may still use the previous configuration. The only way to ensure this does not happen is to reboot the SPEEDLAN 9000 router.

If your WAN interface were the wireless network, you would share the wireless network interface's IP address with nodes on the Ethernet network. For more options, click on the **Advanced** link to the right of the "Add" button.

The following page will appear:

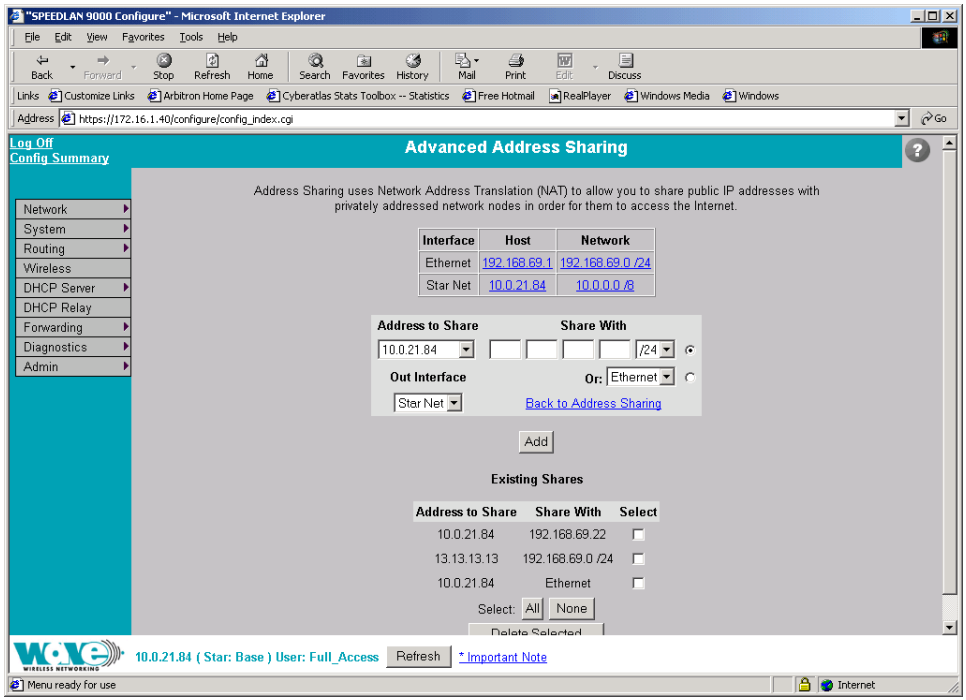


Figure 3-43: Advanced Address Sharing

Description of Advanced Address Sharing

The Address Sharing page allows you to share an address with all nodes connected to one of the SPEEDLAN 9000's network interfaces. This page allows you to narrow down the IP addresses to a specific network.

- **Interface, Host and Network:** This table lists the name of the interface, IP address of the wired and wireless host, and the IP address of the network. If you click an IP address, it will populate the **Share With** text box.

- **Address(es) to Share:** Select a virtual address from this drop-down list. You will need to select an **Out Interface** if using a virtual address from the **Address to Share** list. This tells the SPEEDLAN 9000 which interface is acting as the WAN for this operation.

- **Share With:** Do of the following:
  - enter the wired or wireless private IP address where you want the public IP address to be shared. Select a netmask that specifies a network or host (/32), or
  - select the interface that the private nodes are connected to (e.g., Ethernet).

Click **Add** to implement this setting. This will also be added to the Existing Shares list on the bottom of this page.

Note: Click the **Back To Address Sharing** link to return to the previous page.

Existing Shares

This list displays the public IP addresses that are being shared with the private IP nodes. To remove an existing share, select its check box and then click **Delete Selected**. Click **All** to select all shares. Click **None** to clear all selections.

Internal Servers

Use this feature to host public (Internet) services with internal (privately addressed) servers on your network. This allows you to offload services to multiple servers for a given public IP address. To activate this feature, choose **Internal Servers** from the **Forwarding** menu. The following page will appear:

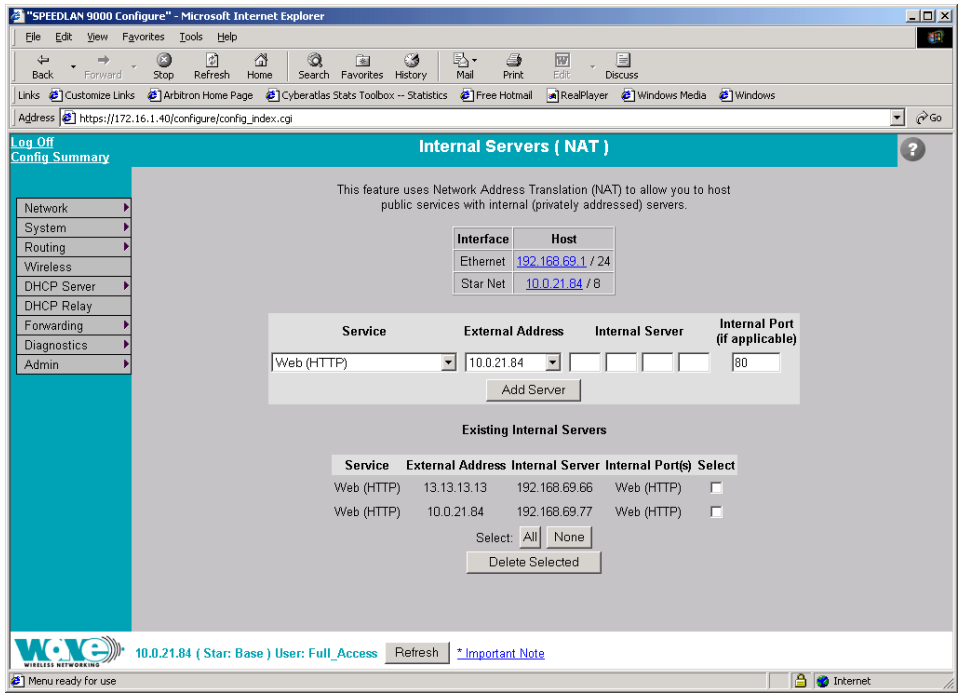


Figure 3-44: Internal Servers (NAT) page

Note: If you upgrade from version 2.x to 3.x, verify that your forwarding rules are displayed correctly on the Internal Servers page. If your forwarding rule appears as an "Unknown" service, define the service on the Services page. For more information, see *Services, page 3-49*.

The elements on this page are described below:

- **Interface and Host:** This table lists the name of the interface and host IP addresses assigned to the wired and wireless interfaces. If you click on an IP address, it will populate the **Internal Server** text box.
- **Service:** This is the network service (e.g., HTTP, FTP, etc.) that is provided to the client. The current services are displayed in the Existing Internal Servers list on the bottom of this page. (**Note:** If you want to add to the list of services, choose **Services** from the **Forwarding** menu. Then, follow the directions for *Services, page 3-49*.)
- **External Address:** Select the IP address where the service will be hosted.

- **Internal Server**: Enter the IP address of the computer on the network that will host the service.
- **Internal Port (if applicable)**: If the port is different than the standard for that service, enter it here.

When finished making changes, click **Add Server**. This will add the server to the existing internal servers list. If the service has multiple TCP or UDP ports defined, a pop up will appear allowing you to map these to ports on the internal server.

Existing Internal Servers

To remove an internal server, select its check box and click **Delete Selected**. Click **Select All** to select all of the existing internal services. Click **None** to clear all selections.

1:1 NAT

To access 1:1 NAT settings, choose **1:1 NAT** from the **Forwarding** menu. The following page will appear:

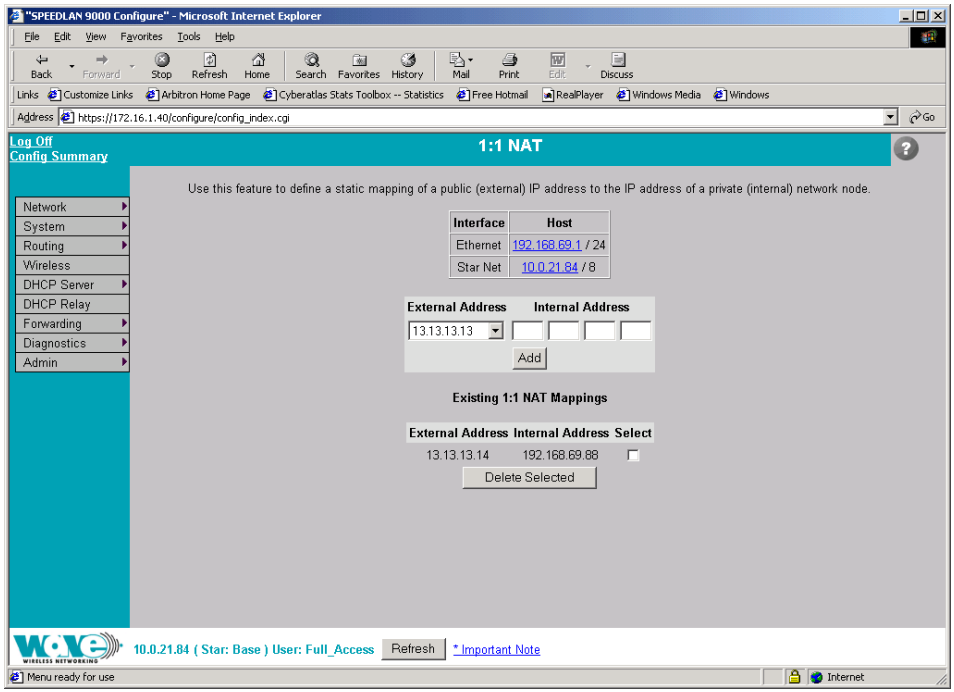


Figure 3-45: 1:1 NAT page

Make sure you define at least one virtual address prior to using 1:1 NAT. To define a virtual address, see *Virtual Addresses, page 3-24*.

The elements on this page are described below:

- **Interface and Host:** This table lists the name of the interface and host IP addresses assigned to the wired and wireless interfaces.
- **External Address:** This lists the IP address on the "outside" network. (In the previous figure, the user entered "13.13.13.14" for the virtual address.)
- **Internal Address:** Enter the IP address for the inside or private network. This address "hides" behind the public IP address you selected. (In the previous figure, the user entered "192.168.69.88" for the internal IP address.)

Existing 1:1 NAT Mappings

To remove a 1:1 NAT mapping, select its check box and click **Delete Selected**. Click **All** to select all 1:1 NAT mappings. Click **None** to clear all selections.

Firewall

The SPEEDLAN 9000 (via the SPEEDLAN 9000 Configurator) allows you to control incoming and outgoing traffic.

A firewall prevents unauthorized access to a network. Utilizing the SPEEDLAN 9000 Configurator, SPEEDLAN 9000 routers can increase security and provide additional support to the users of the network. In addition, it may help prevent dangerous packets from intruding on a network that contains sensitive data. It does this by analyzing the network traffic that is permitted or not permitted to enter the firewall based on pre-established rules.

The firewall contains a checklist, and it filters traffic that enters and exits the firewall based on the rules you set (e.g., allowing or denying certain source/destination combinations). When traffic passes through the firewall, the firewall starts at the top of its checklist and looks for the rule that matches its criteria. Traffic that meets the criteria in the checklist will be permitted, and traffic that does not meet the criteria in the checklist will be blocked. This feature allows you to restrict specific network packets from entering or leaving your network.

Tips on Creating Rules for Your Firewall

Before you create a rule, make sure you:

- Understand the purpose of the rule. For example, will this rule block all IRC traffic from the LAN to the Internet? Will this rule allow a remote mail server to send data at the same time over the Internet to an internal mail server?
- Do you want the firewall to allow or deny certain traffic? What type of traffic? What type of IP protocol?
- What is the direction of the traffic: from the Internet to the LAN or from the LAN to the Internet?
- What IP services will this rule affect?
- Which nodes (or workstations) on the LAN will these rules affect? Make a mental note of the IP address (those on the private and public LANs) that these rules will affect.
- Consider the security of the network. For example, once you enable this rule, which areas of the network will become more vulnerable?
- Will this rule override any other rules you created?

To control traffic flow through the router, choose **Firewall** from the **Forwarding** menu. The following page will appear:

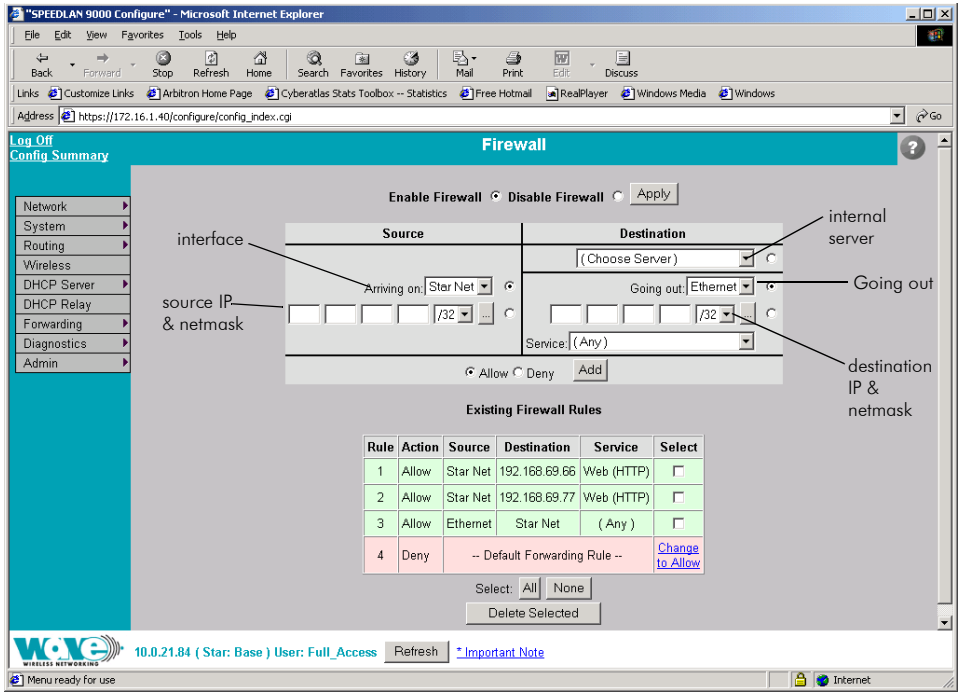


Figure 3-46: Firewall page

Note: When DHCP relay is enabled, it may appear as if DHCP requests get through the firewall when they are not explicitly allowed. The reason for this is that DHCP requests come in as link layer broadcasts (which are not filtered by the firewall) and then the relay server unicasts from the SPEEDLAN 9000 router to the ultimate DHCP server. These unicasts originate from the SPEEDLAN 9000 and thus are not considered to be "forwarded" by the firewall. Turning off DHCP relay stops this behavior.

The elements on this page are explained below:

- **Enable Firewall:** Select the **Enable Firewall** option to activate the firewall feature.
- **Disable Firewall:** Select the **Disable Firewall** option to disable the firewall feature. Click **Apply** to activate the option you selected.

Source Section

Arriving on: Select one of the following:

- the interface or
- the IP address/netmask. Then, enter the IP address for the source and select the netmask.

Note: If you click the "…" button, the physical addresses of the interfaces will be displayed.

Destination Section

Select one of the following:

- **Internal Servers:** If there are any internal servers defined on this SPEEDLAN 9000, you can choose one as the destination in a rule. If there are no internal servers defined, this combo box will be disabled and you can click on the **Define one** link to create an internal server.
- **Going Out:** Select one of the following: the interface for the destination or the IP address/netmask. Then, enter the IP address for the destination and select the netmask.
- **Service:** Select the name of the service if this rule applies to a single service. This is the network service (e.g., HTTP, FTP, etc.) that is provided to the client.

Allow or Deny Action

Select one of the following:

- **Allow:** Select the **Allow** option to enable that traffic through the firewall.
- **Deny:** Select the **Deny** option to block that traffic through the firewall.
- **Add:** Click this button to add this rule to the Existing Firewall Rules list.

Existing Firewall Rules

This lists the existing firewall rules, and the firewall will run through the checklist as explained in the introduction. To remove a firewall rule from the list select its check box and click **Delete Selected**. Click **All** to select all firewall rules. Click **None** to clear all selections. To change the Default Forwarding Rule, click the link that either says, "**Change to Allow**" or "**Change to Deny**".

Note: Once you have finished configuring your firewall, reboot the SPEEDLAN 9000 router. This will terminate any undesired connections that may have existed prior to the firewall configuration. You can verify if such undesired connections exist by opening the IP Sessions page, which is last function under the Forwarding menu. For more information, see *IP Sessions, page 3-66*.

Special Rules for Virtual Addresses

When you create a firewall rule that references a 1:1 NAT mapping or an internal service using a virtual address, you must specify the internal address as the destination. This is important to know because the virtual addresses have already been translated to their defined internal addresses before the firewall examines the packet's destination.

Tutorial: What is happening in this firewall rule set?

As previously explained, a rule set tells the firewall what it can do. The rule set checklist follows the top-down concept. The first row takes priority, and then follows the second row's criteria, followed by the third, and so on.

Can you explain what is happening in the example below?

Existing Firewall Rules

Rule	Action	Source	Destination	Service	Select
1	Allow	Star Net	172.16.70.245	FTP	☐
2	Allow	Star Net	192.168.69.66	Web (HTTP)	☐
3	Allow	Star Net	Ethernet	Internet Mail (SMTP)	☐
4	Allow	Star Net	Ethernet	Bootps	☐
5	Allow	Star Net	Ethernet	Bootpc	☐
6	Allow	Star Net	Ethernet	AIM	☐
7	Allow	Ethernet	Star Net	(Any)	☐
8	Deny	-- Default Forwarding Rule --			Change to Allow

Figure 3-47: Example of Firewall Rules

The explanation:

Rule 1 (FTP server): This rule will allow incoming traffic coming from the Star Net interface to enter the firewall and go to the FTP server on 172.16.70.245.

Rule 2 (Web server): This rule will allow incoming traffic coming from the Star Net interface to enter the firewall and go to the web server on 192.168.69.66.

Rule 3 (Mail server): This rule will allow incoming traffic from the Star Net interface to enter the Internet mail server on the Ethernet interface.

Note about DHCP Rules 4 and 5: DHCP spans both rules 4 and 5. These rules allow DHCP requests to a DHCP server from the Star Net interface to enter the firewall. The Bootps service support server requests, and the Bootpc service provides client support for DHCP.

Rule 4 (DHCP request): This rule allows DHCP requests to a server.

Rule 5 (DHCP reply): This rule allows replies to a client.

Rule 6 (AOL Instant Messenger: AIM): This rule will allow incoming traffic from the Star Net interface to enter the firewall so clients can run AOL Instant Messenger.

Rule 7 (Anywhere): This rule will allow traffic coming from the Ethernet interface to go through the firewall via the Star Net interface. The intention is to go anywhere on the internet or the network).

Rule 8 (Deny incoming traffic): This rule will tell the firewall to deny other incoming traffic. The firewall will not allow any incoming traffic to go through the firewall.

IP Sessions

The SPEEDLAN 9000 firewall offers stateful packet filtering. IP Sessions allows you to view sessions whose state is currently active. Choose **IP Sessions** from the **Forwarding** menu. The following page will appear:

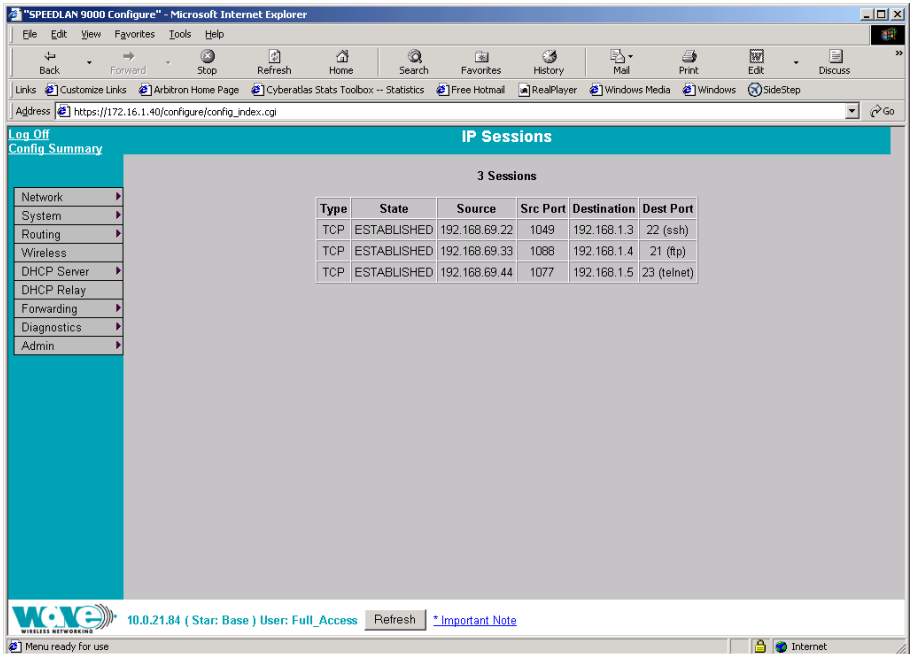


Figure 3-48: IP Sessions

This list includes IP sessions terminating or originating on this router, as well as any forwarded sessions. It is recommended that you open the IP Sessions page after you alter any firewall rules to verify that all sessions comply with the new rules. Existing sessions that are not allowed by the new firewall rules will be terminated. You must reboot the router to remove these types of sessions, or wait for them to finish.

Diagnostics Menu (Troubleshooting the Network)

Choose **Diagnostics** to troubleshoot network problems.

- Choose **Statistics** under the Diagnostics menu to view information about inbound and outbound traffic for the interfaces (or routers).
- Choose **ARP Table** to locate systems on the LAN that are configured with incorrect IP addresses.

- Choose **ICMP Stats** to view ICMP messages and errors between the host servers and gateways.

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 8-14*. You can also perform a ping test if need. For more information, see *Performing a Ping Test, page 8-15*.

Interface Statistics

The Interface Statistics menu lists the current available network interfaces. To view the statistics of an interface, choose **Statistics** from the **Diagnostics** menu. The following page will appear.

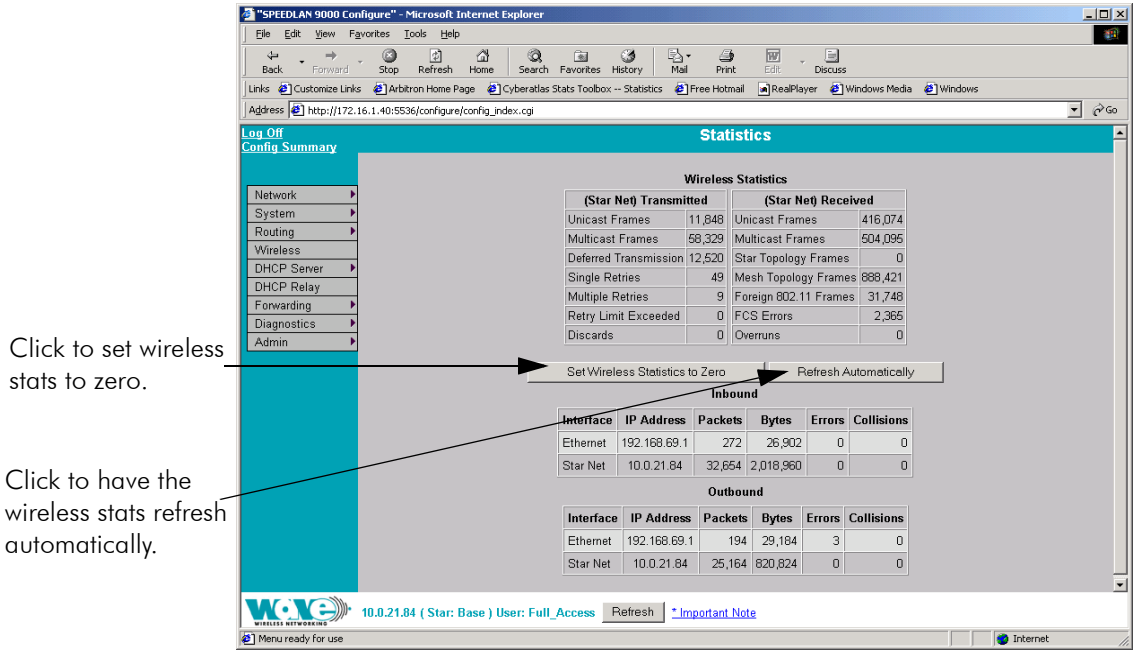


Figure 3-49: Interface Statistics page

Wireless Statistics

Transmitted

- **Unicast Frames**: Total number of unicast frames transmitted.
- **Multicast Frames**: Total number of multicast frames transmitted.
- **Deferred Transmission**: Total number of frames for which one or more transmission attempt(s) was deferred to avoid a collision.
- **Single Retries**: Total number of frames successfully transmitted after one (and only one) retransmission.
- **Multiple Retries**: Total number of frames successfully transmitted after more than one retransmission.
- **Retry Limit Exceeded**: Total number of frames not transmitted successfully because the retry limit was reached.
- **Discards**: Total number of frames discarded to free up buffer space.

Received

- **Unicast Frames**: Total number of unicast frames received.
- **Multicast Frames**: Total number of multicast frames received.
- **Star Topology Frames**: Total number of star topology frames received.
- **Mesh Topology Frames**: Total number of mesh topology frames received.
- **Foreign 802.11 Frames**: Total number of 802.11 frames received.
- **FCS Errors**: Total number of frames considered to be destined for this station, but received with an FCS error.
- **Overruns**: Total number of frames discarded to free up buffer space.

Inbound & Outbound

Refer to the definitions below for traffic moving inbound or outbound, depending on the direction of movement. Each inbound and outbound statistic is defined below:

- **Interface**: The interface on which this entry is effective.
- **IP address**: This address tells the network how to locate the computers or network equipment connected to it.
- **Packets**: A unit of data transmitted between a receiver and a sender. Each packet contains embedded information, as well as a place to go on the network (known as the IP address).
- **Bytes**: The length of the packet.

- **Errors:** The number of packets that did not reach their destination due to an error.
- **Collisions:** The number of packets that did not reach their destination because two network nodes tried to transmit at the same time.

Note: The statistics are refreshed every time you refresh the web page.

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. This helps diagnose MAC addresses that your router knows about.

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

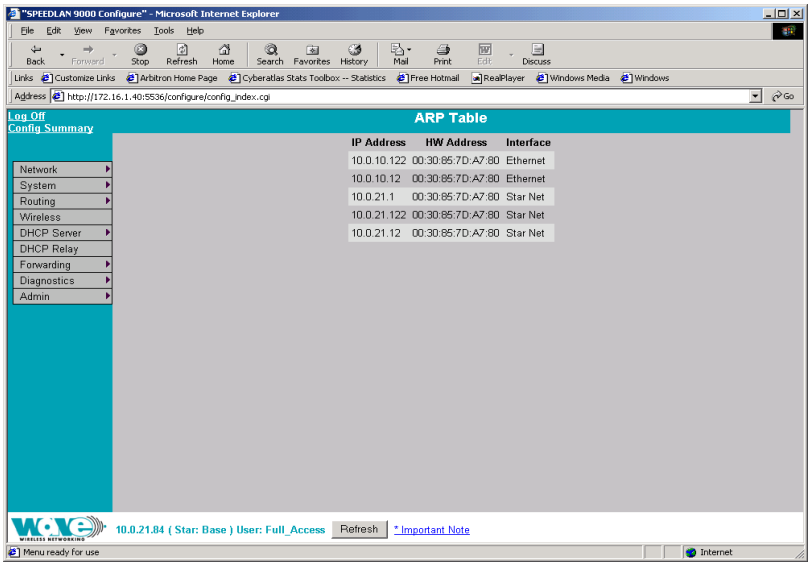


Figure 3-50: ARP page

The ARP statistics are defined below:

- **IP address:** The IP address corresponding to the media-dependent 'physical' MAC address.

- **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. The ICMP stats can be used to diagnose a connectivity problem. If you are trying to ping a router and you're not getting a response, you can check the "InMsgs" to see if the ping arrived at the router and just could not get back. This might indicate that the router has no route back to the originator.

To view ICMP information, choose **ICMP Stats** from the **Diagnostics** menu. The following page will appear.

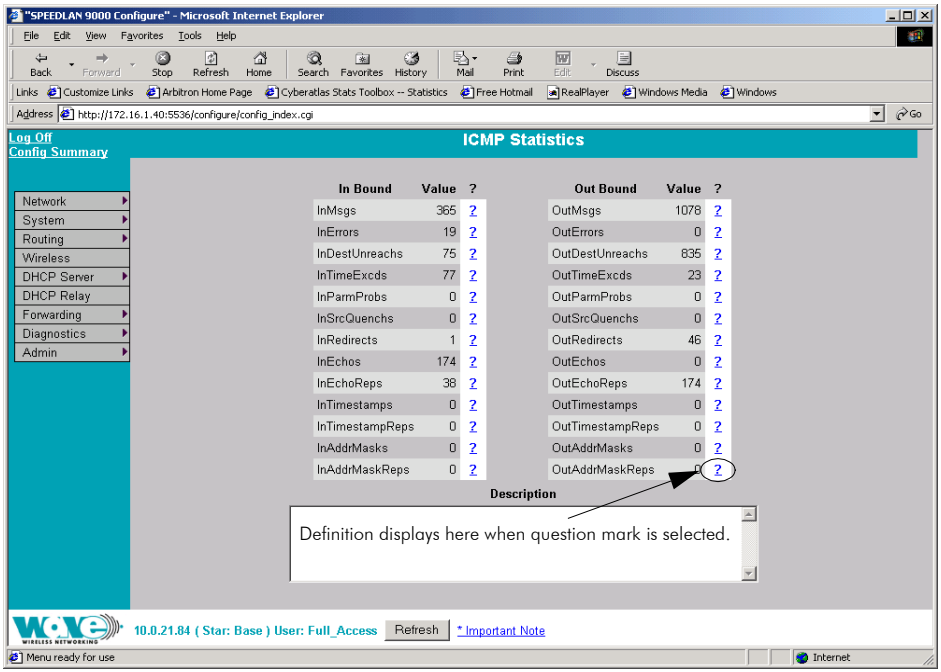


Figure 3-51: ICMP page

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.

Admin Menu

If you want to limit administrative rights to certain users, choose the **Admin** menu.

- Choose **Users** to set passwords for the type of account needed.
- Choose **Permissions** if you want to restrict certain settings to users.
- Choose **Software Update** to update the 9000 router.
- Choose **Support** to reset the entire configuration of the SPEEDLAN 9000 factory default settings, enable manufacturer access to the router for advanced troubleshooting, and enable/disable communication with SPEEDSignal.
- Choose **Current Sessions** from the **Admin** menu to view the status of a session or to terminate it.

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.

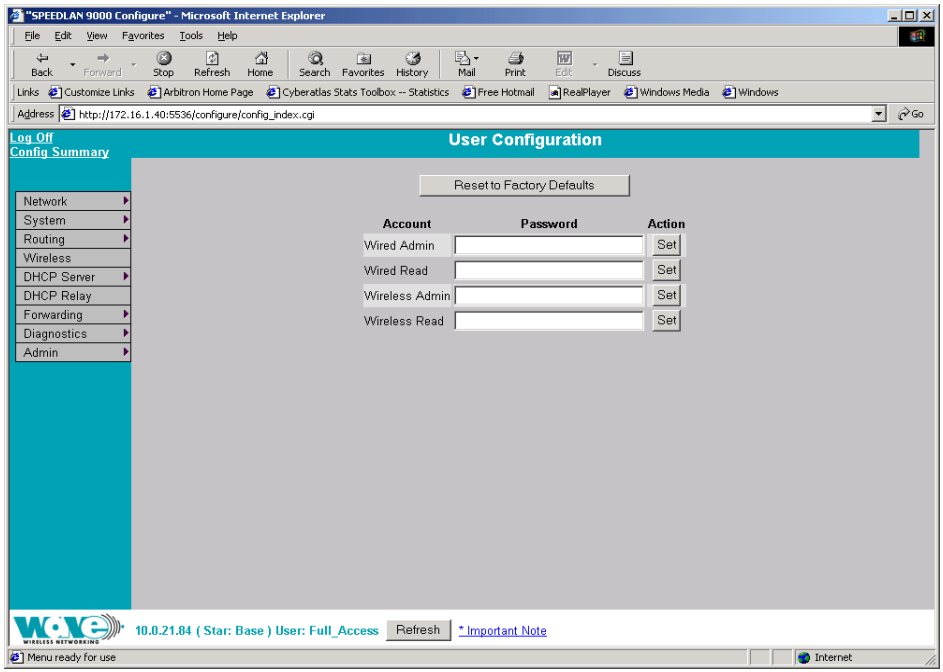


Figure 3-52: User Configuration page

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

The User Configuration page allows you to set the SPEEDLAN 9000 Configuration to 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 **Set**.

Note: The minimum password length is 8 characters. The maximum password length is 16 characters (including the underscore character or spacebar). 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 view permission configuraton for wired administrative users.
- **Wired Read**: To view permission configuration for read-only wired users.

- **Wireless Admin:** To view permission configuration for wireless administrative users.
- **Wireless Read:** To view permission configuration for wireless read-only users.

Next, the Permission Configuration page will appear.

Note: If **Full Access** appears, it allows you view permission configuration for full-access users.

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

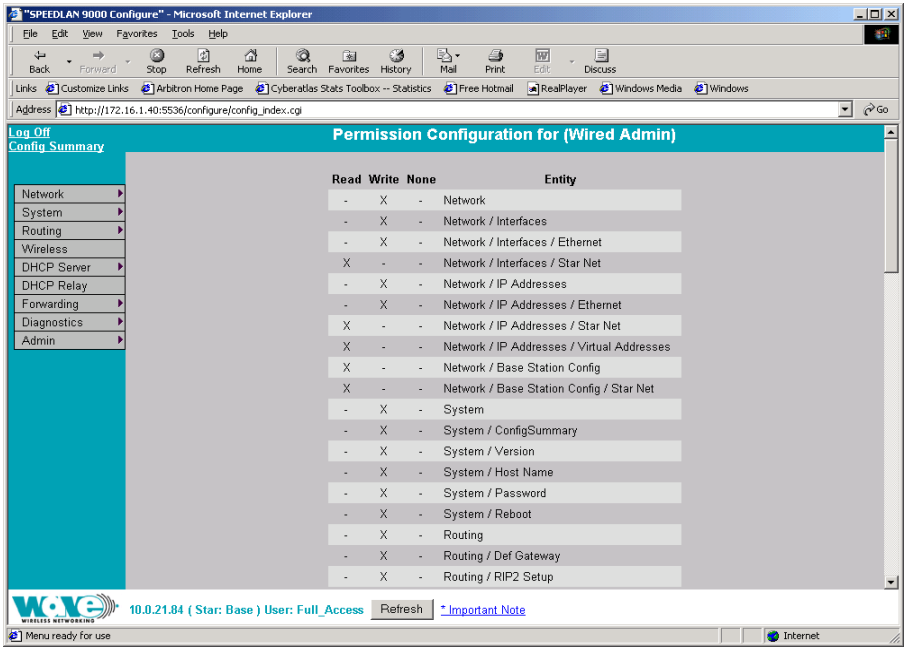


Figure 3-53: Permissions page

- **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.

Note: Be sure to click **Apply** after you made your changes.

Software Update

There are differences in updating the software on the base station compared to updating the software on the CPE (the page references are listed below).

Note: The Software Update zip file (found on the Wave Wireless web site under the Support + Firmware link) will contain a document describing the recent changes and any other additional information needed to perform the update. The zip file will also include the update (.wwn) file to perform the update.

After you have unzipped the file, make sure you extract the update file (.wwn) file to your desktop. Then, follow the directions under the Software Update section for the particular router.

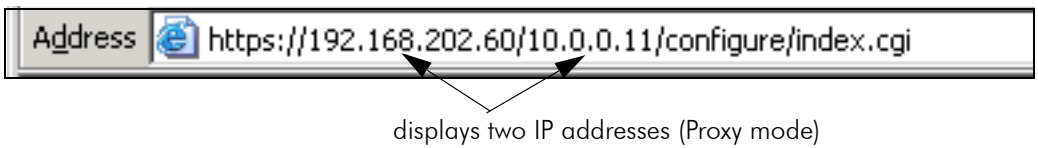
- For updating the software on a base station, see *Software Update, page 4-16*.
- For updating the software on a CPE, see *Software Update, page 5-11*.
- For updating the software on a point-to-point router, see *Software Update for Point-to-Point Primary or Secondary Routers, page 6-13* and *Updating the Software on a Local Router and Remote Router: Primary Mode Only, page 6-15*.
- For updating the software on a mesh router, see *Software Update, page 7-14*.

Proxy Mode Warning

Warning! Do not use Proxy mode when performing the update. Update from the location (host) where you are connected. If you are not directly connected, then you are proxied to another host and the update will not work. There is a limitation of proxy mode that restricts a transaction to 60 seconds. If the update takes longer than 60 seconds, which it frequently does, the update will be stopped.

How do you tell if you are directly connected to the host? Look in the Address bar on your Internet browser. If you only see one IP address in the Address bar, you are directly connected. However, if you see two IP address in the Address bar, as shown in the following figure, then you are in "Proxy" mode.

If you are not able to make a direct connection to a base in Star Mode or a primary station in point-to-point mode, then set up a static route through a CPE or secondary station in order to establish a "direct" connection.



Support

This page displays some support function features for Technical Support, Access to SPEEDSignal (for Pocket PC) and Reset to Factory Default. You can access these features by choosing **Support** from the **Admin** menu. The following page will appear:

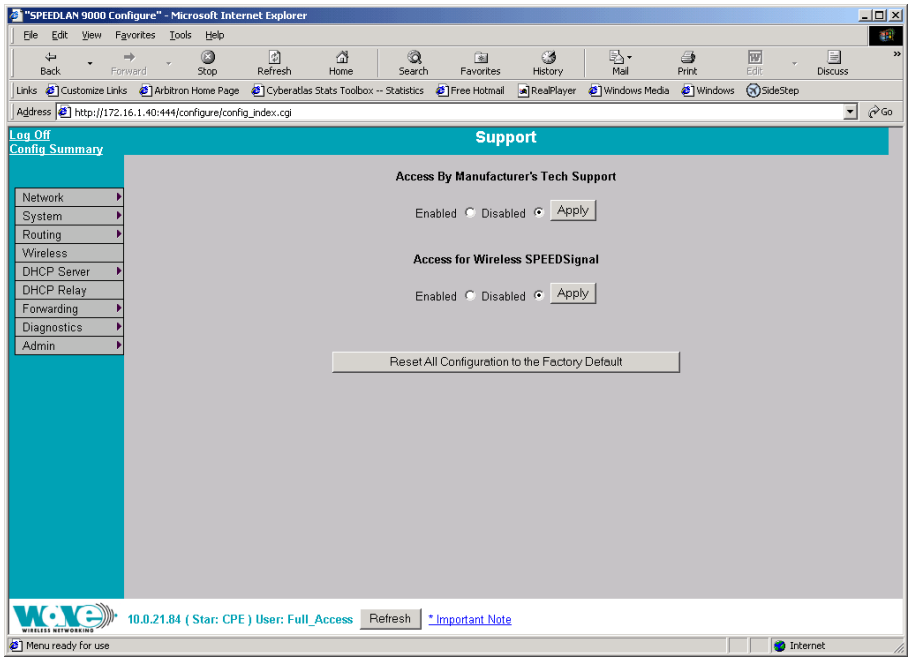


Figure 3-54: Support page

The elements on this page are explained below:

Access By Manufacturer's Tech Support

This is where you can enable the manufacturer to access the router for advanced troubleshooting (by choosing the **Enabled** option). The factory default is disabled and should remain disabled unless requested by a manufacturer's technical support representative (by choosing the **Disabled** option). Click **Apply** when finished.

Access for Wireless SPEEDSignal

This feature is used to enable or disable Pocket PC PDAs to communicate with SPEEDSignal.

- Click the **Enabled** option to enable communication with SPEEDSignal.
- Click the **Disabled** option to disable communication with SPEEDSignal. Click **Apply** when finished.

Note about upgrading SPEEDSignal: After upgrading an earlier version than 3.0, the default setting for SPEEDSignal for Pocket PC PDA is disabled. After upgrading a version greater than 3.0, the current state is maintained.

Reset to Factory Default

If you need to reset the entire configuration of the SPEEDLAN 9000 to factory default settings, click **Reset All Configuration to the Factory Default**.

Current Sessions

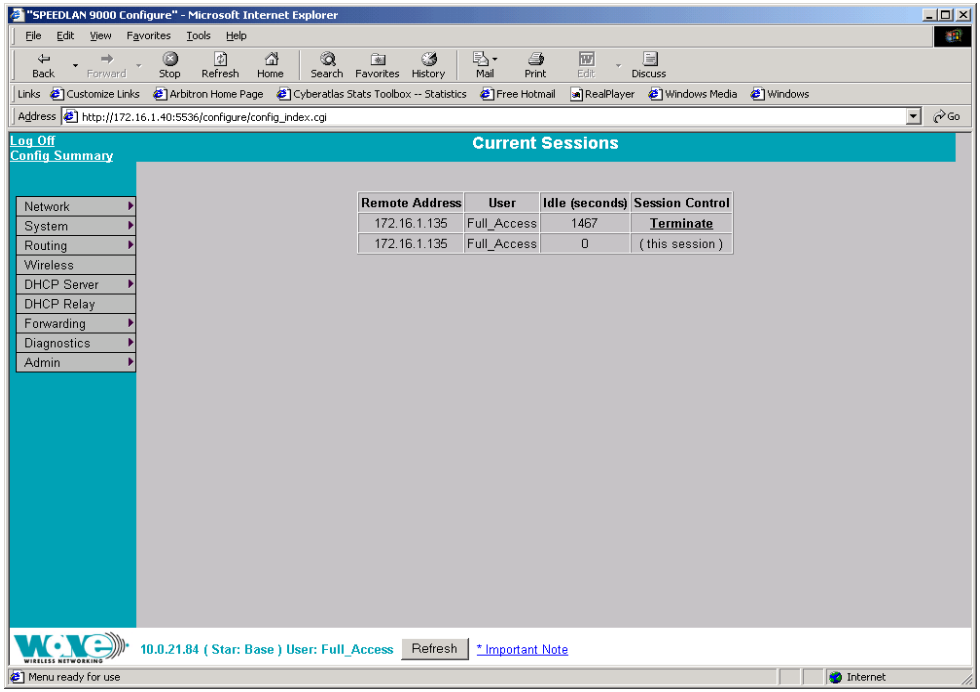


Figure 3-55: Current Sessions

Current Sessions is activated by choosing **Current Sessions** from the **Admin** menu. This page displays the active actions for the web server. It displays who is logged on and also lets you terminate the session by clicking the **Terminate** link.

Notes:

Chapter 4
Using the Configurator to Set Up Special Parameters for a Base Station

This chapter covers only those special parameters needed to set up a base station, such as:

- Network menu: *Interfaces for Base Mode, page 4-2*; *Authentication Section, page 4-4*; *Star Timing Parameters Section, page 4-7* and *Turning on Encryption, page 4-8*
- Wireless menu: *Channel and Rates, page 4-10*; *Max Tx Retries and Signaling Rate Fallback, page 4-12* and *Max Throughput (Regulating Bandwidth), page 4-14*
- Admin menu: *Software Update, page 4-16* and *Updating the Software on a Base Station and CPE, page 4-17*

All other common configuration information can be found in *General Functions of the Configurator, page 3-1*.

Network Menu

- To enter the interface (router) type and network name of the interface(s), choose **Interfaces** from the **Network** menu.
- To define what CPE routers are participating in the network, choose **Base Station Config** from the **Network** menu. If you choose this option, see *If you clicked the "System Wide Settings" button..., page 4-4* and *If you clicked Per CPE Settings Button..., page 4-8*.

Interfaces for Base Mode

The Network Interfaces page will appear when you choose **Interfaces** under the **Network** menu. This is where you enter the interface type and network name of the interface or the router.

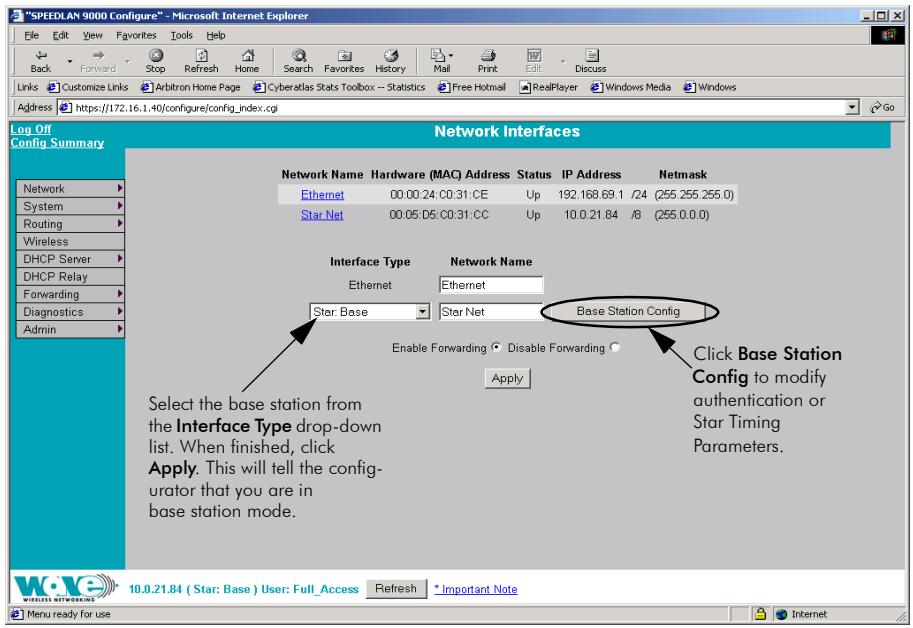


Figure 4-1: Selecting base station mode

- **Network Name:** This is the fixed or wireless interface (e.g., base station).
- **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.

- **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.
- **Interface Type:** Select the interface (e.g., base station) from this drop-down list. (This will tell the configurator that you are in base station mode.)
- **Network Name:** The type of network for the wireless or fixed router.
- **Enable Forwarding:** Select the **Enable Forwarding** option to enable the forwarding of IP packets from the wired interface to the wireless interface and vice-versa.
- **Disable Forwarding:** Select the **Disable Forwarding** option to disable the forwarding of IP packets from the wired interface to the wireless interface and vice-versa.
- **Apply:** Click after making changes.
- **Base Station Config:** Click to define what CPE routers are participating in the star network. When you click this button, a new page will appear as follows:

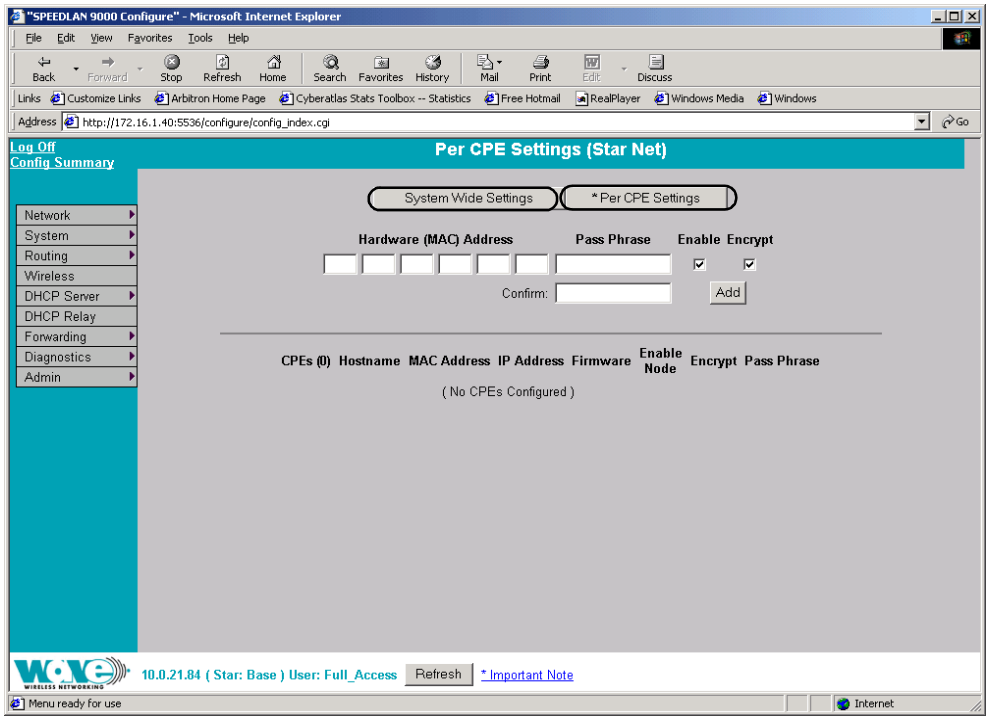


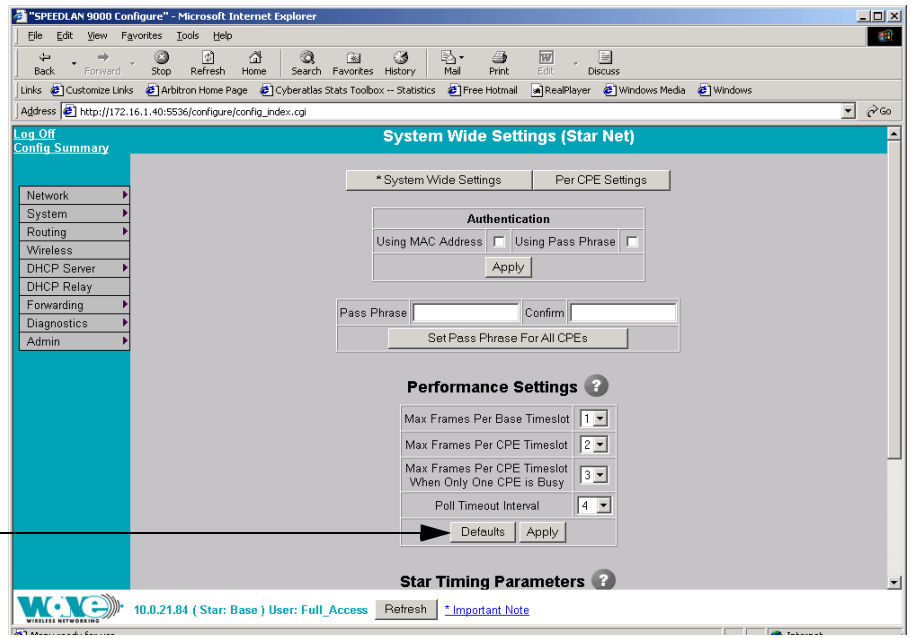
Figure 4-2: Per CPE Settings page

- Click **System Wide Settings** (left circle in Figure 4-2 on page 4-3) to set the timing parameters for the CPE routers on the star network. This will bring up a page where you can control how a base station treats CPE routers during time periods when they have no network traffic to send and set the pass phrase for all CPE routers. The following sections will be on this page:

  - See *Authentication Section, page 4-4*
  - See *Star Timing Parameters Section, page 4-7*

- Click **Per CPE Settings** (right circle in Figure 4-2 on page 4-3) to bring up a page so you can turn on encryption. For more information, see *If you clicked Per CPE Settings Button..., page 4-8*.

If you clicked the "System Wide Settings" button...



Click **Defaults** to load the proper default settings for the Config.

Figure 4-3: System Wide Settings page

Authentication Section

- **Using MAC Address:** Select this check box if you want to authenticate using the MAC address. Then, click **Apply**.
- **Using Pass Phrase:** Select this check box if you want to authenticate using the pass phrase. Then, click **Apply**.

- Enter the pass phrase in the **Pass Phrase** text box and confirm it (for authentication). Then, click **Set Pass Phrase for All CPEs**.
  (Pass Phrases have a minimum of 8 characters and a maximum of 32 characters.)

Performance Settings

If you dick the question mark next to "Performance Settings," the following text will appear in a separate dialog box:

New timing parameters have been added to allow the network manager to customize the network to a particular operating environment. Use these settings to tailor the network with respect to both link strength/reliability, as well as the type of network application(s).

(Background information: In the star topology, the base station polls each CPE router periodically, giving the routers the chance to transmit some of their queued data. The base station must set a timeout timer, in case a response is not received from the polled CPE router. After each CPE router is polled, the base station also has the opportunity to transmit some queued data.)

The following parameters are used in the implementation of the polling strategy, as described above:

- Max Frames Per BASE Timeslot
  The maximum number of frames of queued data that the base will transmit during one poll slot.
- Max Frames Per CPE Timeslot
  The maximum number of frames of queued data that the CPE router will transmit during one poll slot.
- Max Frames Per CPE Timeslot When only 1 CPE is Busy
  The maximum number of frames of queued data that the CPE router will transmit during one poll slot when only a single CPE router is considered to be "busy." This parameter is an optimization that allows a CPE router to transmit more queued data during a single poll slot if the network is idle. If a CPE router is the only CPE router responding to polls with actual queued data for a period of time, as measured by the base, it is deemed to be the only busy CPE router in the network. In that event, this parameter will govern how much the

CPE router is allowed to transmit during each poll. Note that determining the "single busy CPE" router is dynamic. And, as soon as other CPE routers respond to a poll with queued data, the network is deemed to have multiple busy CPE routers.

- **Poll Timeout Interval (expressed in units of 10 milliseconds)**
  The base station waits for each CPE router to respond to each poll. If a response never arrives, the base station must continue polling other CPE routers (or the same router again). This parameter governs how much time the base station is willing to wait for a response to a given CPE poll. Note that this value is strictly a timeout value in the case of no CPE response, and is not the amount of time between polls. The range is from 1-30. The default value is 20.

Click **Apply** after making changes.

Notes:

- The Max Frames Per Base/CPE parameters should be optimized for each individual network topology, environment, and requirement set. For example, in networks where high throughput is desired, higher values for maximum frames per base/ CPE timeslot are often desirable. On the other hand, in a network that needs to be optimized for low latency, these parameters can be set to lower values.
- The network administrator must take several points into consideration when setting the poll timeout interval. It should be set high enough to allow any CPE router to send its queued data (with retries taken into account). For example, if Maxi Frames Per CPE Timeslot=4 and the CPE retry limit = 6 for that CPE, in the extreme case one could encounter the following: The CPE router transmits 7 (original frame + 6 retries) frames for each allowed frame per timeslot (4) = 28 frames. The time to do this depends on the signaling rate being used and the length of each frame, which are network and application specific. The timeout interval is reset after each successful received frame, but if (due to noise), all frames where lost, you would need to wait the full 28 frame period before moving on to the next CPE router. If you poll the next CPE router before the previous CPE router is finished transmitting, collisions (and more loss) will result.
- **It is not necessary to reboot the system after changing these parameters because these changes immediately become active.**

Star Timing Parameters Section

The timing parameters control how a base station treats CPE routers during time periods when they have no network traffic to send.

The different polling parameters relate to aging inactive nodes (or sites) off the active list so a base station does not have to continuously poll them, thereby slowing down other sites that are more active. If a base station has to poll a router which continuously responds with "No, I don't have any traffic to send," bandwidth potential is lost since other routers with traffic to send must wait. On the other hand, if a router is rarely polled, or even removed from the polling table, it will encounter an additional delay the next time it has data to transmit. The trade-off is one of latency versus throughput. If you make the latency too high, users may complain about the delay they will encounter when they send traffic after a period of inactivity. Conversely, if you make the latency too low, total network throughput decreases. Although each router has fixed parameters for each of the three polling stages already set when it leaves Wave Wireless, the end user is allowed to configure them to fit their own requirements and applications.

Note: All values are in seconds. The minimum is 0.1 seconds and the maximum is 1,000 seconds (or 1ms).

- **Idle Time:** The consecutive amount of time since a CPE has transmitted traffic when it was polled. There are 3 categories (listed below).
- **Idle Category 1:** The default time is 2 seconds.
- **Idle Category 2:** The default time is 5 seconds.
- **Idle Category 3:** The default time is 30 seconds.
- **Idle Penalty:** How long, at a maximum, a CPE in the corresponding category (Idle Category 1, 2 or 3) has to wait until it gets polled. At a minimum it takes 2ms to poll a CPE. For example, if it takes 2ms to poll a CPE, multiply the number of CPE routers (e.g., 8 routers) by 2 (e.g., 8 x 2 = 16). Then, divide 1 second (1,000ms) by this quantity (e.g., 16) to get the maximum number of times a CPE router can be polled per second (e.g.,1,000 divided by 16 = 62). (In this example, the calculation really comes to 62.5 but you cannot poll in half seconds, only full seconds so it’s rounded down.)
- **Penalty 1:** The default penalty time is 0.25 seconds.
- **Penalty 2:** The default penalty time is 1 second.
- **Penalty 3:** The default penalty time is 2 seconds.

Note: If you want to reset the above parameters, click **Defaults**.

If you clicked Per CPE Settings Button...

Turning on Encryption

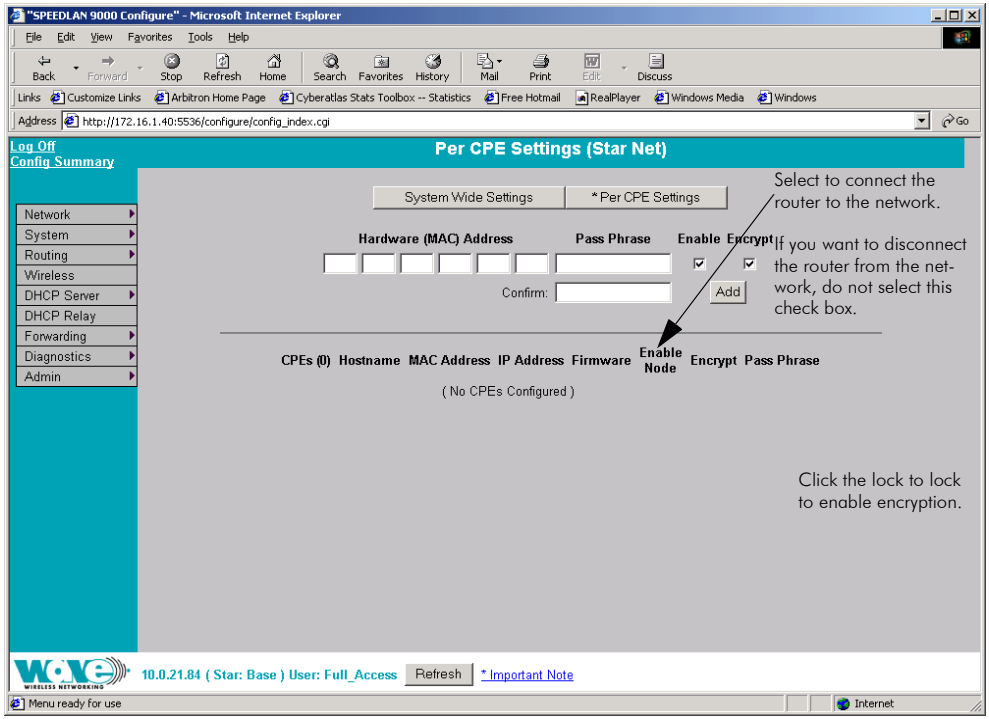


Figure 4-4: Per CPE Settings page

1. On the top half of the page: You have to authenticate an IP address for each CPE so it is listed in the routing table. To do this, enter the hardware address of the CPE in the **Hardware (MAC) Address** text box. Determine if you want to enable or encrypt it by selecting the appropriate checkbox and click **Add**. The IP addresses will not be active until the user logs on the particular CPE router.
2. On the bottom half of the page: If you want the router to be connected to the network, click the **Enable Node** checkbox. If you want to disable the router from the network, make sure this check box is not selected. Encyption is locked if the lock image is displayed, and encyption is unlocked if the unlocked image is displayed under the "Encrypt" column.
3. Click **Modify** to change an existing pass phrase that was set for a given CPE. Click **Create** if the pass phrase has not been set for a given CPE.

Note: You can configure a base station router on this page if you delete the existing one by clicking **Delete**.

4 Click **Create** if the CPE was never given a pass phrase (and it is blank). The following dialog box will appear.

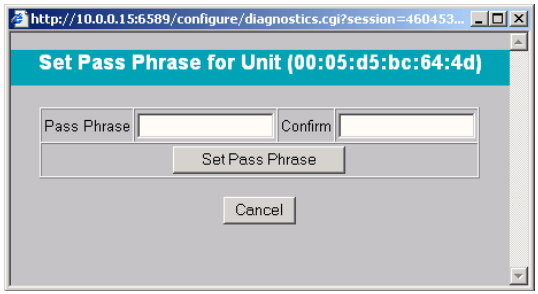


Figure 4-5: Set Pass Phrase for Unit box

5 Enter the appropriate information and click **Set Pass Phrase** when you are done. (Pass Phrases have a minimum of 8 characters and a maximum of 32 characters.) Then, exit this dialog box go back.

6 Click **Apply Changes** to update the system.

Other elements on the Per CPE Settings page:

- **All (at bottom of page):** Click to select all routers under the appropriate category (Enable, Encrypt, MAC or Pass).
- **None (at bottom of page):** Click to clear all routers under the appropriate category (Enable, Encrypt, MAC or Pass).
- **Delete:** Click to remove the hardware address.
- **Apply:** Click after making changes.

Wireless menu

Choose **Configuration** from the **Wireless** menu, and click one of the following buttons:

- If you click the **Channel and Rates** button, you will be able to select the channel and signaling rate of the interface. For more information, see *Channel and Rates, page 4-10*.
- If you click the **Tx Retries** button, you will be able to set the Transmit Retry Limit and Signaling Rate Fallback. For more information, see *Max Tx Retries and Signaling Rate Fallback, page 4-12*.
- If you click the **Max Throughput** button, you will be able to set the Max Transmit Data Rate in Kb/s. For more information, see *Max Throughput (Regulating Bandwidth), page 4-14*.

Channel and Rates

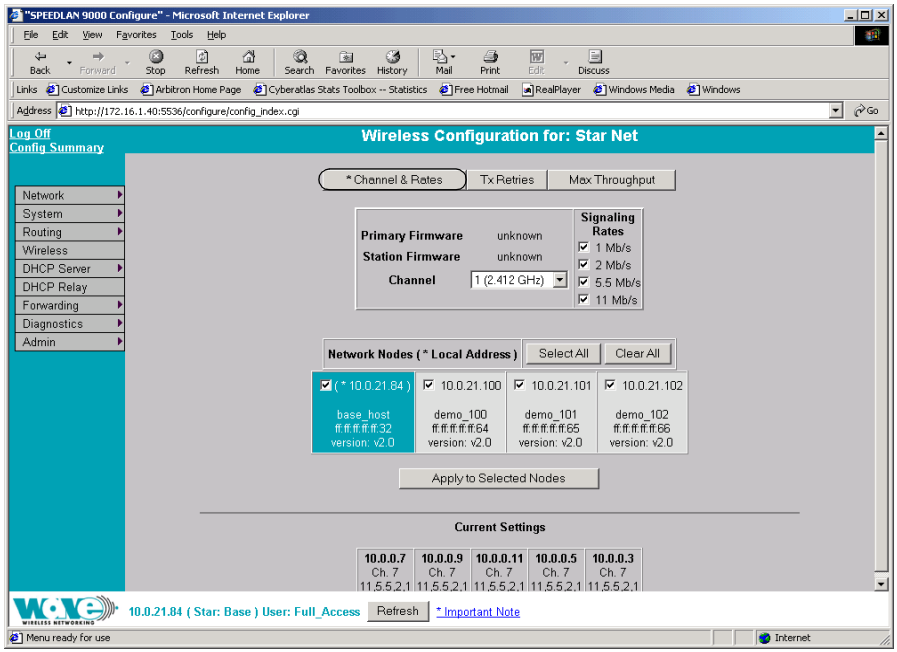


Figure 4-6: Channel and Rates page

- **Primary Firmware:** This is the current primary firmware version in use by the wireless card.
- **Station Firmware:** This is the current station firmware version in use by the wireless card.

- **Channel**: This is the specific band of frequencies (from 1 to 11) to determine the data path between routers. All SPEEDLAN 9000 routers expected to communicate in a network must have the same channel (frequency). Select one of the following channels (all are represented in GHz) from the **Channel** drop-down list:

  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

- **Signaling Rate**: This setting refers to the wireless signaling rate. The SPEEDLAN 9000 routers have four signaling rates that can be used. Select one of the following check boxes:
  - **1 Mb/s**: This setting limits the card by providing 1 Mb/s of bandwidth. The minimum receiver sensitivity of the radio with this setting is -92 dBm.
  - **2 Mb/s**: This setting limits the card by providing 2 Mb/s of bandwidth. The minimum receiver sensitivity of the radio with this setting is -89 dBm.
  - **5.5 Mb/s**: This setting limits the card to providing 5.5 Mb/s of bandwidth. The minimum receiver sensitivity of the radio with this setting is -88 dBm.
  - **11 Mb/s**: This is the full 11 Mb/s signaling rate. This value is recommended for most installations. The minimum receiver sensitivity of the radio with this setting is -85 dBm.

Note: The network can automatically downgrade the bandwidth if needed (that is, if lower Mb/s settings are selected).

Note: If you want to use the signaling rate and frequency settings on remote routers, select them and click **Apply to Selected Nodes**. If you want to select all of the routers, click **Select All**.

Max Tx Retries and Signaling Rate Fallback

This page includes two features: Max Tx Retries and Signaling Rate Fallback. On the figure below, Max Tx Retries is circled in red and Signaling Rate Fallback is circled in blue. The following page appears when the **Tx Retries** button is clicked:

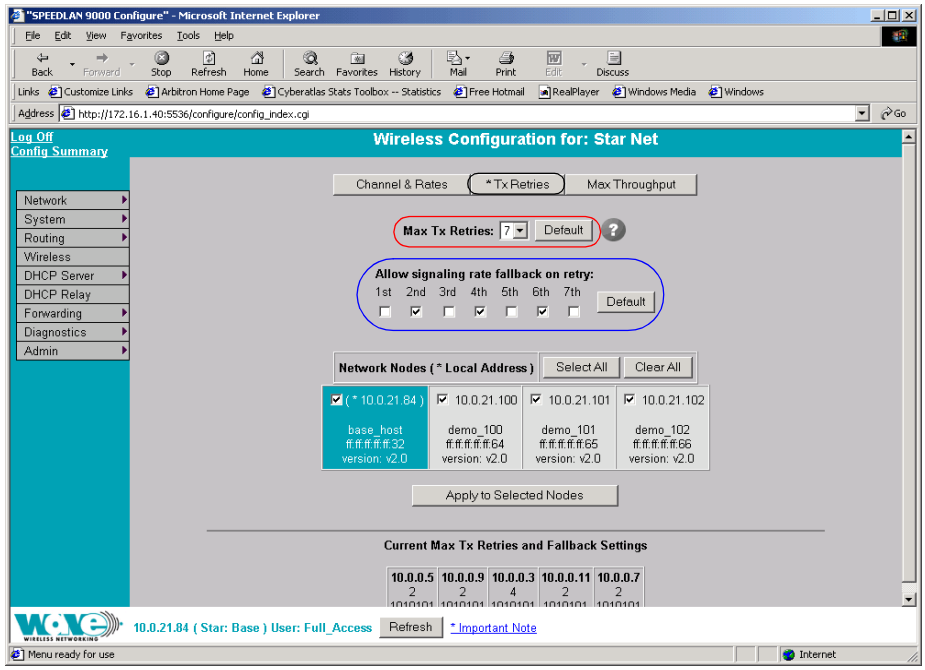


Figure 4-7: Tx Retries and Signaling Rate Fallback page

Note: To apply settings to other network nodes, select them and click **Apply to Selected Nodes**.

Max Tx Retries

Wave Wireless recommends that you use this parameter to increase the throughput of your wireless network. This parameter tells a network node the maximum number of times a unicast frame can be retransmitted before it is discarded. (A unicast frame is one that is transmitted to a single node in a network.) This allows a network manager to tune a network for its particular topology and expected traffic characteristics. The network topology, RF environment, number of nodes, throughput requirements, latency requirements, and type of applications are all factors in choosing an appropriate value for this parameter.

This parameter can be tuned on a per unit basis in order to optimize network performance. Click **Default** to get the default value of 7. You can select a value between 0 and 8 from the **Max Tx Retries** drop-down list.

Signaling Rate Fallback

During the retransmission of a unicast frame, the signaling rate can "fall back" in order to increase the chance of reception. Signaling Rate Fallback can occur multiple times for a single frame. Signaling Rate Fallback occurs from the current rate and will only include those signaling rates selected on the Channel and Rates page. After ten consecutive successful unicast frames, the current rate is restored to the highest selected rate.

The Signaling Rate Fallback parameter allows you to control when the signaling rate will drop, depending on the check box(es) you selected. That is, the check box(es) labeled, "Allow signaling rate fallback on retry" (circled in blue on previous figure).

The following parameters (check boxes) govern at which point in the re-transmission process the rate may be dropped:

- **1st retry**: Will drop signaling rate on first retry.
- **2nd retry**: Will drop signaling rate on second retry.
- **3rd retry**: Will drop signaling rate on third retry.
- **4th retry**: Will drop signaling rate on forth retry.
- **5th retry**: Will drop signaling rate on fifth retry.
- **6th retry**: Will drop signaling rate on sixth retry.
- **7th retry**: Will drop signaling rate on seventh retry.

Example:

The network administrator has configured the allowable transmit signaling rates to be 11, 5.5, 2, and 1 Mb/s. (These values can be selected on the Channel and Rates page under the Wireless menu.) In addition, the network administrator has selected **7** from the **Max Tx Retries** drop-down list and set the signaling rate to "fall back" on the second, fourth, and sixth retry attempts (as shown in blue on previous figure). When the intended recipient does not acknowledge a transmitted unicast frame, it will be retransmitted again (after a short timeout) at the current rate (e.g., 11 Mb/s). If this attempt is also unsuccessful (e.g., the receiver did not acknowledge it), the signaling

rate will drop to 5.5 Mb/s and another attempt will be made. If after the third retry, the transmission is still not successful, the signaling rate will drop to 2 Mb/s for the fourth and fifth retry, and then to 1 Mb/s for the sixth and seventh retry (if needed).

The recipient sends acknowledgements at the same signaling rate at which it receives frames. When a frame is successfully transmitted (acknowledgement received in the case of unicast), the transmitter immediately proceeds to the next frame. The last signaling rate used to transmit (other than acknowledgements) becomes the current rate. After ten consecutive unicast frames, the current rate returns to the highest rate selected, if it is not already at that signaling rate. Note that the receiver's signaling rate is not affected (other than returning the acknowledgement at a possibly different rate). Each transmitter's fallback schedule is independent of the signaling rate used by other transmitters.

Max Throughput (Regulating Bandwidth)

Max Throughput is useful to ISPs that want to regulate the maximum bandwidth provided to each customer. The following page appears when you click the **Max Throughput** button:

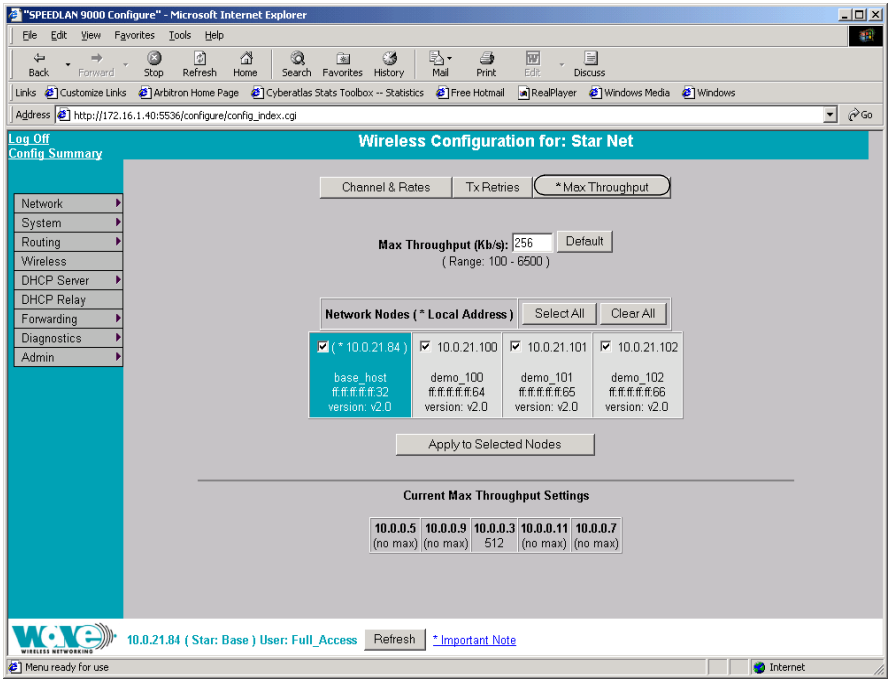


Figure 4-8: Max Throughput page

The Max Transmit Data Rate (in Kb/s) default is set to 6500; click **Default** to get default value. The range is from 100 to 6500 Kb/s.

If you want to use these settings on remote routers, select them and click **Apply to Selected Nodes**. If you want to select all of the routers, click **Select All**.

Admin Menu

Remote Control

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

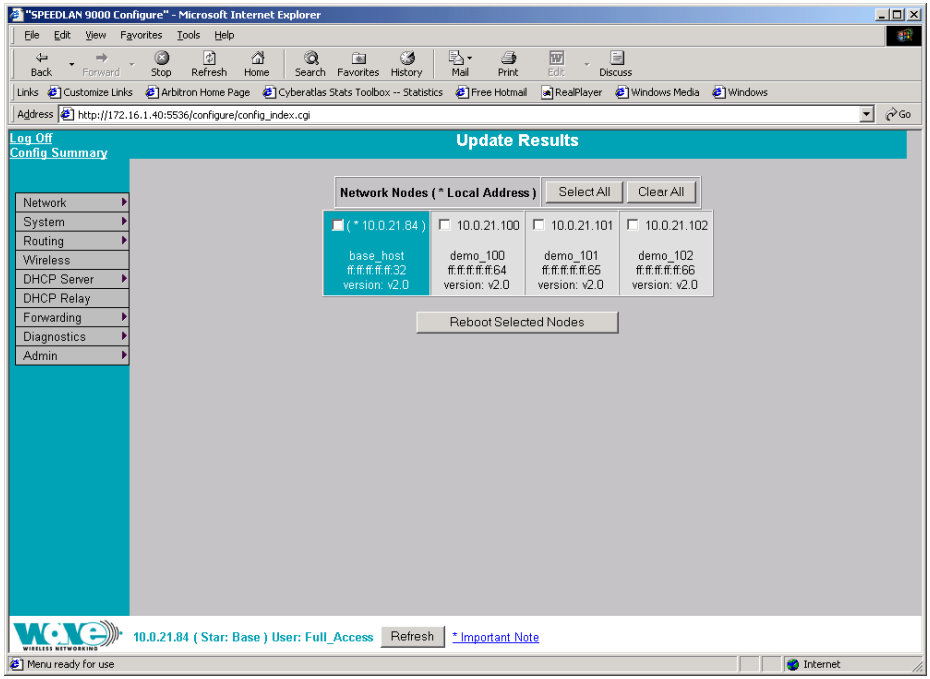


Figure 4-9: Remote Control for base mode

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

Software Update

To update the software on the local base station or on the remotes (e.g., CPE, Ethernet, etc.), choose **Software Update** from the **Admin** menu. The Software Update page will appear (for Local or Star Net). **Note:** The Software Update zip file (found on the Wave Wireless web site under the Support + Firmware link) will contain a document describing the recent changes and any other additional information needed to perform the update. The zip file will also include the update (.wwn) file to perform the update. After you have unzipped the file, make sure you extract the update file (.wwn) file to your desktop. Then, follow these directions:

Updating the Local Base Station

If you only need to update the software on a base station, choose **Local** (under the Software Update submenu).

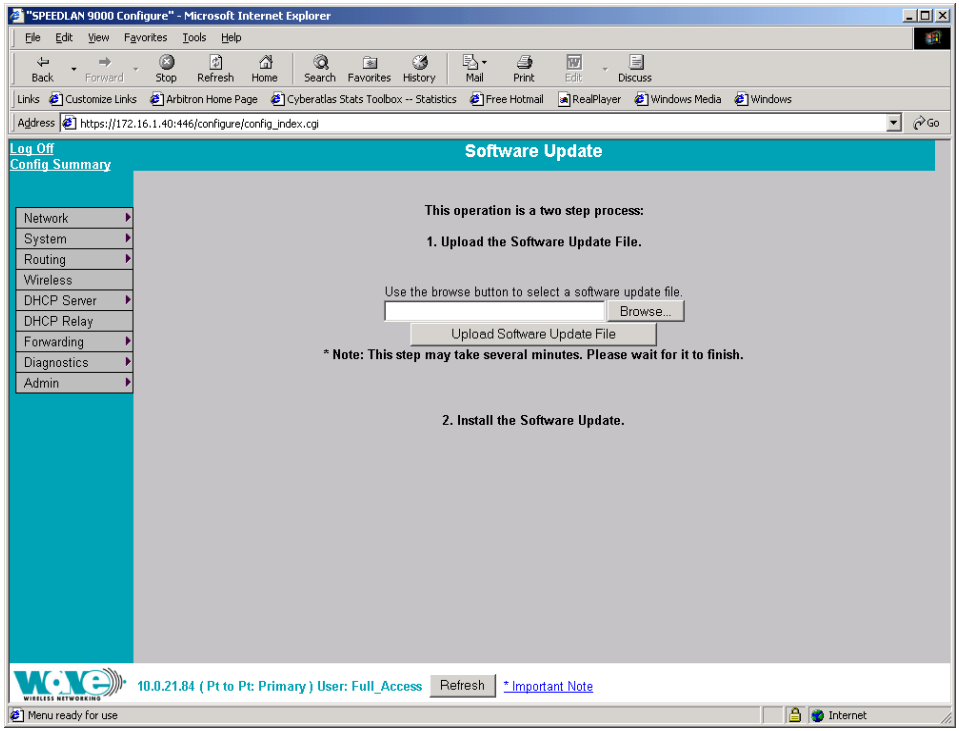


Figure 4-10: Updating the local base station

This operation is a two-step process:

1. Upload the Software Update file. Locate the latest software file (by clicking **Browse**) and click **Upload Software Update File**.
2. Install the Software Update.

Note: When you updated your network in the past, the remotes would not be rebooted until the final step. This step happened after you clicked the **Reboot Updated Nodes** button. Now the remotes are automatically rebooted after a successful upgrade. The local or connected router is not rebooted until you click the **Reboot Updated Nodes** button at the end of the upgrade.

Updating the Software on a Base Station and CPE

To update the software on a base station and on a CPE, choose the interface (e.g., Star Net) under Software Update submenu.

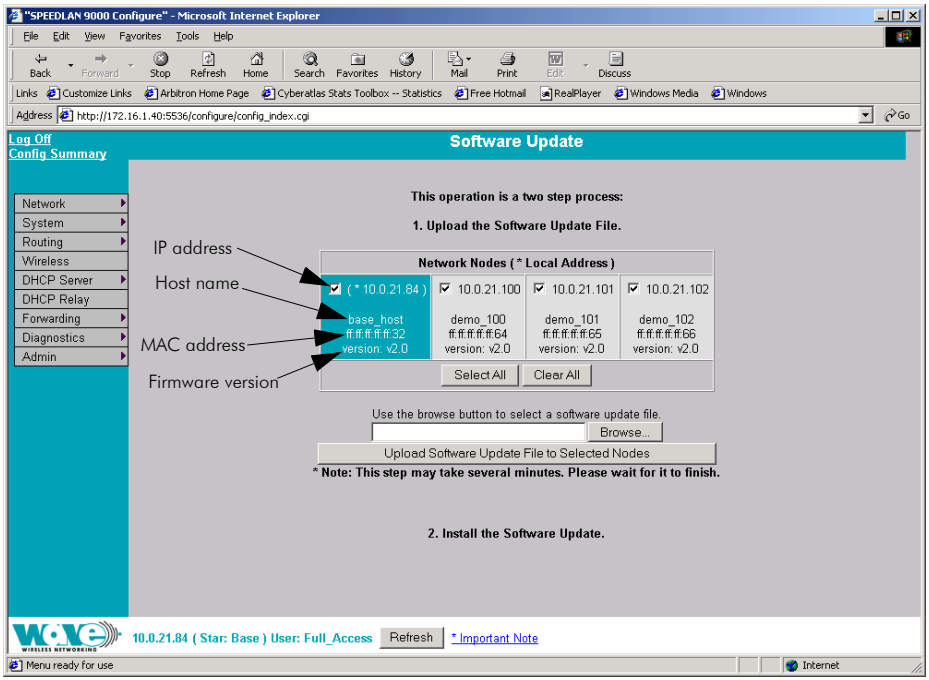


Figure 4-11: Updating software on a base station and CPE

This operation is a two-step process:

1. Select the remotes (CPE routers) where you want to update the software. (The IP addresses that are selectable are active. If only a MAC address is listed, or a bunch of zeros, then these represent inactive devices.
2. Upload the Software Update file. Locate the latest software file (by clicking **Browse**) and click **Upload Software Update File to Selected Nodes**.
3. Install the Software Update. **Note:** When you updated your network in the past, the remotes would not be rebooted until the final step. This step happened after you clicked the **Reboot Updated Nodes** button. Now the remotes are automatically rebooted after a successful upgrade. The local or connected router is not rebooted until you click the **Reboot Updated Nodes** button at the end of the upgrade.

Chapter 5
Using the Configurator to Set Up Special Parameters for CPE Routers

This chapter covers only those special parameters needed to set up the Customer Premise Equipment (CPE), such as:

- Network menu: *Interfaces for CPE Mode, page 5-2*; *Base Station Information, page 5-3*; and *Authentication, page 5-4*
- Wireless menu: *Channel and Rates, page 5-6*; *Max Tx Retries and Signaling Rate Fallback, page 5-8* and *Max Throughput (Regulating Bandwidth), page 5-10*
- Admin menu: *Software Update, page 5-11*

All other common configuration information can be found in *General Functions of the Configurator, page 3-1*.

Network Menu

Interfaces for CPE Mode

The Network Interfaces page will appear when you choose **Interfaces** under the **Network** menu. This is where you enter the interface type and network name of the interface or the router.

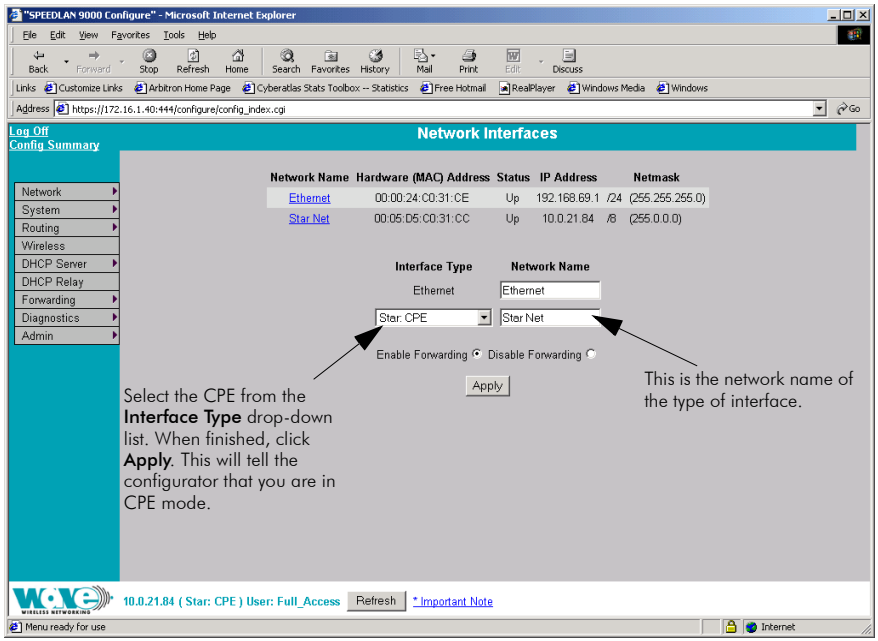


Figure 5-1: Selecting CPE mode

- **Network Name:** This is the fixed or wireless interface (e.g., CPE).
- **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.
- **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.