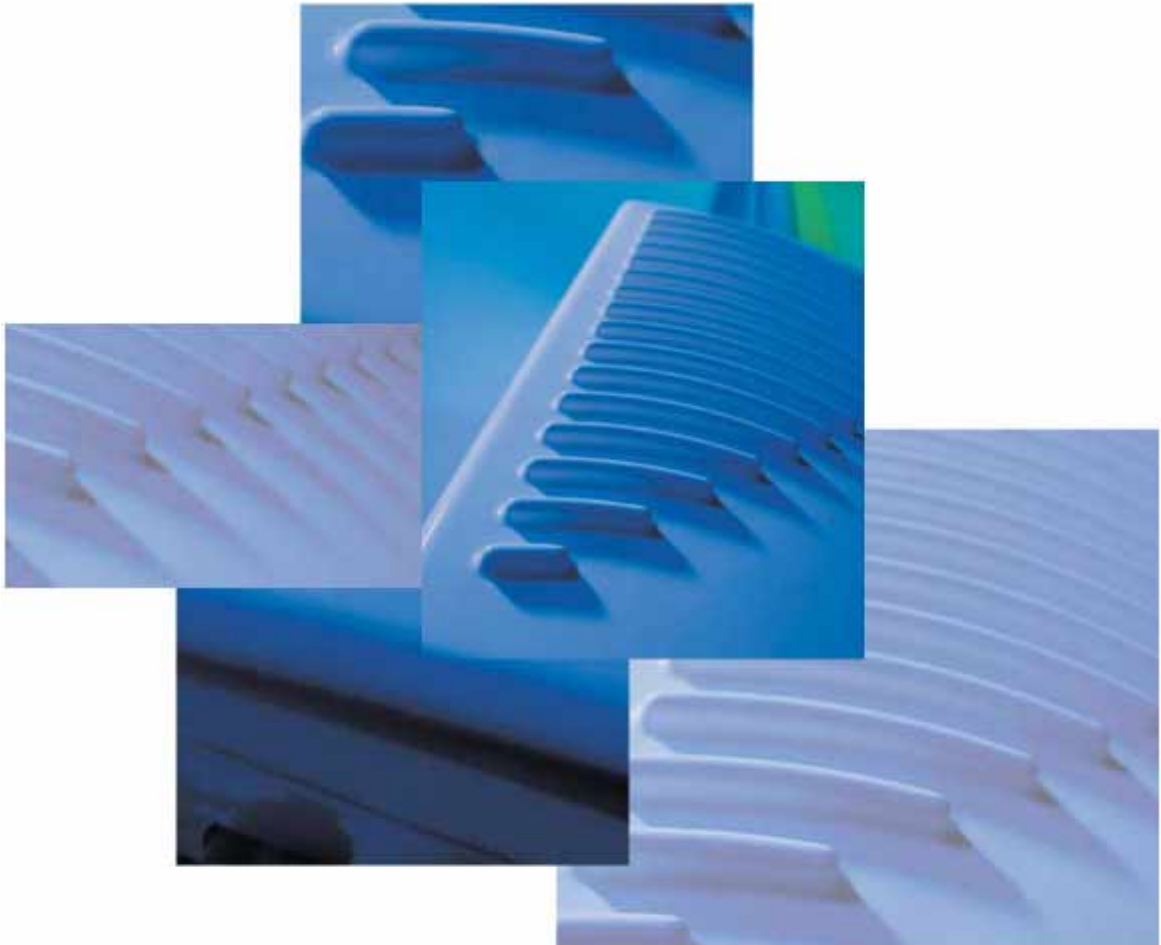

SPEEDLAN 9200 User Guide



**NOT FOR
PUBLIC RELEASE**



Part Number 34357-MNL Rev. 03

Last Revised: 10/7/04

P-Com Copyright Statement (c) 2004.

P-Com Inc. provides this Installation Guide without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. P-Com Inc. may make improvements and changes to the product described in this manual at any time and without any notice. P-Com Inc. assumes no responsibility for its use, nor any infringements of patents or other rights of third parties that would result.

This publication may contain technical inaccuracies or typographical errors. Periodic changes are made to the information contained herein. These changes, and mechanical corrections, will be incorporated in subsequent revision levels of the publication.

No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other records, without the prior written permission of P-Com Inc.

All other brand and product names are the trademarks of their respective holders.

P-Com
Sarasota Office
7020 Professional Parkway East
Sarasota, FL 34240

Technical Support

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

CHAPTER 1 - Introduction

Features and Benefits	1-2
SPEEDLAN 9200 Features.....	1-2
ISP Functionality	1-3
IP Router Functionality	1-3
Configuration Management	1-4
SPEEDManage.....	1-4
Features (and Benefits).....	1-4
Priority Queuing.....	1-5
SNMP	1-6
Equipment and Hardware	1-6
SPEEDLAN 9200 Mesh Protocol -- How It Works in Mesh Cells	1-6
SPEEDLAN's Mesh Cell Architecture.....	1-8
SPEEDLAN 9200 Mesh Core Components	1-9
Neighbor Discovery	1-9
Topology Updates	1-9
Routing.....	1-10
Why SPEEDLAN Outperforms Other Routing Equipment.....	1-10
Document Changes/Corrections.....	1-11
What's New for Firmware	1-11
Contacting Technical Support.....	1-12

CHAPTER 2 - 9200 Hardware

Rooftop and Tower Installations Warning.....	2-2
Regulatory Information	2-2
Declaration of Conformity for RF Exposure.....	2-3
General Safety Requirements for Installation of SPEEDLAN 9200 Models.....	2-3
Hardware Overview	2-4
Tips for Antenna Alignment.....	2-5
Drawings of Outdoor, Remote-Mounted Components	2-6
Indoor Junction Box.....	2-6
The SPEEDLAN 9201/9204 with an Integrated Omni-Directional.....	2-7
Bottom View of SPEEDLAN 9201/SPEEDLAN 9204	2-8
System Description	2-8
Package Contents	2-8
Installation Steps for the SPEEDLAN 9201/SPEEDLAN 9204	2-9
Installation Diagram of the SPEEDLAN 9201/SPEEDLAN 9204	2-11
The SPEEDLAN 9202/SPEEDLAN 9203 with External Antenna	2-12
Bottom View of SPEEDLAN 9202/SPEEDLAN 9203	2-13
System Description	2-13
Package Contents	2-14
Installation Steps for the SPEEDLAN 9202/SPEEDLAN 9203	2-15
SPEEDLAN 9202/SPEEDLAN 9203 Installation Diagram	2-21

CHAPTER 3 - General Functions of the Configurator

Manual Initial Configuration of the SPEEDLAN 9200	3-2
Prerequisites	3-2
Connecting a SPEEDLAN 9200 and a Client PC	3-3
Configuring the SPEEDLAN 9200	3-6
Wireless Interface IP Address Assignment	3-6
Automating the Configuration of Multiple SPEEDLAN 9200s	3-6
Completing Configuration	3-6
Adding Additional SPEEDLAN 9200s to the Wired Network	3-7
Overview of the SPEEDLAN 9200 Configurator General Main Menu	3-7
How the Configurator Menu is Structured	3-7
Network menu	3-7
System menu	3-8
Routing menu	3-8
Wireless menu	3-8
Diagram of SPEEDLAN 9200 Configurator Main Menu	3-10
Logging on the SPEEDLAN 9200 Configurator	3-10
Classes of Users (and Passwords)	3-11
Logging On	3-12
Logging Off	3-13
Understanding the Security Alert Screens	3-13
After Logging On	3-16
Helpful Information to Know... ..	3-17
How do you select the router?	3-17
References on Setting Up the Router	3-17
Caching - viewing the most recent version of a page	3-18
Session Activity	3-18
SPEEDLAN 9200 Firmware Updates, SPEEDManage or Other Utility Programs	3-18
If You Need a Temporary IP Address	3-19
The Configuration Menu	3-19
Network Menu	3-19
Network Interfaces	3-19
IP Address Configuration	3-19
CIDR Table (For Netmask Information Purposes)	3-21
Alias IP	3-22
Virtual Addresses	3-23
System Menu	3-25
Configuration Summary	3-25
SNMP	3-26
Version	3-29
Host Name	3-29
Password	3-30
Reboot	3-31
Routing Menu	3-31
Def Gateway	3-32
RIP2 Setup	3-32
RIP Settings	3-33

Authentication on RIP-2 MD5	3-34
Route Table	3-36
Static Route	3-37
Configuring the Radio Parameters.....	3-38
Configuration	3-38
Max Tx Retries and Signaling Rate Fallback	3-41
Signaling Rate Fallback.....	3-41
Max Tx Retries	3-43
Max Throughput (Regulating Bandwidth)	3-43
DHCP Server Menu.....	3-44
How DHCP Assigns an IP Address	3-44
Setting Up DHCP and DHCP Relay	3-45
Important Note about DHCP	3-45
Setting Up DHCP	3-46
Subnets to Serve Section.....	3-46
Adding a New DHCP Subnet.....	3-47
Adding a Known Client.....	3-48
Adding a DHCP Client.....	3-49
Configuring DHCP Relay	3-50
Viewing Log Messages.....	3-51
Forwarding Menu	3-51
Priority Queuing.....	3-52
Explanation of this feature	3-53
Services.....	3-53
Creating an Advanced Service	3-55
Three Features of NAT	3-56
Address Sharing	3-58
Internal Servers	3-60
1:1 NAT.....	3-62
Firewall.....	3-63
IP Sessions	3-68
Diagnostics Menu (Troubleshooting the Network)	3-68
Special Note about Link & Ping Tests:.....	3-68
Interface Statistics.....	3-69
Wireless Statistics.....	3-69
Inbound & Outbound	3-70
ARP Table.....	3-71
ICMP Statistics	3-71
Admin Menu	3-74
User Configuration Passwords.....	3-74
Software Update	3-75
Proxy Mode Warning	3-75
Support	3-76
Reset to Factory Default	3-76
Current Sessions	3-77

CHAPTER 4 - Using the Configurator to Set Up Special Parameters for Mesh Routers

Network Menu	4-2
Interfaces for Mesh Mode	4-2
Mesh Nodes	4-3
Enabling Network Security.....	4-4
A. Enabling Encryption Between SPEEDLAN 9200 Routers	4-4
B. Enabling WEP Security Between a SPEEDMesh-Enabled Client and SPEEDLAN 9200	4-5
Enabling/Disabling the SPEEDMesh-Enabled Client.....	4-6
Wireless menu	4-7
Request to Send (RTS) / Clear to Send (CTS)	4-8
Receive (Rx) Threshold Parameter	4-9
Blocked Links	4-10
Link Expiration	4-11
Admin Menu	4-12
Remote Control	4-12
Software Update	4-12
Updating the Local Router	4-12
Updating the Software on a Local Router and Remote Router	4-13

CHAPTER 5 - Basics of IP Addressing

Basics of IP Addressing	5-2
What is an IP address?	5-2
Internet Address Classes	5-2
In fact, IP defines five classes:	5-3
Subnetting a Network	5-5
What is a Subnet?	5-5
What is a Subnet Mask?	5-5
Diagram of Subnetting a Network	5-6
How does a network administrator assign an IP address?	5-7
What is DHCP?.....	5-8
Figure of DHCP Addressing	5-9
What is NAT?	5-9
NAPT	5-10
Diagram of Outgoing NAT	5-11
Diagram of Incoming NAT	5-12
Basics of Routing	5-13
Glossary for Standard Data Communications.....	Glossary-2

Appendices

Changing the Router's Topology Mode A-2

SPEEDLAN 9200 Configurator Passwords B-2

 Rooftop and Tower Installations Warning C-2

 General Safety Requirements for Installation of SPEEDLAN 9200 Models C-2

Manufacturer Information C-3

Radio Approvals C-4

 Radio Approval Table for Models SL920x C-4

 Minimum Receive Sensitivity (in dBm) for SL920x C-4

SPEEDLAN 9200 Technical Specifications D-2

..... D-2

List of Acronyms..... E-2

Channels for IEEE 5GHz OFDM (UNII upper band)..... G-2

2.4GHz DSSS Channels & 2.4GHz OFDM Channels G-2

Software License Agreement

 P-Com LIMITED WARRANTY STATEMENT

 Return Policies and Warranties

[illegible]

Chapter 1

Introduction



Features and Benefits

SPEEDLAN 9200 Features

The SPEEDLAN 9000 series introduces the second generation of wireless routers. The SPEEDLAN 9200 offers the following new features:

- New Wireless Mode parameters (e.g., 5GHz OFDM, 2.4GHz DSSS or 2.4GHz OFDM), Preamble, Tx power and SSID). For more information, see *Configuring the Radio Parameters*, page 3-38.
- Double the transmission rate with turbo mode, up to 108Mb/s for 5GHz OFDM. For more information, see *Configuring the Radio Parameters*, page 3-38.
- You can allow a mesh node in a 9200 network to communicate with a SPEEDMesh-enabled client in adhoc mode. For more information, see *Enabling/Disabling the SPEEDMesh-Enabled Client*, page 4-6.
- Provide network security between SPEEDMesh-enabled clients (PDAs and laptops) and SPEEDLAN 9200 routers via WEP. In a SPEEDLAN 9200 network, you can authenticate a SPEEDMesh-enabled client with a standard security mechanism called Wired Equivalent Privacy (WEP). WEP encrypts data that is transmitted over the wireless LAN. WEP protects the wireless link between clients and access points. Network administrators can control access via standard 802.11 client using WEP. For more information, see *B. Enabling WEP Security Between a SPEEDMesh-Enabled Client and SPEEDLAN 9200*, page 4-5.
- Improve WLAN performance with Request to Send / Clear to Send (RTS/CTS). For more information, see *Request to Send (RTS) / Clear to Send (CTS)*, page 4-8.
- Provide DHCP relay: This first release of the SPEEDLAN 9200 shall use the DHCP relay function to forward DHCP requests from non-SPEEDLAN wireless clients to one or more DHCP servers. Those DHCP servers maybe suitably configured SPEEDLAN 9200 routers (in which they won't relay), or they may be dedicated servers, reachable through the Ethernet interfaces of one or more of the SPEEDLAN 9200 routers. To configure DHCP relay, see *Configuring DHCP Relay*, page 3-50.
- Support for DC input sources: Devices that lack AC power will require DC-to-DC supply.
- **At this time, star mode (i.e., base, point-to-point and CPE) is not available. Only mesh mode is available.**

The SPEEDLAN 9200 offers the network manager unsurpassed flexibility in meeting the challenges of designing, building and managing today's wireless broadband networks.

In a mesh topology, the SPEEDLAN 9200 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 cell: 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.

For more information about mesh, see *SPEEDLAN 9200 Mesh Protocol -- How It Works in Mesh Cells*, page 1-6.

ISP Functionality

The SPEEDLAN 9200 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.

IP Router Functionality

The SPEEDLAN 9200 is a highly configurable wireless IP router which supports mesh topologies. In addition to being configurable via a standard web browser, the SPEEDLAN 9200 also contains a firewall to control incoming and outgoing traffic, preventing unauthorized access.

Configuration Management

The SPEEDLAN 9200 Configurator is a web-based management tool that allows a network manager to configure routers. For more information, see *General Functions of the Configurator*, page 3-1.

SPEEDManage

The SPEEDManage suite offers network management tools to help you troubleshoot and resolve network issues to keep your network running. Packaged in SPEEDManage are SPEEDView[®], SPEEDSignal[®] and IP Recover:

- 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 9200 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.
- SPEEDSignal[®] allows you to communicate with SPEEDLAN 9200 routers via their wireless or wired interface. This software makes it easier for installers to troubleshoot antenna alignment problems in the field.
- IP Recover is an application that allows you to temporarily change the IP address on the router if you forgot it. You can also locate the configured IP address of a router's Ethernet interface.

For information about SPEEDManage, see the SPEEDManage User Guide.

Features (and Benefits)

- 2.4GHz DSSS, 2.4GHz OFDM and 5GHz OFDM License-free ISM band (No lengthy licensing delays).
- Mesh topologies (Maximum network flexibility).
- NAT & DHCP server/client (Secure and efficient network).
- SPEEDManage suite for antenna alignment (via SPEEDSignal), troubleshooting network problems and viewing nodes on a network (via SPEEDView) and creating a temporary IP address (via IP Recover).
- Web-based configuration.
- Multihop, Self-healing (Increased network stability and performance).
- Polling base station (Robust performance).

- Hardware AES 128-bit encryption for security between SPEEDLAN 9200 routers.
- You can recover lost IP addresses. (Use IP Recover in SPEEDManage.)

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. These routers use an AES 128-bit encryption key.

Encryption Note! A Web browser must support 128 bit encryption in order to be used with the Configurator. For more information about AES, visit <http://www.nist.gov>. This User Guide explains how encryption works with 9200 products in A. *Enabling Encryption Between SPEEDLAN 9200 Routers*, page 4-4 and B. *Enabling WEP Security Between a SPEEDMesh-Enabled Client and SPEEDLAN 9200*, page 4-5.

Priority Queuing

Despite having two physical interfaces, a SPEEDLAN 9200 router can experience congestion. That is because the interfaces' bit rates are not matched. Specifically, packets can ingress (enter) the Ethernet interface faster than they can egress (exit) the wireless interface. If this occurs briefly, it is called short-term congestion, which can cause increased packet delay and/or jitter. If congestion lasts too long, it can cause packet discard ("loss"). Long-term congestion in a SPEEDLAN 9200 will typically only occur when it receives excessive unthrottled UDP traffic at its Ethernet interface. TCP traffic will self-throttle, typically experiencing only short-term congestion, if any.

A SPEEDLAN 9200 mitigates short-term congestion by providing priority egress queuing at its wireless interfaces. With priority queuing, packets may be transmitted in a different order than they were received. This allows favoring network management, VoIP and SCADA, over SMTP, ftp, and NNTP (for example).

How does Priority Queuing work? The packets are prioritized into a hierarchy of queues, based on class of traffic. The highest priority queue packets are serviced first. When the highest queue is emptied, the next lower queue is serviced. The SPEEDLAN 9200 has four levels of priority queues.

Queue 1 (the highest queue serviced) contains "management" traffic (i.e., RIP, Mesh, K2, SNMP). Queue 2, the next lower queue serviced, contains "real-time" traffic (i.e., VOIP, Video, SCADA). Queue 3, the next lower queue serviced, contains "non-real time interactive" traffic (i.e., HTTP, SSH and Telnet). Queue 4 (the lowest level queue serviced) contains all traffic that doesn't fit into one of the first three queues. There are no matching or requirements for this queue; it is simply the default queue if the packet doesn't qualify for one of the first three queues.

SNMP

The SPEEDLAN 9200 contains a Simple Network Management Protocol (SNMP) Agent that provides a remote Network Management System (NMS) with read-only ("get") access to certain configuration and status parameters. For more information, see SNMP, see *SNMP*, page 3-26.

Equipment and Hardware

For information about equipment and hardware, see *SPEEDLAN 9200 Hardware*, page 2-1.

SPEEDLAN 9200 Mesh Protocol -- How It Works in Mesh Cells

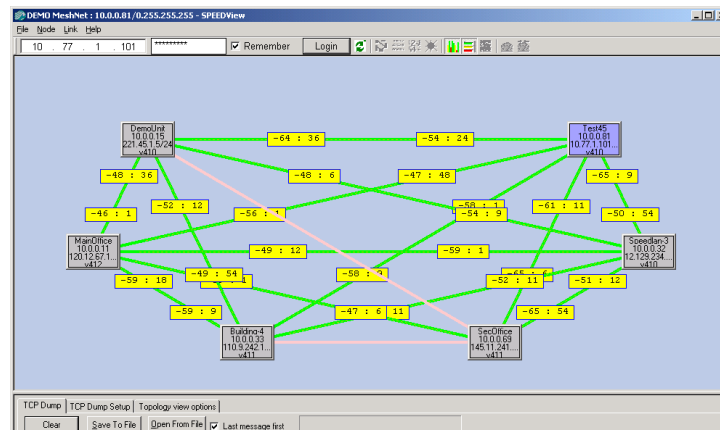


Figure 1-1: SPEEDView illustrating a mesh network (in SPEEDManage suite)

SPEEDLAN 9200 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 1-1 on page 1-6?

- 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 cell can be heard by every other router in the cell, except for the blocked link indicating that there is no signal between those two nodes.

SPEEDView allows you to block traffic over any link in the cell. When you block a connection, the node pair will not be able to communicate. The advantage of blocking a connection is verifying that the path can be re-routed for successful connectivity. (This is done using the "Block" feature in SPEEDView. The broken [or disconnected] link will appear as a red 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

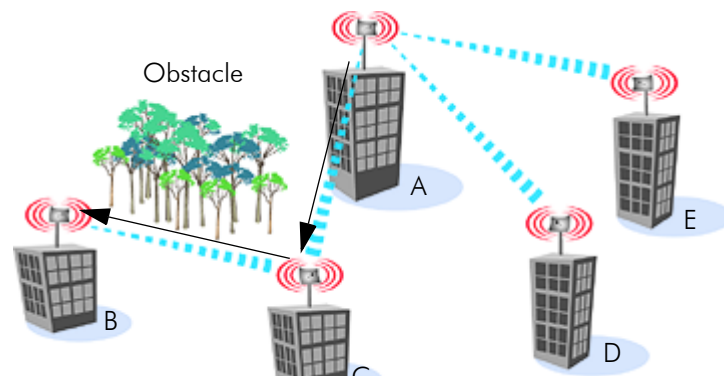


Figure 1-2: Routing around obstacles

Explaining this scenario on the simplest level (using the Mesh protocol as shown in Figure 1-2 on page 1-7). 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 *Document Changes/Corrections*, page 1-11).

SPEEDLAN's Mesh Cell Architecture

Separate multi-user and residential models (SPEEDLAN 9201 for business and residential use, as well as the SPEEDLAN 9204 for residential use) are specifically designed to meet the connectivity demands for everyone from single users to large corporations. SPEEDLAN 9201 and SPEEDLAN 9204 are mesh units. These models will communicate with every other mesh router within an unobstructed radius of 1/2 mile for SPEEDLAN 9201 and 1/4 mile for SPEEDLAN 9204.

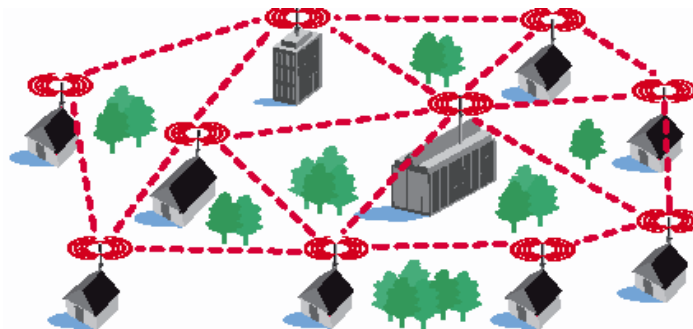


Figure 1-3: An example of a mesh network

SPEEDLAN 9200 Mesh Core Components

SPEEDLAN 9200 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 9200 outperforms other routers because the SPEEDLAN 9200 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 9200 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.

Document Changes/Corrections

- Removed SPEEDLAN 9205 references. Refer to Chapter 2, beginning on *SPEEDLAN 9200 Hardware*, page 2-1 for more information
- 2.4GHz OFDM and DSSS references have been added to this User Guide. This means that the preamble setting is now functional.
- The List of MIBs supported by SPEEDLAN 9200 table has been corrected to display the right version. For more informaton, see Table 3-1, "List of MIBs supported by SPEEDLAN 9200," on page 3-28.
- TX power level drop-down list has been added on the Wirelesss Configuration page. See *Configuration*, page 3-38. Also, the default value for the SSID on the Wireless Configuration page is "SPEEDLAN9200" instead of "SP9200".
- Default values for Maximum Throughput were added for 2.4GHz OFDM and 2.4GHz DSSS values. For more information, see *Max Throughput (Regulating Bandwidth)*, page 3-43.
- The Glossary has been improved. The following terms were revised: attenuator, CSU/DSU, channel spacing, dB, DHCP, E1, MAC, MIB, MTBF, passive repeater, polarization, QAM, raditaion, refraction, reliability, sidelobe and system gain. For more information, see the Glossary.
- 2.4GHz OFDM and 2.4GHz DSSS values have been added to the Minimum Receive Sensitivity table in Appendix C-4.

The section below, "What's New," displays the firmware's recent changes. Changes prior to the version listed below can be found in Previous Firmware Changes, Appendix F-1.

What's New for Firmware

- The TX power level drop-down list has been added to the Wireless Configuration page. See *Configuration*, page 3-38.

Contacting Technical Support

For more information, contact P-Com at:

7020 Professional Parkway East

Sarasota, FL 34240

941-907-2300 (phone)

941-355-0219 (fax)

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 "www.wavewireless.com/support" directory.

Chapter 2

SPEEDLAN 9200

Hardware



Rooftop and Tower Installations Warning



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

Regulatory Information



Install this device in accordance with the instructions provided in this User Guide. To determine the type of device you should use in your country, see the Radio Approval Table *Radio Approvals, Appendix C-4*.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause interference. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the installer should correct the interference by one of the following measures:

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

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



Warning! This part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using the following antennas:

- 2.4GHz: 9dBi external omni or 18 dBi directional grid antenna.
- 5GHz: 10dBi external omni or 29dBi directional dish antenna or 23dBi sector flat panel antenna.
- Integrated omnis are 8dBi for SPEEDLAN 9201 and 5dBi for SPEEDLAN 9204.

For more information, see *9200 Hardware Configuration Table, page 2-5*.

Declaration of Conformity for RF Exposure

The radio module has been evaluated under FCC Bulletin OET65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The radiated output power of this wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized. When using this device, a certain separation distance between the antenna and nearby persons must be maintained to ensure RF exposure compliance. In order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antenna and your body or nearby persons should not be less than 20cm (8 inches) for the 10dBi external omni antenna or 2m (6.5 feet) for the 29dBi directional dish antenna.

General Safety Requirements for Installation of SPEEDLAN 9200 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 9200 on a tower, pole or 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 9200 offers all the equipment you need to meet your connectivity requirements:

- SPEEDLAN 9201: A router used in a non-line-of-sight pico cell (using the Mesh protocol). This router contains an integrated 8 dBi, omni antenna (for 2.4 GHz only) which is directly attached on the top. You do not need an additional external antenna. The parameters are configured with the Mesh protocol in the SPEEDLAN 9200 Configurator. This type of self-healing Mesh topology process helps you reach buildings that do not have a clear line-of-sight back to a base station without the possibility of interference from hidden transmitters. For more information on this topic, see *SPEEDLAN 9200 Mesh Protocol -- How It Works in Mesh Cells*, page 1-6.
- SPEEDLAN 9202: This model can be configured as Customer Premise Equipment (CPE) at one end of the point-to-point or point-to-multipoint link. It can be used with a 2.4GHz or 5GHz external antenna.
- SPEEDLAN 9203: 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. It can be used with a 2.4GHz or 5GHz external antenna.
- SPEEDLAN 9204: This model provides the same functionality as a SPEEDLAN 9201, but it uses an integrated 5 dBi omni (for 2.4GHz only). The SPEEDLAN 9204 is intended for more densely populated cells.

Table 2-1: 9200 Hardware Configuration Table

9200 Model	Mode	Integrated antenna	External antenna
9201	mesh	2.4GHz only	N/A
9202	flexnode	N/A	2.4 & 5GHz
9203	base station	N/A	2.4 & 5GHz
9204	mesh	2.4GHz only	N/A

The SPEEDLAN 9200 is housed in a waterproof, cast enclosure that mounts outside the building, on a mast, or tower. The SPEEDLAN 9200 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.

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 the SPEEDManage User Guide. The SPEEDSignal application will also help installers align or position antennas on SPEEDLAN 9200 units.

Drawings of Outdoor, Remote-Mounted Components

Indoor Junction Box

When the green light is illuminated,
the DC voltage is being injected

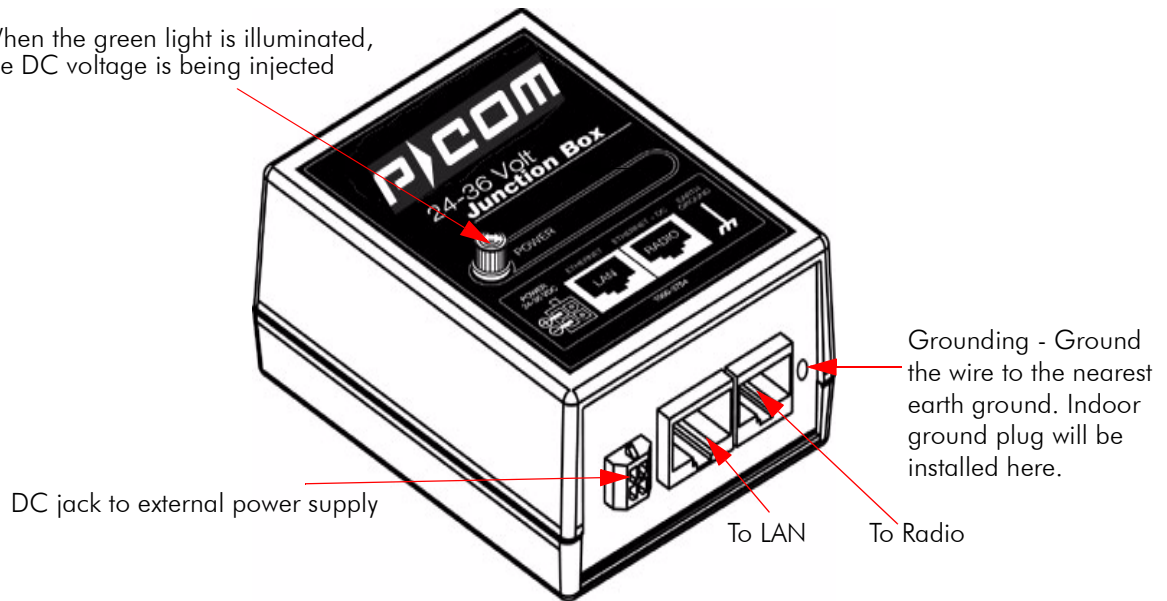


Figure 2-1: Indoor junction box for SPEEDLAN 9200

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.

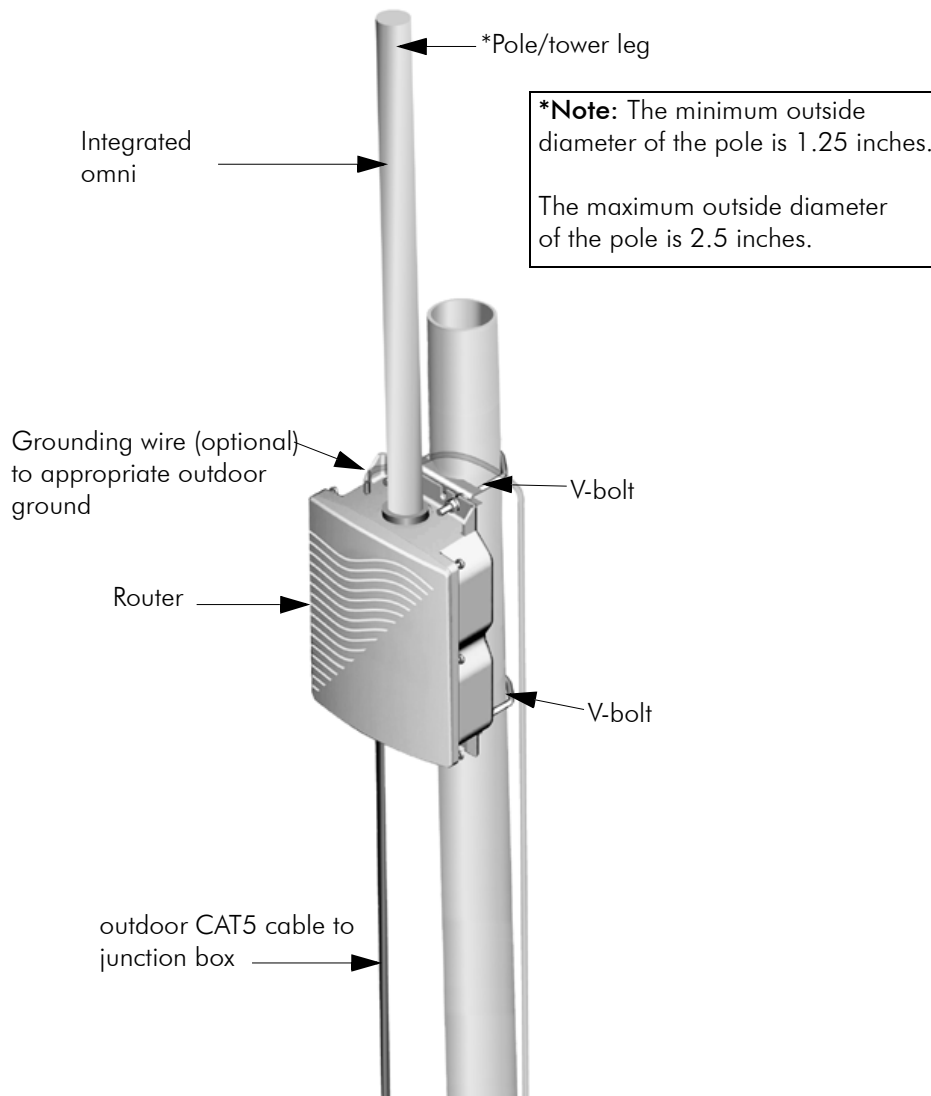
The SPEEDLAN 9201/9204 with an Integrated Omni-Directional-

Figure 2-2: SPEEDLAN 9201/SPEEDLAN 9204 installation

The installation steps for the SPEEDLAN 9201 and SPEEDLAN 9204 are similar, but the SPEEDLAN 9201 uses a larger omni and the SPEEDLAN 9204 uses a smaller omni-directional antenna.

Bottom View of SPEEDLAN 9201/SPEEDLAN 9204

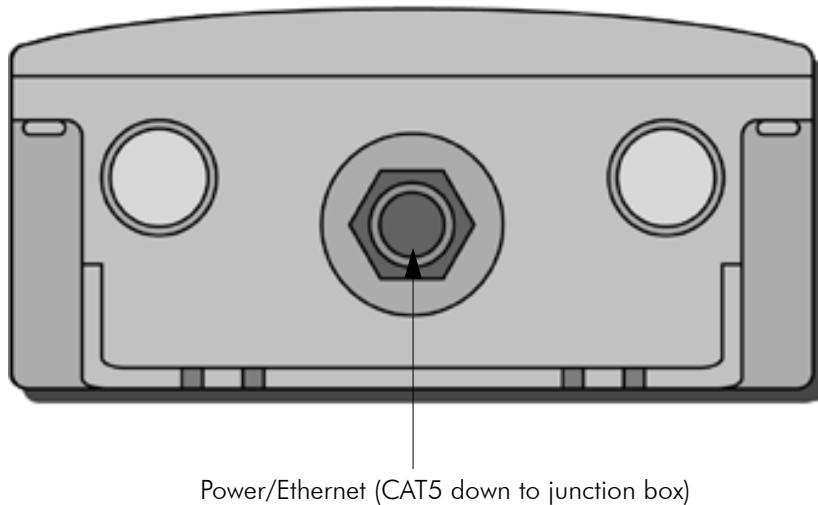


Figure 2-3: Bottom view of case

System Description

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

Package Contents

- SPEEDLAN 9201/SPEEDLAN 9204
- CD containing: Adobe Acrobat Reader, SPEEDManage software & User Guide, this User Guide, Installation Diagram booklet and Getting Started Guide
- Indoor junction box
- Power supply
- Integrated, omni-directional antenna
- V-bolt kit which includes the following
 - Bolt, V, Tower Mount, Stainless Steel (quantity 2)
 - Nut, 1/4"-20, Serrated Flange, Stainless Steel (quantity 4)
 - V-Bracket, Tower Mount, Aluminum (quantity 2)

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 P-Com are: cable, connectors, crimpers, spectrum analyzer, shrink wrap, 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 9201/SPEEDLAN 9204

To install your SPEEDLAN 9201/SPEEDLAN 9204, follow the steps below:

Step 1: Mounting the SPEEDLAN 9201/SPEEDLAN 9204

This router will have an omni directly attached. No additional steps are needed for this step. Go to Step 2.

Step 2: Mounting the SPEEDLAN 9201/SPEEDLAN 9204 on the Pole

- **Pole Mount:** Attach the router to the mounting pole using the two V-bolted clamps and aluminum bracket, one on top of the router and the other on the bottom of the router. Make sure you tighten the nuts for the clamps securely to prevent shifting of the router after antenna alignment.

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 proper indoor ground plug into the junction box. Connect the outdoor CAT5 Ethernet to the "radio" jack. Connect the LAN Ethernet cable to the "LAN" jack of the junction box. Install the power supply 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 9201/SPEEDLAN 9204 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 "LAN" on indoor junction box. Connect the other end of the Ethernet CAT5 cable to your Ethernet hub, switch or router.

Important Note: Waterproofing the External 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 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 9201/SPEEDLAN 9204

The diagram below displays where the main components are located for the SPEEDLAN 9201/SPEEDLAN 9204 with an integrated omni.

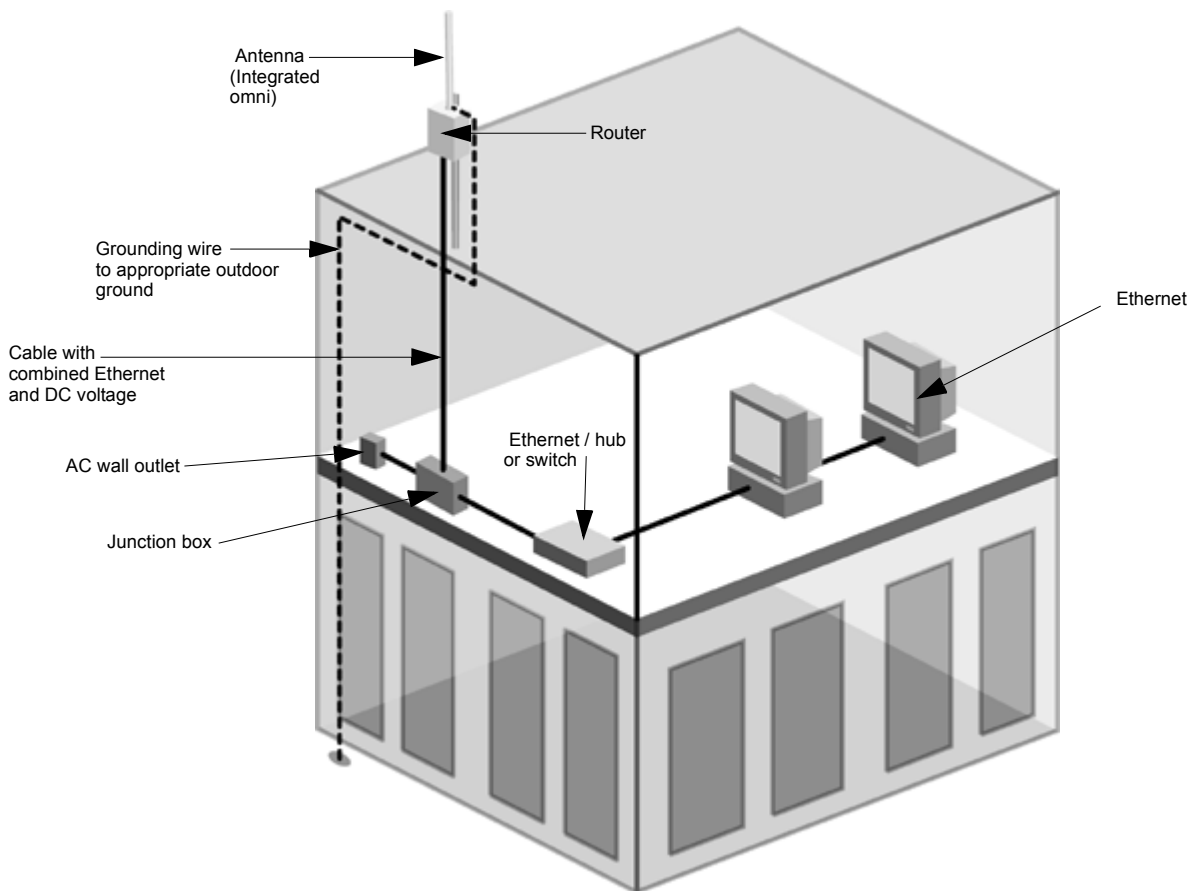


Figure 2-4: SPEEDLAN 9201/SPEEDLAN 9204 installation diagram

The SPEEDLAN 9202/SPEEDLAN 9203 with External Antenna

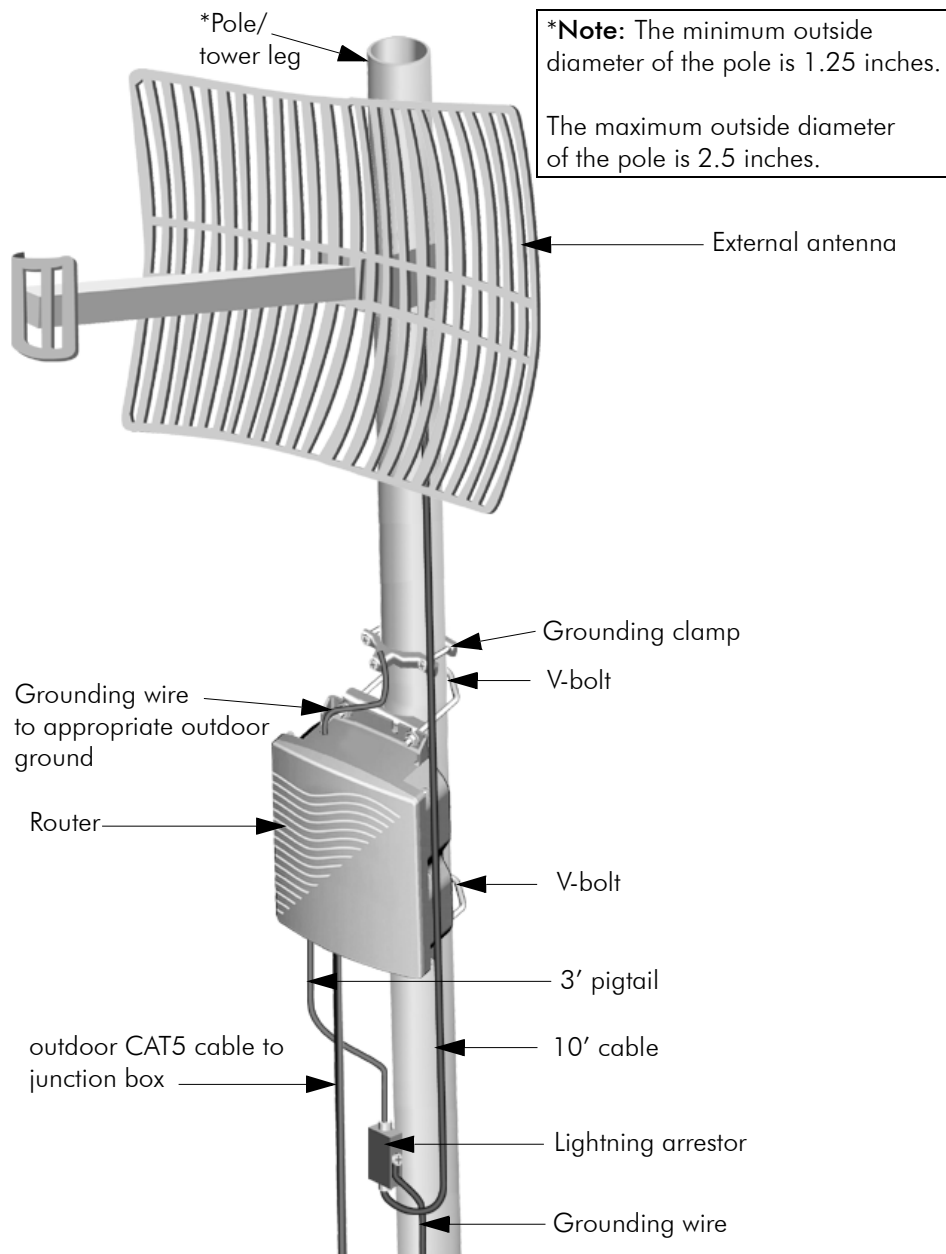


Figure 2-5: SPEEDLAN 9202/SPEEDLAN 9203 installation

Bottom View of SPEEDLAN 9202/SPEEDLAN 9203

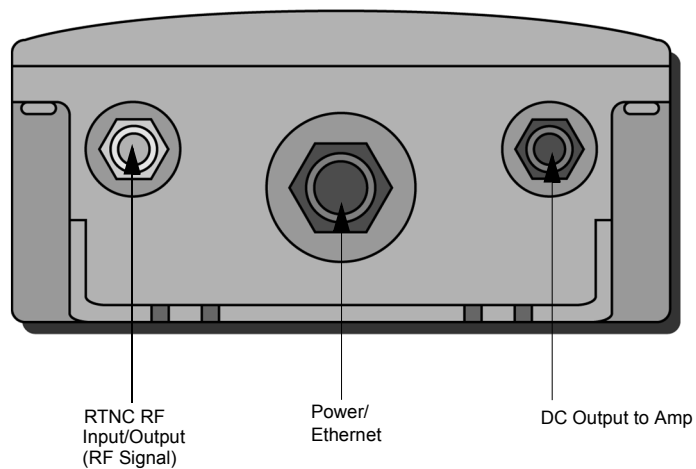


Figure 2-6: Bottom view of case

System Description

The SPEEDLAN 9202/SPEEDLAN 9203 routers are high speed, long range wireless LAN routers that provide connectivity to remote Ethernet networks.

Package Contents

The following items are included in the package contents:

- SPEEDLAN 9202/SPEEDLAN 9203 router
- CD containing: Adobe Acrobat Reader, SPEEDManage software & User Guide, this User Guide, Installation Diagram booklet and Getting Started Guide
- Indoor junction box
- 3' pigtail
- 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 router are 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 P-Com are: cable, connectors, crimpers, spectrum analyzer, shrink wrap, 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 9202/SPEEDLAN 9203

Generally, these routers follow the same general installation steps. Some installation instructions are specific to customers who purchased Installation Kits from P-Com. To view a diagram of the installation listed below, see Figure 2-9 on page 2-21.

If you are having trouble and need a full site installation, contact P-Com for services and fees.

Antenna Selection Tip: Use a high-gain omni or sectoral antenna for a base station (SPEEDLAN 9203), and use a grid or directional antenna for a CPE or point-to-point router (SPEEDLAN 9202).

To install your 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.

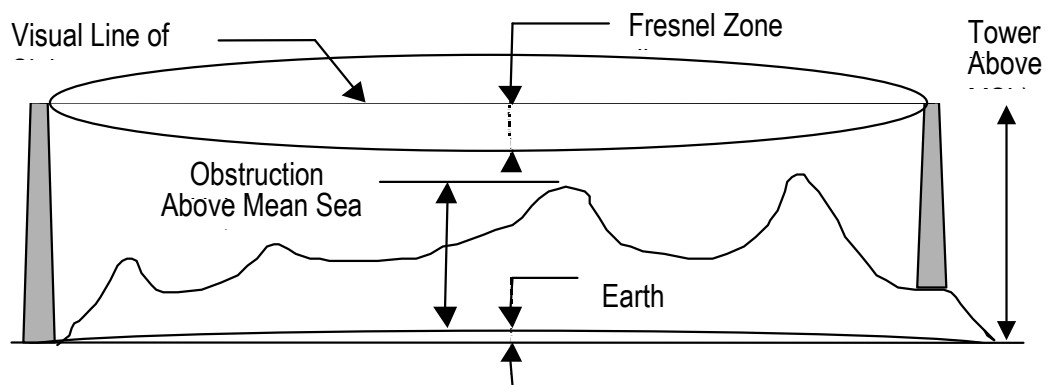


Figure 2-7: Line-of-sight (LOS) diagram

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 2-5.

Figure 2-8: 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 Router

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 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 2-19.

- g** Next, ground the lightning arrestor. For more information, see *Grounding the Lightning Arrestor*, page 2-19. 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 "LAN" 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 SPEEDLAN 9202/SPEEDLAN 9203 routers that will be communicating with this one.

SPEEDLAN 9202/SPEEDLAN 9203 Installation Diagram

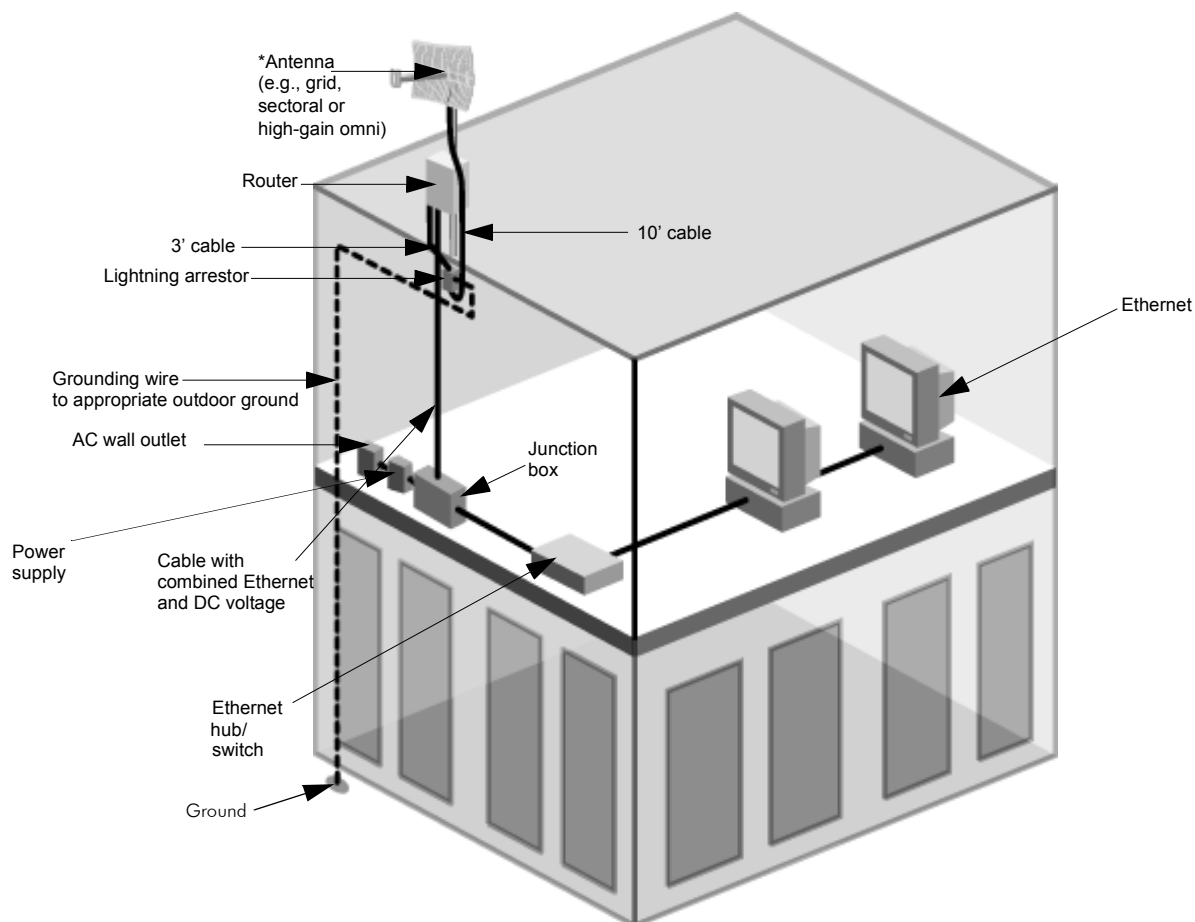


Figure 2-9: SPEEDLAN 9202/SPEEDLAN 9203 installation diagram

***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.

2-22

Chapter 3

General Functions of the Configurator

This chapter covers general functions when configuring any SPEEDLAN 9200 router, such as:

- General Information: *Manual Initial Configuration of the SPEEDLAN 9200*, page 3-2, *Logging on the SPEEDLAN 9200 Configurator*, page 3-10 and *Logging Off*, page 3-13
- Network menu: *IP Address Configuration*, page 3-19, *Alias IP*, page 3-22 and *Virtual Addresses*, page 3-23
- System menu: *Configuration Summary*, page 3-25, *SNMP*, page 3-26, *Version*, page 3-29; *Host Name*, page 3-29; *Password*, page 3-30 and *Reboot*, page 3-31
- Routing menu: *Def Gateway*, page 3-32; *RIP2 Setup*, page 3-32 and *RIP Settings*, page 3-33; *Authentication on RIP-2 MD5*, page 3-34, *Route Table*, page 3-36 and *Static Route*, page 3-37
- Wireless menu: *Configuring the Radio Parameters*, page 3-38 (i.e., setting the SSID, wireless mode, channel, signaling rate, turbo mode, Tx power and preamble); *Max Tx Retries and Signaling Rate Fallback*,



page 3-41; Request to Send (RTS) / Clear to Send (CTS), page 4-8; and Max Throughput (Regulating Bandwidth), page 3-43)

- DHCP Server menu: Setting Up DHCP, page 3-46; Adding a New DHCP Subnet, page 3-47, Adding a DHCP Client, page 3-49, Configuring DHCP Relay, page 3-50, Viewing Log Messages, page 3-51 and Forwarding Menu, page 3-51
- Forwarding menu: Forwarding Menu, page 3-51, Priority Queuing, page 3-52, Three Features of NAT, page 3-56, Firewall, page 3-63 and IP Sessions, page 3-68
- Diagnostics menu: Interface Statistics, page 3-69; ARP Table, page 3-71 and ICMP Statistics, page 3-71
- Admin menu: User Configuration Passwords, page 3-74; Software Update, page 3-75; Software Update, page 3-75, Support, page 3-76 and Current Sessions, page 3-77

Note: For more information on how the Configurator menu and this chapter is structured, see *Overview of the SPEEDLAN 9200 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 back to the manufacturer.

Manual Initial Configuration of the SPEEDLAN 9200

Each SPEEDLAN 9200 is produced with a default configuration that renders it usable in many applications. However, if you need to manually configure your SPEEDLAN 9200 router, follow the directions below.

Prerequisites

Configuration of the SPEEDLAN 9200 is done through the SPEEDLAN 9200 Configurator. In order to access the SPEEDLAN 9200 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 9200.

A TCP/IP connection to the SPEEDLAN 9200 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 9200 router through that wireless LAN.

The following section assumes that a SPEEDLAN 9200 router is being configured via its wired interface, possibly before it is installed at its intended physical location.

Connecting a SPEEDLAN 9200 and a Client PC

A connection between a SPEEDLAN 9200 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.

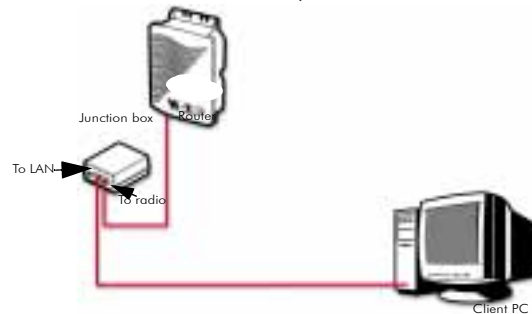


Figure 3-1: Using one crossover RJ-45 Ethernet cable

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

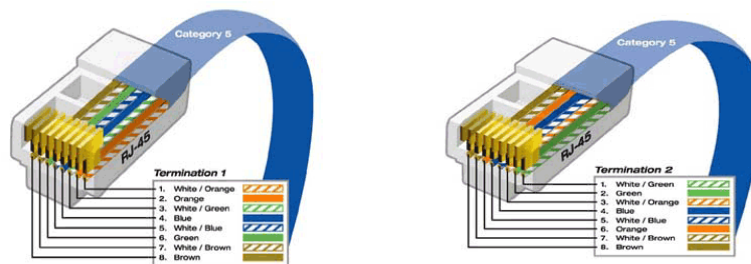


Figure 3-2: Crossover cable and pin out diagram

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.

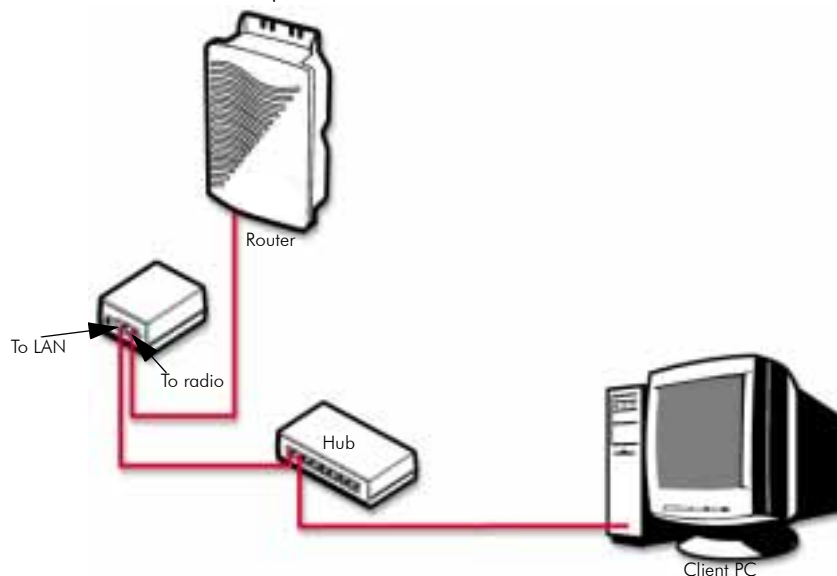


Figure 3-3: Using two straight-through RJ-45 Ethernet cables

Upon power up, a SPEEDLAN 9200 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 9200 will use the IP address, netmask, (etc.) that the DHCP server provides. Otherwise, the unconfigured SPEEDLAN 9200 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 9200 router and the client PC be on the same subnet. Otherwise, the ability to configure intervening routers may be required.

If the SPEEDLAN 9200 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 9200.
- 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 9200. 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 9200

Once your PC can access the SPEEDLAN 9200, you can open the client's browser and enter the IP address of the SPEEDLAN 9200 router. If using DHCP and DNS, it may be possible to refer to the SPEEDLAN 9200 router by its name.

Note: SPEEDView gives you a "management" view of the network. You will use the SPEEDLAN 9200 Configurator (web browser) to configure the SPEEDLAN 9200 routers. If you want to configure a router in SPEEDView, just double-click any router and it will open the SPEEDLAN 9200 Configurator. For more information about SPEEDView, see the SPEEDManage User Guide.

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 9200'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 9200s to communicate on this network.

Automating the Configuration of Multiple SPEEDLAN 9200s

In mesh mode, some of the configuration parameters for the SPEEDLAN 9200 are common to all SPEEDLAN 9200s 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 9200 should be rebooted when its configuration is complete. Multiple SPEEDLAN 9200 routers can be rebooted at the same time from either the SPEEDView application or the SPEEDLAN 9200 Configurator. To reboot the router in the SPEEDLAN 9200 Configurator, choose **Reboot** from the **System** menu (see *Reboot*, page 3-31).

Adding Additional SPEEDLAN 9200s to the Wired Network

If you need to add an additional SPEEDLAN 9200 to the wired network, do the following:

- Connect the additional SPEEDLAN 9200 routers to a hub or switch on the network and have DHCP assign IP addresses dynamically.
- Connect additional SPEEDLAN 9200 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 9200 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 Figure 3-4 on 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 configuration that is common for the base station, CPE, point-to-point, and mesh router is located in this chapter. At this time, star mode (base, point, CPE) is not available. Only mesh mode is available.**

Network menu

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 and add an Alias IP. For more information, see *IP Address Configuration*, page 3-19.

- If you need to view mesh routers currently on the network, *Mesh Nodes*, page 4-3. To authenticate your mesh routers and enable security for SPEEDMesh-enabled clients, see *Enabling Network Security*, page 4-4.

To enable AES encryption in your network, see *A. Enabling Encryption Between SPEEDLAN 9200 Routers*, page 4-4. To enable WEP security on a SPEEDMesh-enabled client, see *B. Enabling WEP Security Between a SPEEDMesh-Enabled Client and SPEEDLAN 9200*, page 4-5. To allow a mesh node in a 9200 network to communicate with a SPEEDMesh-enabled client, see *Enabling/Disabling the SPEEDMesh-Enabled Client*, page 4-6.

System menu

Use this menu to define information about the host, view information about the SPEEDLAN 9200 Configurator, set the current password and reboot the SPEEDLAN 9200 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. The SPEEDLAN 9200 contains a Simple Network Management Protocol (SNMP) Agent that provides a remote Network Management System (NMS) with read-only ("get") access to certain configuration and status parameters. For more information, see *SNMP*, page 3-26.

Routing menu

Use this menu to view and set routing configuration. For more information, see *Routing Menu*, page 3-31. This is also where you can set RIP-2 MD5 Authentication (see *Authentication on RIP-2 MD5*, page 3-34).

Wireless menu

Use this menu to configure the wireless parameters.

- If you choose **Configuration**, you will be able to set the following radio parameters: SSID, wireless mode, channel, signaling rate, turbo mode, Tx power and preamble. For more information, see *Configuration*, page 3-38 for more details.
- If you choose **Tx Retries**, 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 3-41.
- If you choose **Max Throughput**, you will be able to set the Max Transmit Data Rate in Kb/s. For more information, see *Max Throughput (Regulating Bandwidth)*, page 3-43.

Other specialized parameters not common under the Wireless menu for mesh routers:

- RTS/CTS has been added to this chapter. See *Request to Send (RTS) / Clear to Send (CTS)*, page 4-8.
- If you choose **Rx Threshold**, you will be able to set the threshold for each mesh router on the network. For more information, see *Receive (Rx) Threshold Parameter*, page 4-9 for details.
- If you choose **Blocked Links**, you will be able to block or unblock mesh routers. For more information, see *Blocked Links*, page 4-10 for more details.
- If you want to enter the number of times that a neighbor node can fail to reply to a neighbor discovery probe before it is declared unreachable, see *Link Expiration*, page 4-11.
- **DHCP**
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 3-44. You can also enable DHCP Relay and set the parameters as needed.
- **Forwarding**
Use this menu to control how traffic is forwarded through this router. For more information, see *Forwarding Menu*, page 3-51.
- **Diagnostics**
Use this menu to troubleshoot your SPEEDLAN 9200 network. For more information, see *Diagnostics Menu (Troubleshooting the Network)*, page 3-68.
- **Admin**
Use this menu to perform administrative tasks, such as setting up user password and permission information. You can also remotely control the SPEEDLAN 9200 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 3-74.
 - If you need to remotely reboot or turn off the SPEEDLAN 9200 mesh routers, see *Remote Control*, page 4-12.
 - If you need to remotely reboot a mesh router, see *Remote Control*, page 4-12. If you need to update the software on the mesh routers, see *Software Update*, page 4-12.

Diagram of SPEEDLAN 9200 Configurator Main Menu

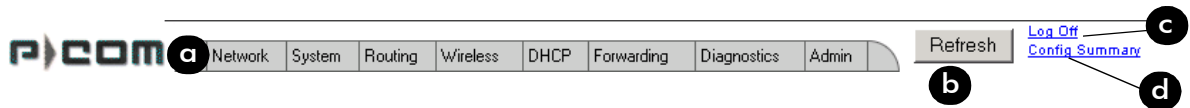


Figure 3-4: Main menu

- a Main menu:** Contains the following menus: Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics and Admin.
- b Refresh button:** Click to Refresh data on the web page.
- c Log Off link:** Click to close a user session.
- d Config Summary link:** Click to view a summarized list of the configuration on the routers (units). For more information, see *Configuration Summary*, page 3-25

Note: If you want to learn more about IP addressing, see *Basics of IP Addressing*, page 5-2.

Logging on the SPEEDLAN 9200 Configurator

To access the SPEEDLAN 9200 Configurator, open your web browser and enter the URL (https://) or IP address of the router you want to configure. The factory default IP address is 192.168.69.1.

Note: The SPEEDLAN 9200 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 9200 Configurator and SPEEDManage share the same password(s). The only place where you change the password for all of these is in the SPEEDLAN 9200 Configurator. For more information about SPEEDManage, see the SPEEDManage User Guide.

There are five classes of users on the SPEEDLAN 9200. 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 Recover in the SPEEDManage suite). Use this option when changing passwords. You cannot change the password to an existing password.
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 9200 network)
- **Wireless Read:** "wave_wireless" (account for the wireless SPEEDLAN 9200 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 and the SPEEDManage suite.

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 3-74.

Logging On

Follow these steps (starting on the following page) to log on to the SPEEDLAN 9200 Configurator.

- 1 Make sure you entered the correct URL or IP address of the router. For more information, see *Logging on the SPEEDLAN 9200 Configurator*, page 3-10.

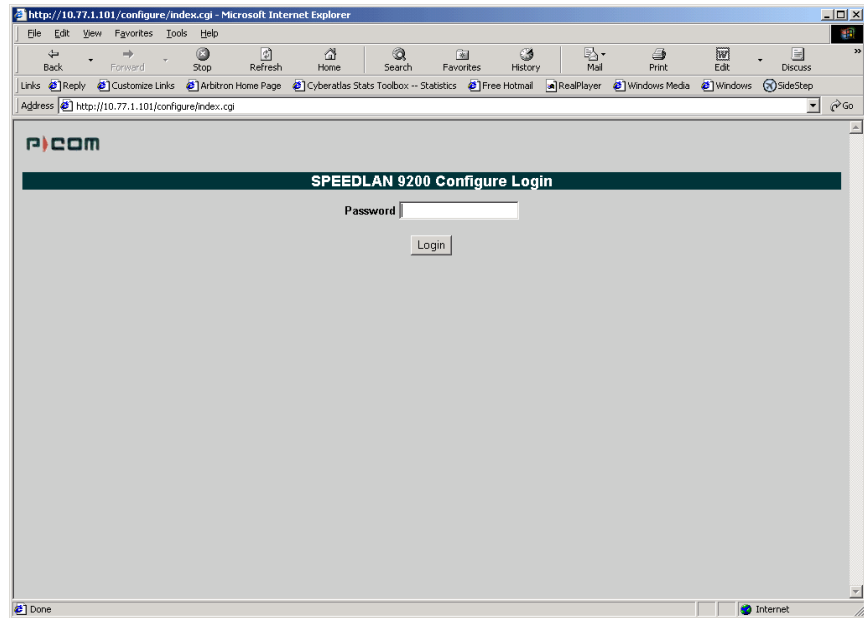


Figure 3-5: Login page

- 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 3-11.
- 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 red in the figure below).

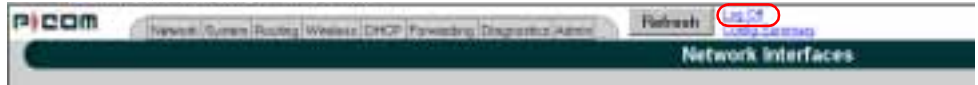


Figure 3-6: Logging Off

Understanding the Security Alert Screens

In order to avoid a security alert each time the SPEEDLAN 9200 Configurator is accessed, you must install its security certificate into Internet Explorer. If the SPEEDLAN 9200'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.

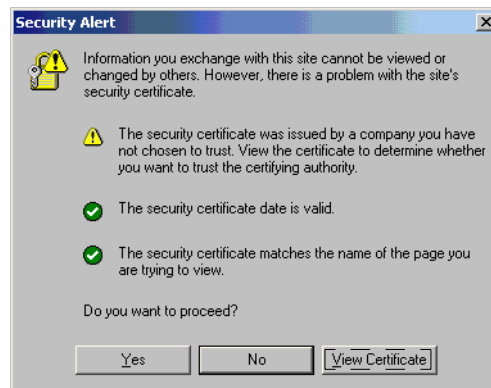


Figure 3-7: Security Alert screen

2 Click Install Certificate.

Figure 3-8: Certificate screen

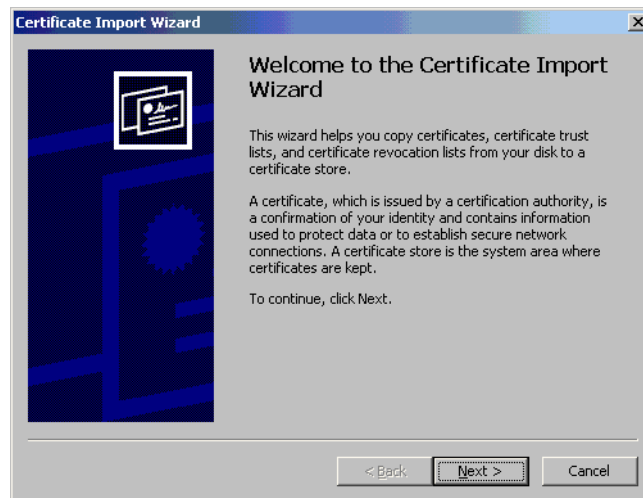
3 The Certificate Import Wizard will appear.

Figure 3-9: Certificate Import Wizard screen 1

- 4 Click **Next**.
- 5 The following dialog box will appear.

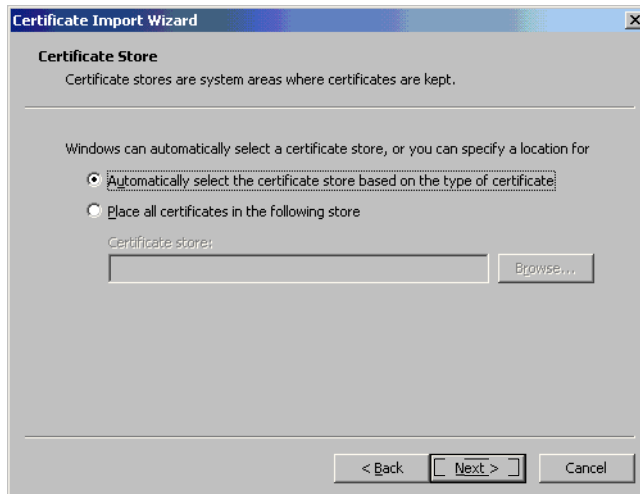


Figure 3-10: Certificate Import Wizard screen 2

- 6 Click **Next** again.
- 7 The following dialog box will appear.

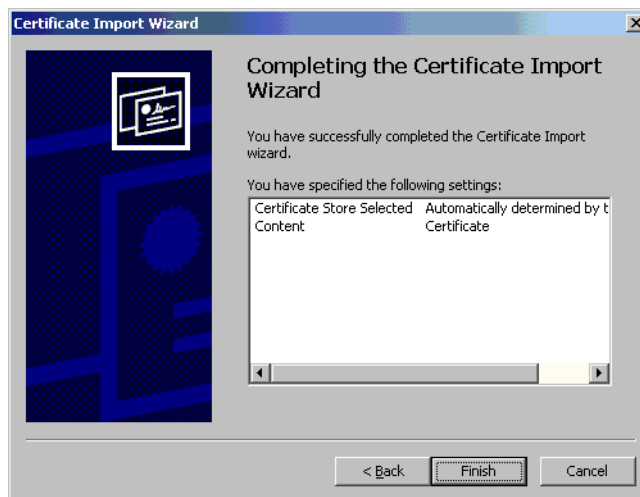


Figure 3-11: Certificate Import Wizard screen 3

- 8 Click **Finish**. A message will appear asking you "if you want to add a certificate to the Root Store." Click **Yes**.

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

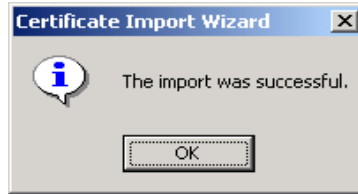


Figure 3-12: Certificate Import Wizard message box

You should not get the Security Alert the next time you access this site. The SPEEDLAN 9200 Configurator web site will appear.

After Logging On

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

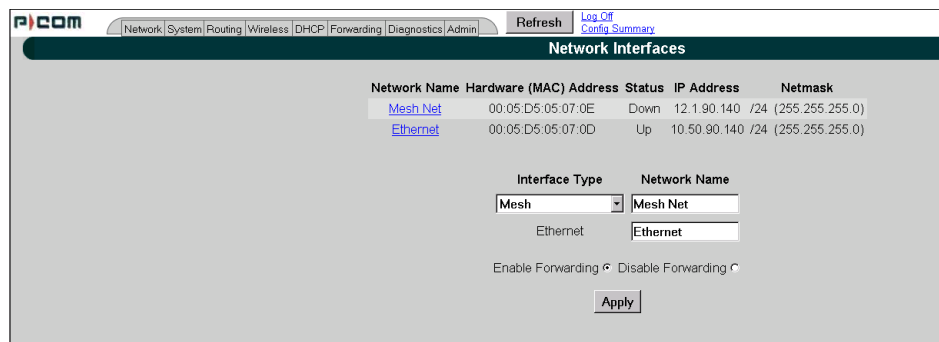


Figure 3-13: 1st screen after logging on

Elements to know on the Network Interfaces page:

- If you click the interface link, **Ethernet**, you will jump to the IP Addresses page.
- The "Interface Type" drop-down list is where you select the type of router. To select a different mode, select it and click **Apply**. The Configurator will log you out, and the next time you log in the mode will be available.
- Click the **Refresh** button to refresh data.
- The name you enter in the **Network Name** text box (shown in Figure 3-13 on page 3-16) 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.

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 3-13 on page 3-16, select the type of router (e.g., mesh) from the **Interface Type** drop-down list. Then, click **Apply**. The SPEEDLAN 9200 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*. (Directions are also described in the previous figure, see Figure 3-13 on page 3-16.)

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 9200 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 3-13 on page 3-16. 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.

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.

SPEEDLAN 9200 Firmware Updates, SPEEDManage or Other Utility Programs

Registered customers should check our web site on a regular basis for updates to router firmware, SPEEDManage, and other utility programs. If you haven't registered your products yet, you may do so by visiting "www.wavewireless.com". Then, click the "Support" directory. For more information about SPEEDManage, see the SPEEDManage User Guide.

If You Need a Temporary IP Address

- See the IP Recover chapter in the SPEEDManage User Guide.

OR

- If after learning the IP address of the Ethernet interface, you cannot log on to the router using the HTML Configurator (SPEEDLAN 9200 Configurator), then you will be able set a temporary Ethernet IP address so that a connection can be 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 3-13 on page 3-16. 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.

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 similar to the following will appear. (This is showing a Mesh interface.)

The screenshot shows the 'IP Address Configuration (Ethernet)' page. At the top, there is a navigation bar with links: Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, Admin. There are also 'Refresh' and 'Log Off' links. Below the navigation bar, a table displays the current configuration:

Hardware Address	IP Address	Netmask	Network	Broadcast	Mode
00:05:D5:05:07:0D	10.50.90.142	/24 (255.255.255.0)	10.50.90.0	10.50.90.255	Static

Below the table, there are three buttons: 'Restart Interface', 'Additional IP Addresses', and 'Restore Factory Default (192.168.69.1)'. The 'Use DHCP' section is active, showing a 'Client Hostname (Optional)' field. The 'Use this static address' section is also visible, with fields for 'IP Address' (10.50.90.142), 'Netmask' (/24 (255.255.255.0)), 'Network' (10.50.90.0), and 'Broadcast' (10.50.90.255). An 'Apply' button is at the bottom.

Figure 3-14: 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.
- **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.
- **Mode:** "Static" 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 3-15: CIDR information page

- **Restart Interface:** Click to restart the interface.
- **Additional IP Addresses:** Click this button to add an Alias IP. (You can add an alias IP address to the Ethernet interface.) This allows you to assign more than one IP address to an Ethernet interface. For more information, see *Alias IP*, page 3-22.
- **Restore Factory Default:** 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. (See also *Important Note about DHCP*, page 3-45.)

- **Use this static address:** 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 "**Use this static address**" 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 restart the interface. Otherwise, the information will not be updated. If you follow this step correctly, the next time you open the SPEEDLAN 9200 Configurator, these changes will be updated.

Alias IP

Note: Alias IP addresses can only be created for the Ethernet interface. They are not for the wireless interface.

To add an Alias IP, do the following:

- 1 Choose **IP Addresses + Ethernet** from the **Network** menu. Next, click the **Additional IP Addresses** button on the IP Address Configuration (Ethernet) page. The IP Addresses Configuration (for Ethernet) page will appear:

#	IP Address	Netmask	Network	Broadcast
1	192.168.202.34	/27 255.255.255.224	192.168.202.32	192.168.202.63

Figure 3-16: Adding an Additional IP Address (Alias IP)

- 2 Aliased addresses cannot be dynamically assigned from the DHCP server, so you must manually type in the Alias IP in the text box, circled above. Verify the netmask and click **Add**. Repeat this step for each Alias IP you add to the Ethernet interface.

Other elements on this window are described below:

- **# - (Address Number):** The first address is the primary IP address on the Ethernet interface. Addresses numbered 2 or higher are aliases.
- **IP Address:** Lists the IP address of the primary or alias address.
- **Netmask:** Lists the netmask of the primary or aliased address.
- **Network:** Lists the network number of the primary or aliased address.
- **Broadcast:** Lists the broadcast address of the primary or aliased address.

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 9200 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 and higher requires explicit creation of a virtual address prior to referencing it. Virtual addresses can be used to access the SPEEDLAN 9200 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 9200'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 3-17: 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.
- **SNMP:** The SPEEDLAN 9200 contains a Simple Network Management Protocol (SNMP) Agent that provides a remote Network Management System (NMS) with read-only ("get") access to certain configuration and status parameters. For more information, choose **SNMP**.
- 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. (You can also select the Config Summary link in the upper-right hand corner of each page.) This is very useful tool if you want to capture a screen shot of the summary and email it to 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.
- **SNMP:** Displays the read-only SNMP statistics, which are described in *SNMP*, page 3-26.
- **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, Max Throughput, Rx Threshold and Link Expiration.
- **Blocked Wireless Links:** Displays blocked links. For more information, see *Receive (Rx) Threshold Parameter*, page 4-9.

- **Wireless Security Settings:** See *Enabling Network Security*, page 4-4.
- **RIP Configuration:** The routing table displays routing information between destinations.
- **Routing Configuration:** Indicates if RIP is on or off, lists global settings and send and receive information, authentication and distribute information.
- **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:** Lists the implementation(s) of NAT: address sharing, internal servers and 1:1 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 **Firewall** link on the Configuration Summary page, it will bring up the Firewall 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.

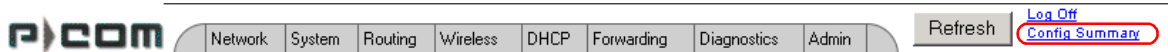


Figure 3-18: Config Summary Link

SNMP

The SPEEDLAN 9200 contains a Simple Network Management Protocol (SNMP) Agent that provides a remote Network Management System (NMS) with read-only ("get") access to certain configuration and status parameters. Those parameters are Management Information Base (MIB) objects. The currently supported MIBs are identified in table the MIBs.

The SPEEDLAN 9200 supports communications with an NMS using SNMP versions 1, 2 or 3. Secure communications between NMS and Agent requires use of SNMP version 3.

To enable the SNMP Agent, do the following:

- 1 Choose **SNMP** from the **System** menu. The following page will appear:

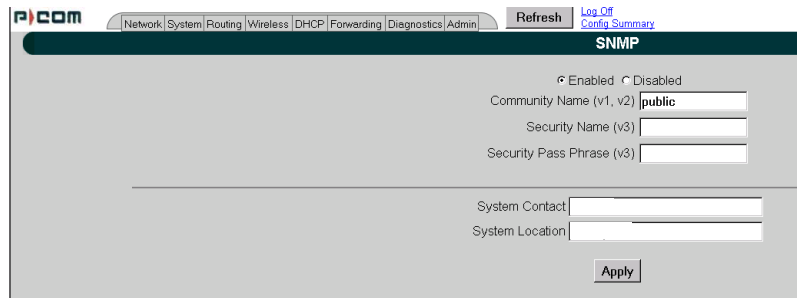


Figure 3-19: SNMP

- 2 Enter the following information, depending on the version(s) of the SNMP protocol supported by your NMS, and the level of security required:
 - **Community Name (v1, v2):** This is the read-only password. This entry is blank by default - you have to create one for the service to work. (If this entry is left blank, SNMP v1 or v2 service will be disabled.) The minimum number of characters entered is 1 and the maximum number of characters entered is 30. The default name is "public". If you want to use SNMP v1 or v2, enter the community name. Otherwise, leave this entry blank.
 - **Security Name (v3):** This is the read-only 'user name' used for SNMP v3. This entry should be set to a value that is only known by the network administrator. The minimum number of characters entered is 1 and the maximum number of characters entered is 30.
 - **Security Pass Phrase:** This is the 'password' for SNMP v3. The minimum number of characters entered is 8 and the maximum number of characters entered is 30.

Note: If you want to use SNMP v3, enter the Security Name and Security Pass Phrase. Otherwise, leave these entries blank.

- **System Contact:** This field should contain the identification of the contact person for this SNMP-managed node.

- **System Location:** This field should contain the administratively assigned name for this managed node. By convention, this is the node's fully qualified Internet Domain name (e.g., "noc.domain.com").
- 3 After you have entered the information described above, click **Apply**.
 - 4 Enable SNMP by selecting the **Enabled** option. When SNMP is enabled, the SPEEDLAN 9200 router will respond to SNMP queries initiated by your NMS. (See the section below for MIBII strings and definitions.) If you want to disable it, click the **Disabled** option. (SNMP is disabled by default.)
 - 5 You will receive a confirmation that your settings have been applied. SNMP is now enabled on the node you want to monitor.
 - 6 To view SNMP information, you must now use a NMS. Consult your NMS software for information on polling and logging the MIB objects.

Table 3-1: List of MIBs supported by SPEEDLAN 9200

MIB Name	RFC ⁺	SPEEDLAN 920x Firmware
MIB-II	RFC1213	1
SNMPv2-MIB	RFC3418	1

⁺RFC = Internet Engineering Task Force (IETF) Request for Comments
(<http://www.rfc-editor.org/rfc.html>)

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.

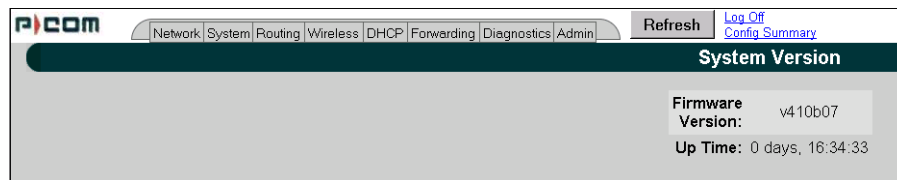


Figure 3-20: Version page

- **Firmware Version:** The version of the firmware.
- **Up Time:** The time since the last system startup was initialized.

Host Name

To enter the host name of a SPEEDLAN 9200 router, choose **Host Name** from the **System** menu. The following page will appear.

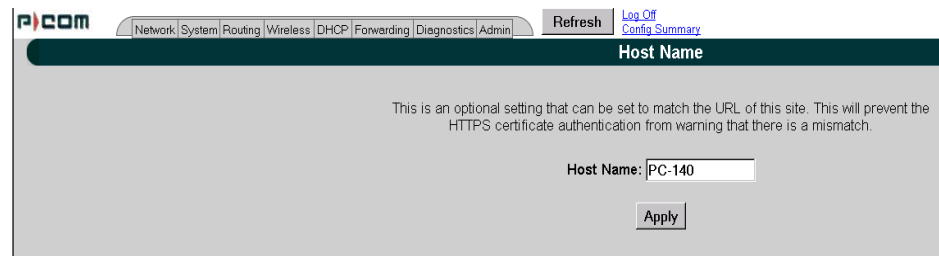
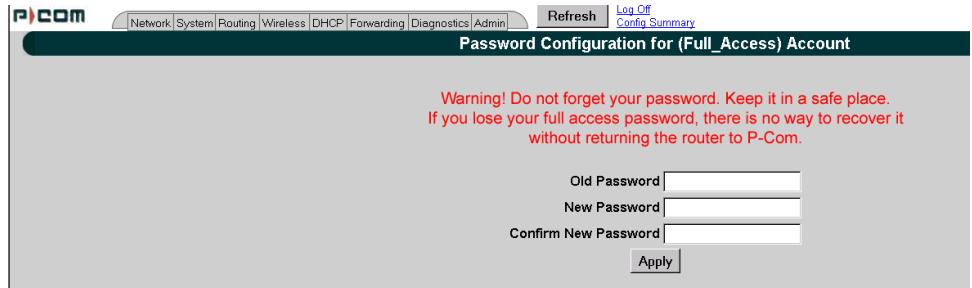


Figure 3-21: Host Name page

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 9200 Configurator. To modify password information, choose **Password** from the **System** menu. The following page will appear.



The screenshot shows the P-Com web interface. At the top, there is a navigation bar with links: Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, Admin, Refresh, Log Off, and Config Summary. Below this is a title bar that reads "Password Configuration for (Full_Access) Account". The main content area has a warning message in red text: "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 P-Com." Below the warning, there are three text input fields labeled "Old Password", "New Password", and "Confirm New Password". An "Apply" button is located at the bottom right of the form.

Figure 3-22: 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 the manufacturer.

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 SPEEDLAN 9200 to become fully operational following a reboot.

Routing Menu

Note that full interoperability with RIP-1 domains requires that the RIP-2 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 3-23: 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 9200 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 3-24: Default Gateway page

Default Gateway: Enter the IP address of the default gateway. This is the "door" 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 3-25: 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 what is connected to it. Do not select this check box if you do not want other devices on the network to know what network(s) the router is connected to.

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.

RIP Settings (Mesh Net)

Off ☐ On ☐

Receive: Global ☐ RIP 1 ☐ RIP 2 ☐ RIP 1 and 2 ☐

Send: Global ☐ RIP 1 ☐ RIP 2 ☐ RIP 1 and 2 ☐

Authentication

None ☐

Plain Text ☐

MD5 Key ☐

Network Route Filters

☐ Distribute any routes except for the following:

☐ Do not distribute any routes except for the following:

-----Filters-----

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

Delete

Add /24 (255.255.255.0)

Figure 3-26: 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 RIP-1 from/to the interface.
- **RIP 2:** Click this option to receive/send RIP-2 from/to the interface.
- **RIP 1 and 2:** Click this option to receive/send RIP 1 & 2 from/to the interface.

Authentication on RIP-2 MD5

- **None:** Select this option when authentication is not needed.
- **Plain Text:** Select this option to enable authentication (security) for legacy systems.
- **MD5 key:** Select this option to enable RIP-2 MD5 authentication for security. It is recommended that you select this option.

Note: Both the RIP-2 MD5 authentication key and Plain Text entries are restricted to digits or alphabetic characters. Both are entered like a password, but the characters are visible. The minimum amount of characters entered is **4** and the maximum is **16**.

What is RIP-2 MD5 Authentication?

Both RIP-1 and RIP-2 are vulnerable to hostile messages and attacks. This is because broadcast (RIPv1) or multicast (RIPv2) packets alone lack authentication. When RIP-2 is used with an authentication algorithm, such as MD5, network security is increased since the destination receiving the RIP packet knows that it was generated by a reliable source (i.e., the actual sender of the packet).

RIP-2 MD5 authentication transmits the output of the authentication algorithm rather than the RIP-2 authentication key. Therefore, the RIP-2 authentication key is never transmitted over the network and cannot be heard by other routers. This means a router can determine exactly who sent the message and not assume which router sent it.

Select one of the following options:

Note: You will need to enter the same authentication type and text / key for all participating SPEEDLAN 9200 routers.

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

Network Route Filters:

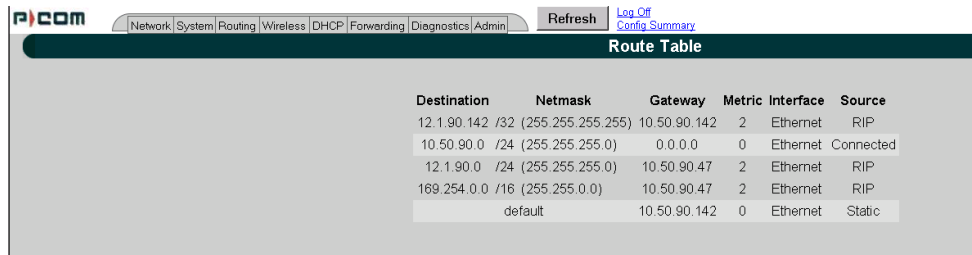
- **Distribute any routes except for the following:** Select this option to distribute all the network routes, except those which are selected in the Filters box.
- **Do not distribute any routes except for the following:** Select this option to only distribute the selected network routes in the Filters box.
- **Filters box:** Select those filters needed for option 1 or 2 as explained above.
- **Add:** Click this button to add a network route 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.



Destination	Netmask	Gateway	Metric	Interface	Source
12.1.90.142 /32	(255.255.255.255)	10.50.90.142	2	Ethernet	RIP
10.50.90.0 /24	(255.255.255.0)	0.0.0.0	0	Ethernet	Connected
12.1.90.0 /24	(255.255.255.0)	10.50.90.47	2	Ethernet	RIP
169.254.0.0 /16	(255.255.0.0)	10.50.90.47	2	Ethernet	RIP
default		10.50.90.142	0	Ethernet	Static

Figure 3-27: Route Table page

Each statistic is defined below:

- **Destination:** This is the destination network or host.
- **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.
- **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).
- **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.
- **Source:** This lists the how the information is routed to/from the router (e.g., RIP enabled, static or connected route).

Static Route

The Static Route page allows you to add static routes that the SPEEDLAN 9200 routers do not contain in their routing table. To open the Static Route page, choose **Static Routes** from the **Routing** menu.

The screenshot shows the P/COM web interface for the Static Routes page. At the top, there's a navigation bar with links like Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, and Admin. Below this, the 'Static Routes' section is active. It displays a table with columns: Destination, Netmask, Gateway, and Interface. The table is currently empty. Below the table, there's a 'New Static Route' form. This form has a 'Type' dropdown menu set to 'Network'. To its right are input fields for 'Destination' and 'Netmask' (set to '/24 (255.255.255.0)'). Below these are input fields for 'Gateway'. To the left of the form is a 'Local Interfaces' table with two entries: 'Mesh Net' with IP '12.1.90.140 /24' and 'Ethernet' with IP '10.50.90.140 /24'. An 'Add' button is located at the bottom right of the form.

Figure 3-28: Static Route page

Terms for this page are defined below:

- **Type:** Select either **Network** or **Host** from this drop-down list.
- **Network:** Traffic will be destined either to, from or between network segments.
- **Host:** Traffic will be destined either to, from or between specific hosts.
- **Destination:** The destination network or host.
- **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 3-21.
- **Interface:** Select the appropriate interface from this drop-down list.
- **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).

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**.

Configuring the Radio Parameters

Choose one of the options from the **Wireless** menu:

- If you choose **Configuration**, you will be able to set the following radio parameters: SSID, wireless mode, channel, signaling rate, turbo mode, Tx power and preamble. For more information, see *Configuration*, page 3-38 for more details.
- If you choose **Tx Retries**, 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 3-41.
- If you choose **Max Throughput**, you will be able to set the Max Transmit Data Rate in Kb/s. For more information, see *Max Throughput (Regulating Bandwidth)*, page 3-43.

Note: If you're looking for mesh-only functions like Blocked Links, Rx Threshold and Link Expiration, see the *Wireless menu*, page 4-7. If you're looking for the mesh Remote Control feature, see the *Admin Menu*, page 4-12. Mesh software/firmware update instructions are also located under the Admin menu section.

Configuration

- 1 To set these parameters, choose **Configuration** from the **Wireless** menu. The Configuration page will appear:

PICOM [Network | System | Routing | Wireless | DHCP | Forwarding | Diagnostics | Admin] [Refresh](#) [Log Off](#) [Config Summary](#)

Wireless Configuration

To apply settings to remote nodes, select them and then click Apply to Selected Nodes.

The screen will populate those fields for the Wireless Mode selected. Therefore, select the Wireless mode first.

Wireless Mode	5.8 GHz OFDM	Turbo	☐	Signaling Rates
Preamble	Long Only			☒ 6 Mb/s
Channel	165			☐ 9 Mb/s
TX Power	15 dBm (30mW)			☐ 12 Mb/s
SSID	SPEEDLAN9200			☐ 18 Mb/s
				☐ 24 Mb/s
				☐ 36 Mb/s
				☐ 48 Mb/s
				☐ 54 Mb/s

[Apply](#)

Current Settings

12.1.90.140
Ch. 36
1

Figure 3-29: Configuration page

- 2 Select one of the following from the **Wireless Mode** list:
 - 5.8 GHz OFDM
 - 2.4 GHz DSSS
 - 2.4 GHz DSSS/OFDM

Note: Extended turbo mode provides up to 108 Mb/s, which is automatically selected when you select 5GHz OFDM. If 5GHz OFDM is not selected, the "Turbo mode" is disabled. The Channel drop-down list will populate the appropriate values for the Wireless Mode you selected.

- 3 You can select a **Long**, or **Short & Long** preamble during the transmission process between two or more systems from the **Preamble** drop-down list. This parameter specifies the preamble setting in 2.4GHZ DSSS mode. There are two types of preamble, short and long - referring to the length of the sync field. The default setting is Short & Long. This setting is useful when you cannot determine the field size of the data being sent. The system will sync itself for both short and long. Users should select a **Long** preamble when there is a lot of interference or noise on the network. (A short preamble is more likely to be used in stable links with low noise levels.) The field size of a long preamble is 128 bits and a short preamble is only 56 bits.
- 4 Select the appropriate channel from the **Channel** drop-down list. This is the specific band of frequencies to determine the data path between routers. All SPEEDLAN 9200 routers expected to communicate in a network must have the same channel (frequency).

Table 3-2: Channel list

	5GHz OFDM	2.4 DSSS/OFDM	2.4 DSSS
Channels supported	149 (5.745GHz)	1 (2.412GHz)	1 (2.412GHz)
	153 (5.765GHz)	2 (2.417GHz)	2 (2.417GHz)
	157 (5.785GHz)	3 (2.422GHz)	3 (2.422GHz)
	161 (5.805GHz)	4 (2.427GHz)	4 (2.427GHz)
	165 (5.825GHz)	5 (2.432GHz)	5 (2.432GHz)
		6 (2.437GHz)	6 (2.437GHz)
		7 (2.442GHz)	7 (2.442GHz)
		8 (2.447GHz)	8 (2.447GHz)
		9 (2.452GHz)	9 (2.452GHz)
		10 (2.457GHz)	10 (2.457GHz)
		11 (2.462GHz)	11 (2.462GHz)

Note: Valid operating channels for the FCC and IC (Canada) are listed in *Channels for IEEE 802.11x, Appendix G-1*.

- 5 The following transmit power levels are currently available for 5GHz and 2.4: Select the appropriate value from the **TX Power** drop-down list.

Table 3-3: TX Power List

Frequency	5GHz	2.4GHz	
Specific Channels	All	1, 2, 10 and 11	3-9
TX Power supported	10 dBm (10mw) 13 dBm (20mW) 15 dBm (30mW) 17 dBm (50mW)	10 dBm (10mw) 13 dBm (20mW)	10 dBm (10mw) 13 dBm (20mW) 15 dBm (30mW) 17 dBm (50mW)

- 6 Check the appropriate **Signaling Rate** check boxes. This setting refers to the wireless signaling rate. The SPEEDLAN 9200 routers have different signaling rates that can be used, depending on the wireless mode selected.

The signaling rate is intended to control the transmit rate, depending on the quality of the link. If the link is getting better/worse, the signaling rate is automatically increased/decreased by one increment. By default, all the supported signaling rates for the appropriate protocol are selected. An alternative is to select a subset of the supported rates.

The table below lists the supported Signaling Rates for the wireless modes offered:

Table 3-4: Signaling Rates

	5GHz OFDM	Turbo Mode OFDM	OFDM/DSSS 2.4 OFDM/DSSS	2.4 DSSS
Signaling Rates Supported (in Mb/s)	6,9,12,18, 24,36, 48, 54	12,18,24,36, 48,72,96,108	1,2,5.5,11 (DSSS) 6,9,12,18, 24,36, 48, 54 (OFDM)	1,2,5.5,11

Note: For information about the minimum receiver sensitivity, see: “Minimum Receive Sensitivity (in dBm) for SL920x” on page 4 of Appendix D.

- 7 Enter the Service Set Identifier in the **SSID** text box. This is a sequence of characters that provides a unique name for the wireless network. This field has a maximum limit of 32 characters. The default value for SSID is "SPEEDLAN9200".

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.

P1COM Network System Routing Wireless DHCP Forwarding Diagnostics Admin Refresh Log Off Config Summary

Tx Retries

Allow signaling rate fallback on retry:						
1st	2nd	3rd	4th	5th	6th	7th
☒	☒	☒	☒	☒	☒	☒
Default						

Max Tx Retries: [Default](#)

[Apply](#)

Current Max Tx Retries and Fallback Settings

12.1.90.140
0
00000000

Figure 3-30: Tx Retries and Signaling Rate Fallback page

Note: To apply settings to other remote network nodes, select them and click **Apply to Selected Nodes**. If you want to select all of the routers, click **Select All**.

The default for Max Tx Retries is 6.

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.

Here is one example.....

2.4GHz DSSS 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 Tx Retries

P-Com 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.

Max Throughput (Regulating Bandwidth)

Max Throughput is useful to ISPs that want to regulate the maximum wireless bandwidth provided from each customer.

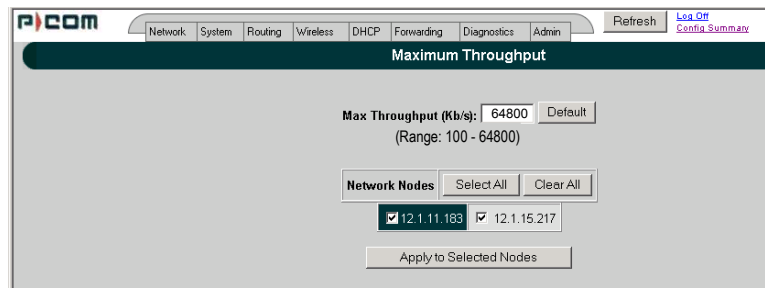


Figure 3-31: Max Throughput page

The Max Transmit Data Rate (in Kb/s) defaults are 29300 Kb/s for 2.4GHz & 5GHz OFDM modes, and 6500 Kb/s for DSSS. The range is from 100 to 64,800 Kb/s (6.5 Mb/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**.

DHCP Server Menu

The SPEEDLAN 9200 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 *Setting Up DHCP and DHCP Relay*, page 3-45.

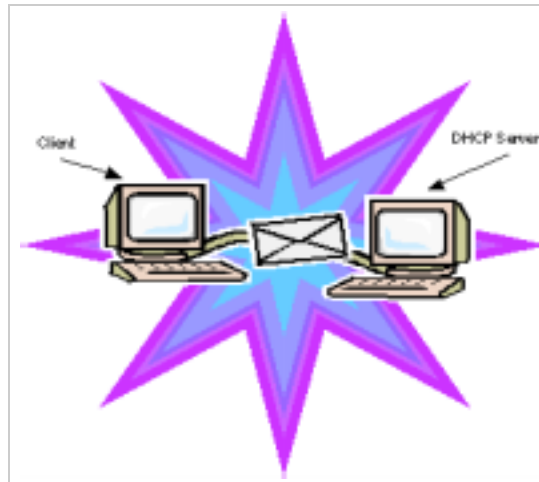


Figure 3-32: DHCP client and server

- 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 9200 Configurator allows you to assign IP addresses via DHCP on the interfaces.

Setting Up DHCP and DHCP Relay

These instructions will explain how to:

- Configure and Manage the SPEEDLAN 9200 DHCP Server
- Configure DHCP Relay

Important Note about DHCP

The DHCP Server serves IP addresses via the wireless interfaces in addition to the Ethernet interface. The DHCP Server does not serve other nodes on the same wireless cell.

For example, for Node A's DHCP server to serve IP addresses via its wireless interface, at least one of the following must be true:

- Another SPEEDLAN 9200 router on the same cell has DHCP Relay enabled, and configured to use Node A's DHCP server.
- Beyond the Ethernet of a SPEEDLAN 9200 router on the same cell, there is a router (wired or wireless) whose DHCP Relay is enabled and configured to use Node A's DHCP server.

Setting Up DHCP

To set up DHCP, do the following:

- 1 Choose **DHCP** from the main menu. Choose **Server** from the DHCP menu. This will display the DHCP page, as shown below:

Subnets to Serve				
Network Address	Netmask	Edit	Delete	Known Clients
10.50.90.0	/24 (255.255.255.0)			

Figure 3-33: Setting UP DHCP

- 2 This is where you can:
 - enable or disable the DHCP service
 - configure the subnet(s) that the DHCP server will manage
- 3 Select the following information:
 - **Disabled:** Select this option to disable the DHCP server.
 - **Enabled:** Select this option to enable the DHCP server.
 - **Apply:** Click this button to save the settings.
 - **Add Subnet:** Click this button to create a new subnet for the DHCP server to manage.

Note: If you have any problems configuring the DHCP server, you can look for logged messages generated by the server. For more information, see *Viewing Log Messages*, page 3-51.

Subnets to Serve Section

- **Network Address:** This is the network address.
- **Netmask:** This is the netmask for the network.
- **Edit:** Click this button to modify the subnet on the DHCP server.
- **Delete:** Click this button to remove the subnet from the DHCP server.

- **Known Clients:** Click this button if you want to assign specific IP addresses to specific client computers on a given subnet. This feature will also enable you to allow or decline specific client requests. For more information, see [Adding a Known Client](#).

Adding a New DHCP Subnet

- 1 To add a new DHCP subnet, click **Add Subnet** on the DHCP page. The following page will appear:

[Refresh](#)
[Log Off](#)
[Config Summary](#)

Network
System
Routing
Wireless
DHCP
Forwarding
Diagnostics
Admin

New DHCP Subnet

Mesh Net Network

12.1.90.0/24

10.50.90.0/24

Network

IP Start

Default Gateway

Domain Name

Netmask

IP End

Lease Time

minutes

Domain Name Servers

1

2

3

Add

Cancel

Figure 3-34: Adding a New DHCP Subnet

Notes: After you have added a subnet, you can click the IP address under the "Ethernet/Mesh Net" Network section, as circled Figure 3-34 on page 3-47, which populates the following information:

- Network
- Netmask
- IP Start
- IP End
- Default Gateway

Notes:

In most cases, if you use values that are compatible with the appropriate network, you will only need to change a few values (e.g., the last octet of "IP Start" and "IP End").

When you define the range of IP addresses to be assigned, make sure you do not include any of the static IP addresses that you have assigned on the network.

2 Enter the following elements:

- **Network:** Enter the network address.
- **Netmask:** Select the netmask from the drop-down list. This is the 4-byte number that masks the network part of the Internet Protocol address, so only the host computer part of the address remains.
- **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.
- **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 addresses and can be reassigned to another computer. The default is 480. (Entering "0" means the lease time never expires.)
- **Domain Name:** This is the internet domain of the organization, such as p-com.com.
- **Domain Name Servers:** Enter the IP address of your DNS server (optional). Prioritize them by listing the DNS to be used first, followed by the second and third DNS addresses.
- Click **Add** to implement the changes.

Adding a Known Client

If you click the **Known Client** button on the DHCP page, the following page will appear:

The screenshot shows the P-COM web interface. At the top, there is a navigation bar with tabs: Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, and Admin. To the right of the tabs are buttons for 'Refresh', 'Log Off', and 'Config Summary'. Below the navigation bar, the main heading is 'Known Clients for DHCP Subnet 10.50.90.0 /24 (10.50.90.150 - 10.50.90.155)'. Below this heading is a link 'Back to Main DHCP Page'. There are two radio buttons: 'Provide addresses for any requests.' (which is selected) and 'Provide addresses for known clients only.'. To the right of these radio buttons is an 'Apply' button. Below the radio buttons is an 'Add Client' button. At the bottom of the page, it says 'No Clients Defined.'

Figure 3-35: Adding a Known Client

The elements on this page are described below:

- **Provide addresses for any requests:** Provides addresses to any client.
- **Provide addresses for known clients only:** Provides addresses to the clients that appear in this list only.
- **Apply:** Click to implement changes.
- **Add Client:** Click this button to add a DHCP client. For more information, see Adding a DHCP Client.
- **Edit:** Click this button to edit a DHCP client. **Note:** Clicking this button displays similar information explained in the next section, but it allows you to modify the current client information. The fields will be populated, based on the client information entered.
- **Delete:** Click this button to remove a DHCP client.

Note: To go back to the main DHCP page, click the **Back to Main DHCP Page** link, as shown on the page above.

Adding a DHCP Client

When you click the **Add Client** button on the Known Clients for DHCP Subnet page, the following page will appear:

The screenshot shows a web browser window with the P/COM logo and a navigation menu (Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, Admin). The page title is "Add Known DHCP Client on Subnet 10.50.90.0 /24 (10.50.90.150 - 10.50.90.155)". The form contains the following fields and buttons:

Hardware (MAC) Address	

Name	IP Address
	10 50 90 0

Buttons: Add, Cancel

Figure 3-36: Adding a DHCP Client

This is where you can specify the name of the computer or device, MAC address and its corresponding IP address that should be assigned to that device at all times. The elements on this page are described below:

- **Hardware (MAC) Address:** In a LAN environment each computer contains its own Medium Access Control (MAC) address, which is the embedded and unique hardware number.
- **Name:** Enter the name of the host.

- **IP Address:** Enter the IP address for the client. Then, click **Add** to save changes, or click **Cancel** to return to the main Known Clients page for this subnet.

Note: The above fields (Hardware Address, Name and IP Address can be clicked to automatically populate the textboxes on this page.)

If you need to modify this information later, click **Edit** on the Known Clients for DHCP Subnet page.

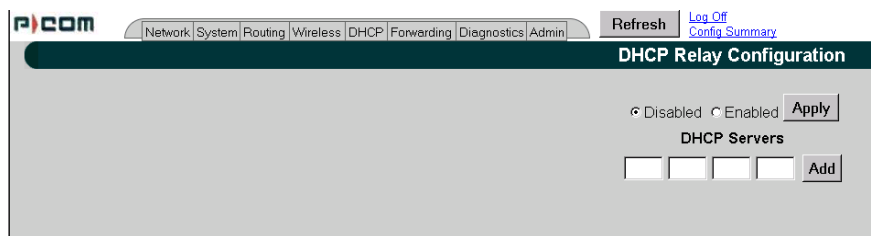
Note: If you have only one DHCP subnet defined, the DHCP server will offer addresses from that subnet. If you have two or more subnets defined, offered addresses will be from the subnet designated as the primary subnet, unless a match is found with a "known client" defined in a non-primary subnet.

Configuring DHCP Relay

DHCP Relay allows you to configure the SPEEDLAN 9200 to relay (forward) any DHCP requests originating on the Ethernet interface to a remote DHCP server. This allows you to use existing DHCP servers to assign IP addresses and other configuration parameters for SPEEDLAN 9200 routers via their wireless interfaces. If this service is enabled and no DHCP servers are listed, the SPEEDLAN 9200 will relay DHCP requests to the DHCP server that the SPEEDLAN 9200 used to get its interface address. If this service is enabled and the SPEEDLAN 9200 did not use DHCP to get an address for its interface, there must be at least one DHCP server address listed for this feature to work.

To add DHCP Relay information, do the following:

- 1 Choose **DHCP Relay** from the **DHCP** menu. The following page will appear:



The screenshot shows the web interface for configuring DHCP Relay. At the top, there is a navigation bar with tabs: Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, and Admin. The 'DHCP' tab is selected. To the right of the tabs are links for 'Refresh', 'Log Off', and 'Config Summary'. Below the navigation bar is a dark header with the text 'DHCP Relay Configuration'. The main content area has a light gray background. It contains two radio buttons: 'Disabled' (selected) and 'Enabled'. To the right of these is an 'Apply' button. Below the radio buttons is a section titled 'DHCP Servers'. This section contains four empty text input boxes and an 'Add' button to their right.

Figure 3-37: Configuring DHCP Relay

- 2 Enter the following information:
 - **Disabled:** Click to disable the DHCP Relay service.
 - **Enabled:** Click to enable the DHCP Relay service.
 - **DHCP Servers:** To enter a new DHCP server, enter the IP address and click **Add**. This is the IP address of the DHCP server that is offering IP addresses to its clients.
 - **Delete:** Click this button to remove information related to that DHCP server address.
- 3 Once you have set up the SPEEDLAN 9200 router, configure the clients to obtain an IP address from a DHCP server; **do this on the PC and not on the router!** If the SPEEDLAN 9200 is the DHCP server, it will get the IP address directly from it. If the DHCP server is located beyond the SPEEDLAN 9200 routers, the DHCP request will be forwarded to the DHCP server and then returned to the correct client machine.

If a SPEEDLAN 9200 router is serving as a DHCP relay and it has alias IP addresses, the IP network information that the SPEEDLAN 9200 relays to the DHCP server will always be that of the primary Ethernet IP.

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.

Forwarding Menu

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

- **Queuing** - Use this page to prioritize traffic out its wireless interface. Select the **Enabled** option to activate the Priority Queuing feature. This feature is enabled by default. For more information, see *Priority Queuing*, page 3-52.

- **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 3-53.
- **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 3-58.
- **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 3-60.
- **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 3-62.
- **Firewall** - The SPEEDLAN 9200 (via the SPEEDLAN 9200 Configurator) allows you to control incoming and outgoing traffic. A firewall prevents unauthorized access to a network. Utilizing the SPEEDLAN 9200 Configurator, SPEEDLAN 9200 routers can increase security and provide additional support to users of the network. See *Firewall*, page 3-63.
- **IP Sessions** - The SPEEDLAN 9200 firewall offers stateful packet filtering. IP Sessions allows you to view sessions whose state is currently active. See *IP Sessions*, page 3-68.

Priority Queuing

Use this page to prioritize traffic out its wireless interface. Select the **Enabled** option to activate the Priority Queuing feature. This feature is enabled by default. Select **Disabled** to turn off this feature. To open this feature, choose **Queuing** from the **Forwarding** menu. The following page will appear:

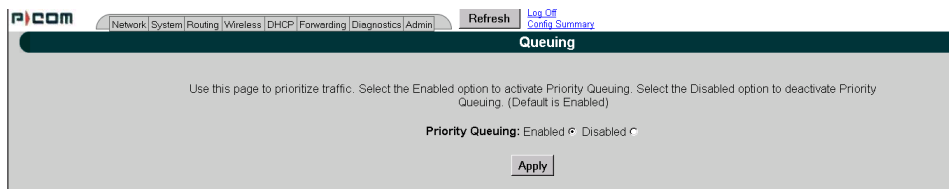


Figure 3-38: Setting Up Priority Queuing

- 1 Select **Enabled** or **Disabled**.
- 2 Click **Apply**.

Explanation of this feature

Despite having two physical interfaces, a SPEEDLAN 9200 router can experience congestion. That is because the interfaces' bit rates are not matched. Specifically, packets can ingress (enter) the Ethernet interface faster than they can egress (exit) the wireless interface. If this occurs briefly, it is called short-term congestion, which can cause increased packet delay and/or jitter. If congestion lasts too long, it can cause packet discard ("loss"). Long-term congestion in a SPEEDLAN 9200 will typically only occur when it receives excessive unthrottled UDP traffic at its Ethernet interface. TCP traffic will self-throttle, typically experiencing only short-term congestion, if any.

A SPEEDLAN 9200 mitigates short-term congestion by providing priority egress queuing at its wireless interfaces. With priority queuing, packets may be transmitted in a different order than they were received. This allows favoring network management, VoIP, and SCADA over SMTP, ftp, and NNTP (for example).

How does Priority Queuing work? The packets are prioritized into a hierarchy of queues, based on class of traffic. The highest priority queue packets are serviced first. When the highest queue is emptied, the next lower queue is serviced. The SPEEDLAN 9200 has four levels of priority queues. Queue 1 (the highest queue serviced) contains "management" traffic (i.e., RIP, Mesh, K2, SNMP). Queue 2, the next lower queue serviced, contains "real-time" traffic (i.e., VOIP, Video, SCADA). Queue 3, the next lower queue serviced, contains "non-real time interactive" traffic (i.e., HTTP, SSH and Telnet). Queue 4 (the lowest level queue serviced) contains all traffic that doesn't fit into one of the first three queues.

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 3-63.

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

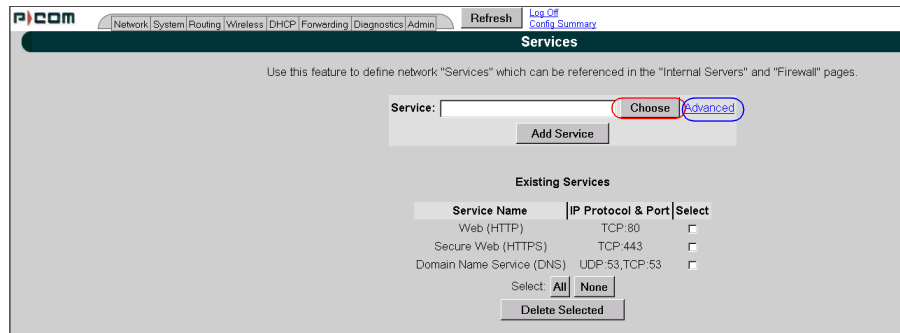


Figure 3-39: Services page

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.

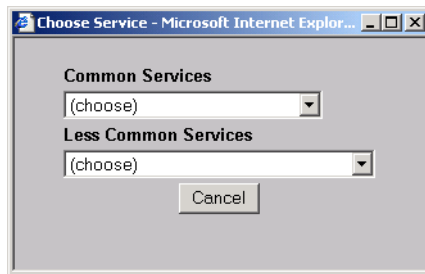


Figure 3-40: Choose Service

- 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 3-39 on page 3-54). The following pop-up will appear:

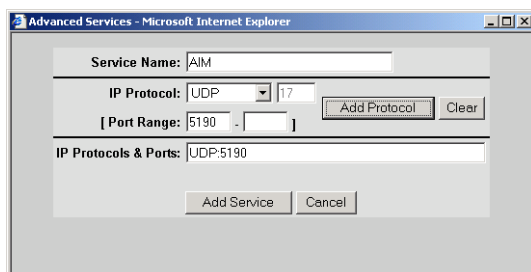


Figure 3-41: Advanced Services (adding AIM)

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.

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 9200 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 9200. The SPEEDLAN 9200 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 9200, 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 9200'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 9200 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 9200 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 "internal" IP address of the node. The node 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:

The screenshot shows the P1COM web interface for the 'Address Sharing (NAT)' configuration page. The breadcrumb trail at the top is: Network > System > Routing > Wireless > DHCP > Forwarding > Diagnostics > Admin. There are 'Refresh' and 'Log Off' links, and a 'Config Summary' link. The main heading is 'Address Sharing (NAT)'. Below it, a description states: '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.' The configuration section has two columns: 'Address to Share' and 'Share With Nodes On:'. Under 'Address to Share', there is a dropdown menu showing '12.1.90.141 (Star Net)'. Under 'Share With Nodes On:', there is a dropdown menu showing 'Star Net'. Below these are an 'Add' button and a link to 'Advanced'. The 'Existing Shares' section shows '(No shares defined.)'.

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 "12.1.90.141"). The "Share With Nodes" will automatically be selected (for the StarNet 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 9200 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 Advanced Address Sharing page will appear:

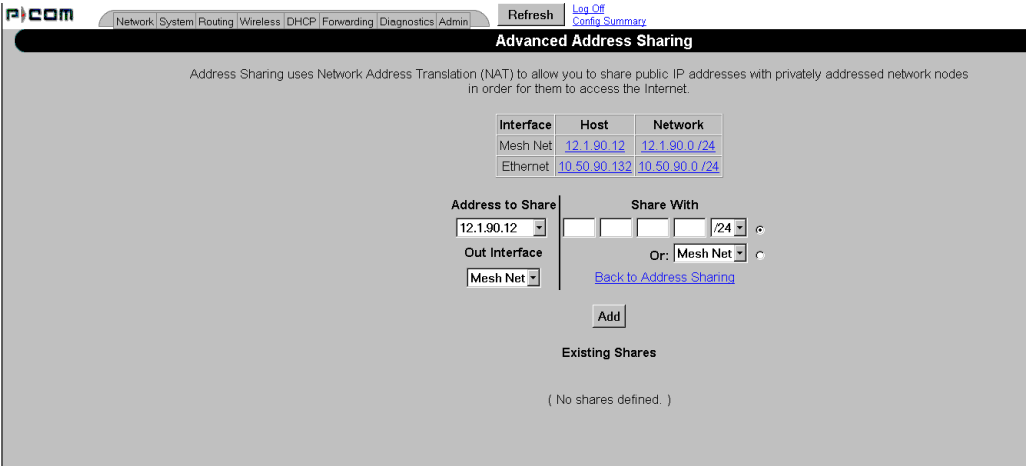


Figure 3-43: Advanced Address Sharing

Description of Advanced Address Sharing

The Address Sharing page allows you to share an address with all nodes connected to one of the SPEEDLAN 9200'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 9200 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:

P-COM Network System Routing Wireless DHCP Forwarding Diagnostics Admin Refresh Log Out Config Summary

Internal Servers (NAT)

This feature uses Network Address Translation (NAT) to allow you to host public services with internal (privately addressed) servers.

Interface	Host
Mesh Net	12.1.90.140 / 24
Ethernet	10.50.90.140 / 24

Service	External Address	Internal Server	Internal Port (if applicable)
Web (HTTP)	12.1.90.140		80

Add Server

Existing Internal Servers
(No Internal Servers defined.)

Figure 3-44: Internal Servers (NAT) page

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 3-53.)
- **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:

The screenshot shows the P1COM web interface for the 1:1 NAT configuration page. The breadcrumb trail is Network > System > Routing > Wireless > DHCP > Forwarding > Diagnostics > Admin. The page title is 1:1 NAT. A message states: "Use this feature to define a static mapping of a public (external) IP address to the IP address of a private (internal) network node." A red warning message says: "You must define at least one 'Virtual Address' to use in a 1:1 NAT mapping. (Found in 'Network / IP Addresses / Virtual Addresses')". Below this is a table with two columns: External Address and Internal Address. The External Address row shows "(none defined)" and the Internal Address row shows four empty input fields. Below the table is a section titled "Existing 1:1 NAT Mappings" which contains the text "(No mappings defined.)".

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 3-23.

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 9200 (via the SPEEDLAN 9200 Configurator) allows you to control incoming and outgoing traffic.

A firewall prevents unauthorized access to a network. Utilizing the SPEEDLAN 9200 Configurator, SPEEDLAN 9200 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:

Firewall

Enable Firewall ☐ Disable Firewall ☒ [Apply](#) Click to define an internal server.

The firewall is currently disabled.

Source

interface _____ Arriving on: **Mesh Net** ☐

source IP & netmask: [][][][] /32 ... ☐

Destination

Internal Servers: [\(define one\)](#) ☐

Going out: **Mesh Net** ☐

[][][][] /32 ... ☐ (highlighted with a red box)

Service: **{ Any }** ☐

☐ Allow ☒ Deny [Add](#)

Existing Firewall Rules

Rule	Action	Source	Destination	Service	Select
1	Deny	-- Default Forwarding Rule --			Change to Allow netmask IP & destination

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 9200 router to the ultimate DHCP server. These unicasts originate from the SPEEDLAN 9200 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 9200, 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 9200 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 3-68.

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.

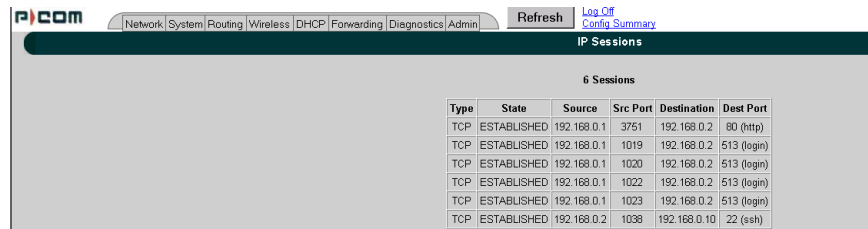
Rule 6 (AOL Instant Messenger: AIM): This rule will allow incoming traffic from the Star Net interface to enter the firewall so clients can run AOL Instant Messenger.

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 9200 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:



The screenshot shows the 'IP Sessions' page in a web browser. The page has a navigation bar with links: Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, Admin. There are also buttons for 'Refresh', 'Log Off', and 'Config Summary'. The main content area is titled 'IP Sessions' and shows '6 Sessions'. Below this is a table with the following data:

Type	State	Source	Src Port	Destination	Dest Port
TCP	ESTABLISHED	192.168.0.1	3751	192.168.0.2	80 (http)
TCP	ESTABLISHED	192.168.0.1	1019	192.168.0.2	513 (login)
TCP	ESTABLISHED	192.168.0.1	1020	192.168.0.2	513 (login)
TCP	ESTABLISHED	192.168.0.1	1022	192.168.0.2	513 (login)
TCP	ESTABLISHED	192.168.0.1	1023	192.168.0.2	513 (login)
TCP	ESTABLISHED	192.168.0.2	1038	192.168.0.10	22 (ssh)

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 an excellent tool. This process will help you with the performance evaluation. For more information on how to perform a link test, see The SPEEDManage User Guide. You can also perform a ping test if need.

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.

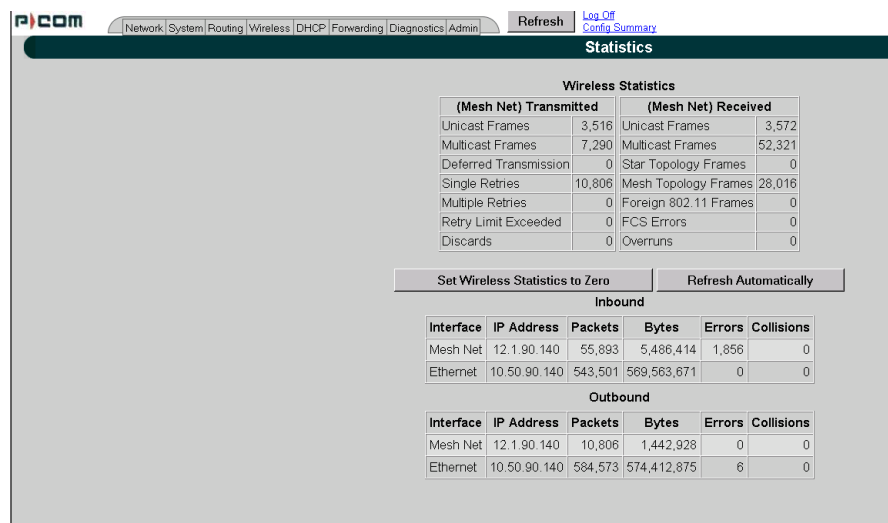


Figure 3-49: Interface Statistics page

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:

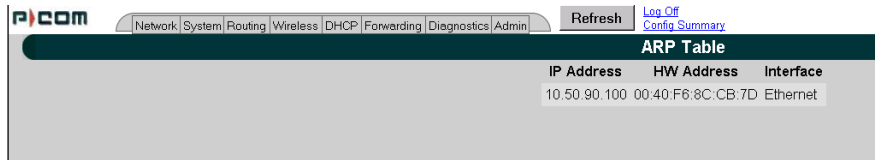
- **Interface:** The interface on which this entry is effective.
- **IP address:** This address tells the network how to locate the computers or network equipment connected to it.
- **Packets:** A unit of data transmitted between a receiver and a sender. Each packet contains embedded information, as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



ARP Table		
IP Address	HW Address	Interface
10.50.90.100	00:40:F6:8C:CB:7D	Ethernet

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.

In Bound			Out Bound		
	Value	?		Value	?
InMsgs	169021	?	OutMsgs	112648	?
InErrors	57029	?	OutErrors	0	?
InDestUnreachs	57029	?	OutDestUnreachs	56966	?
InTimeExcds	0	?	OutTimeExcds	0	?
InParmProbs	0	?	OutParmProbs	0	?
InSrcQuenches	0	?	OutSrcQuenches	0	?
InRedirects	0	?	OutRedirects	0	?
InEchos	55682	?	OutEchos	0	?
InEchoReps	56310	?	OutEchoReps	55682	?
InTimestamps	0	?	OutTimestamps	0	?
InTimestampReps	0	?	OutTimestampReps	0	?
InAddrMasks	0	?	OutAddrMasks	0	?
InAddrMaskReps	0	?	OutAddrMaskReps	0	?

Description

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. The user now has the ability to selectively enable alternate accounts (i.e., accounts other than Full Access). All alternate accounts will be disabled by default.
- Choose **Permissions** if you want to restrict certain settings to users.
- Choose **Software Update** to update the SPEEDLAN 9200 router.
- Choose **Support** to reset the entire configuration of the SPEEDLAN 9200 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 Passwords

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

The screenshot shows the 'User Passwords' configuration page. At the top, there's a navigation bar with links like Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, Admin, Refresh, Log Off, and Config Summary. Below this is a header 'User Passwords'. A button 'Reset All Passwords to the Factory Defaults (Including "Full Access")' is present. The main content is a table with the following structure:

	Account	Status	Password	Action
Enable	Wired Admin	[Disabled]		Set
Enable	Wired Read	[Disabled]		Set
Enable	Wireless Admin	[Disabled]		Set
Enable	Wireless Read	[Disabled]		Set

Figure 3-52: User Configuration page

The classes of users are described in *Classes of Users (and Passwords)*, page 3-11.

The User Configuration page allows you to set a password for each user account in the SPEEDLAN 9200 Configurator.

The user now has the ability to selectively enable alternate accounts (i.e., accounts other than Full Access). All alternate accounts will be disabled by default.

- 1 Do one of the following:
 - Click **Enable** to enable the account.

- Click **Disable** to disable the account
- 2** Enter the password for the user account in the textbox provided. The minimum password length is 8 characters. The maximum password length is 16 characters (including the underscore character or spacebar).
- 3** Click **Set**.

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

Software Update

The Software Update zip file (found on the www.wavewireless.com 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 (.wnn) file to perform the update.

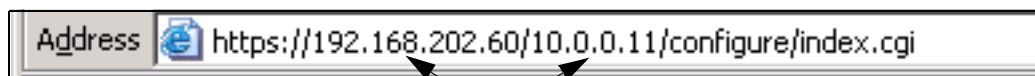
After you have unzipped the file, make sure you extract the update file (.wnn) file to your desktop. Then, follow the directions under the Software Update section for the particular router.

- For updating the software on a mesh router, see *Software Update, page 4-12*.

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.



displays two IP addresses (Proxy mode)

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:

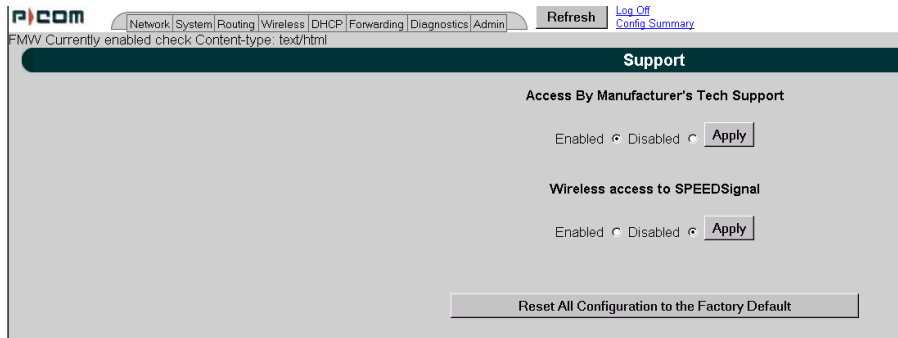


Figure 3-53: Support page

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 to 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.

Reset to Factory Default

If you need to reset the entire configuration of the SPEEDLAN 9200 to factory default settings, click **Reset All Configuration to the Factory Default**.

Current Sessions

P/COM			
Network	System	Routing	Wireless
DHCP	Forwarding	Diagnostics	Admin
Refresh			
Log Off			
Config Summary			
Current Sessions			
Remote Address	User	Idle (seconds)	Session Control
10.50.90.100	Full_Access	0	(this session)

Figure 3-54: 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.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

Chapter 4

Using the Configurator to Set Up Special Parameters for Mesh Routers

This chapter covers only those special parameters needed to set up mesh routers, such as:

- Network menu: *Interfaces for Mesh Mode*, page 4-2; *Mesh Nodes*, page 4-3; A. *Enabling Encryption Between SPEEDLAN 9200 Routers*, page 4-4; B. *Enabling WEP Security Between a SPEEDMesh-Enabled Client and SPEEDLAN 9200*, page 4-5 and *Enabling/Disabling the SPEEDMesh-Enabled Client*, page 4-6
- Wireless menu: ; *Receive (Rx) Threshold Parameter*, page 4-9, *Blocked Links*, page 4-10 and *Link Expiration*, page 4-11. To set up other wireless configuration parameters, see *Configuration*, page 3-38
- Admin menu: *Remote Control*, page 4-12; *Software Update*, page 4-12; and *Updating the Software on a Local Router and Remote Router*, page 4-13
-



For other common configuration, see *Overview of the SPEEDLAN 9200 Configurator General Main Menu*, page 3-7.

Network Menu

Interfaces for Mesh 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 mesh interface.

The screenshot shows the 'Network Interfaces' configuration page. At the top, there is a navigation bar with tabs: Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, and Admin. A 'Refresh' button and links for 'Log Off' and 'Config Summary' are also present. Below the navigation bar, the title 'Network Interfaces' is displayed. A table lists existing interfaces:

Network Name	Hardware (MAC) Address	Status	IP Address	Netmask
Mesh Net	00:05:D5:05:07:0E	Down	12.1.90.140	/24 (255.255.255.0)
Ethernet	00:05:D5:05:07:0D	Up	10.50.90.140	/24 (255.255.255.0)

Below the table, there are configuration options for a new interface:

- Interface Type:** A dropdown menu with 'Mesh' selected.
- Network Name:** A text input field with 'Mesh Net' entered.
- Interface Type:** A text input field with 'Ethernet' entered.
- Enable Forwarding:** A radio button that is selected.
- Disable Forwarding:** A radio button that is unselected.
- Apply:** A button to save the configuration.

Figure 4-1: Selecting mesh mode

- **Network Name:** This is the name you assign to the mesh interface.
- **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 **Mesh** from the **Interface Type** drop-down list. When finished, click **Apply**. This will tell the configurator that you are in mesh 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.

Mesh Nodes

The Mesh Nodes (Network Nodes) page shows you what other routers are currently in your network. This is useful if you do not have SPEEDView on your workstation. This page will appear when you choose **Mesh Nodes** under the **Network** menu.

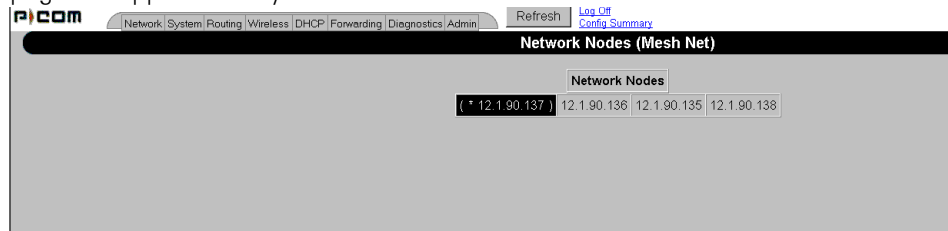


Figure 4-2: Network Nodes page

Enabling Network Security

This section is divided into two sections: A) enabling AES encryption between SPEEDLAN 9200 routers, and B) enabling WEP encryption between a SPEEDMesh-enabled client (PDA or laptop) and a SPEEDLAN 9200.

The screenshot shows the P1COM Network Security Configurations web interface. The top navigation bar includes tabs for Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, and Admin, along with a Refresh button. On the right, there are links for Log Off and Config Summary. The main content area is titled 'Network Security Configurations' and contains two sections. The 'Inter-9200 Security' section has a dropdown for 'Encryption Type' set to 'AES', an 'Apply' button, and a 'Pass Phrase' section with two text boxes labeled 'Pass Phrase' and 'Confirm', and a 'Change (Currently Set)' button. The 'Mobile Client Security' section has a dropdown for 'Encryption Type' set to 'WEP', a 'Key Format' dropdown set to 'Hexadecimal (0-9, A-F)', a 'Transmit Key' dropdown set to 'Key1', and three 'Length' dropdowns all set to '64 Bits', each followed by a 'Key' text box (Key1, Key2, Key3). An 'Apply' button is at the bottom of this section.

Figure 4-3: enabling AES/WEP

A. Enabling Encryption Between SPEEDLAN 9200 Routers

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 9200 routers use an AES 128-bit encryption key.

To enable AES between SPEEDLAN 9200 routers, do the following:

- 1 Choose **Security** from the **Network** menu. The Network Security Configurations page will appear.
- 2 Enter the pass phrase in the **Pass Phrase** text box. The minimum amount of characters is 8. The maximum number of characters is 32. Enter the pass phrase again in the **Confirm** text box. Then, click the **Change (Currently Not Set)** button to apply changes. You will receive a confirmation that the new pass phrase has currently been set.

- 3 To enable encryption on a SPEEDLAN 9200, choose **AES** from the **Encryption Type** drop-down list. "None" is selected by default. (If you select **None**, encryption is disabled.) Click **Apply** to implement your settings.

B. Enabling WEP Security Between a SPEEDMesh-Enabled Client and SPEEDLAN 9200

In a SPEEDLAN 9200 network, you can authenticate a SPEEDMesh-enabled client (PDA or laptop) with a standard security called Wired Equivalent Privacy (WEP). WEP encrypts data that is being transmitted over the wireless LAN. WEP protects the wireless links between clients and SPEEDLAN 9200 routers.

Note: WEP is an encryption scheme used to protect wireless data communications. WEP uses 64-bit, 128-bit or 152-bit key sizes to provide access control to wireless network and encryption security for each data transmission. To decode a data transmission, each point in a network must use an identical 64-bit, 128-bit or 152-bit key.

To enable WEP security, do the following:

- 1 If the Network Security Configurations page is not displayed on your screen, choose **Security** from the **Network** menu. On the bottom section of the Network Security Configurations page, choose **WEP** from the **Encryption Type** drop-down list. "None" is selected by default. (If you select **None**, encryption is disabled.)
- 2 Choose **Hexadecimal** or **ASCII Text** from the **Key Format** drop-down list.
 - "Hexadecimal" is a Base-16 numbering system. The means the 16 sequential numbers are used as a base unit (i.e., "0-9" and "A-F").
 - In ASCII text, each numeric, alphabetic or special character is represented with a 8-bit binary number (i.e., a consecution of eight 0s or 1s).
- 3 Select Key 1-3 from the **Transmit Key** drop-down list.
- 4 Select the length for the Transmit key by choosing either **64 Bits**, **128 Bits** or **152 Bits** from the **Length** drop-down list.

Note: 40-bit WEP and 64-bit WEP are two different names for the same encryption method. This level of WEP encryption has been called "40-bit" because it uses a 40-bit secret key along with a 24-bit initialization vector (i.e., $40 + 24 = 64$). The same is true for 104-128 bit and 128-152 bit WEP.

- 5 In the "Key1-3 text" boxes, enter the key value. For hexadecimal: a maximum of "10 "characters for 64 bits, "26" characters for 128 bits and 32 characters for 152 bits). For ASCII: a maximum of "5 characters for 64 bits, "13" characters for 128 bits and 16 characters for 152 bits.)
- 6 Click **Apply** to implement your changes.

Note: To enable the SPEEDMesh client, you must select the **Enable Mobile Client** check box. For more information, see *Enabling/Disabling the SPEEDMesh-Enabled Client*, page 4-6.

If WEP encryption is enabled, then:

- All frames are WEP-encrypted, regardless of the packet's destination address in the case if AES encryption is disabled, and
- All non-unicast frames are WEP-encrypted, regardless if AES is enabled or disabled.

Enabling/Disabling the SPEEDMesh-Enabled Client

SPEEDLAN 9200 routers allow any 802.11 SPEEDMesh-enabled client (i.e., PC, PDA, laptop) to join the wireless network. Network administrators can control access via WEP.

To enable or disable the SPEEDMesh client, do the following:

- 1 Choose **Mobile Client** from the **Network** menu. The Mobile Client page will appear:

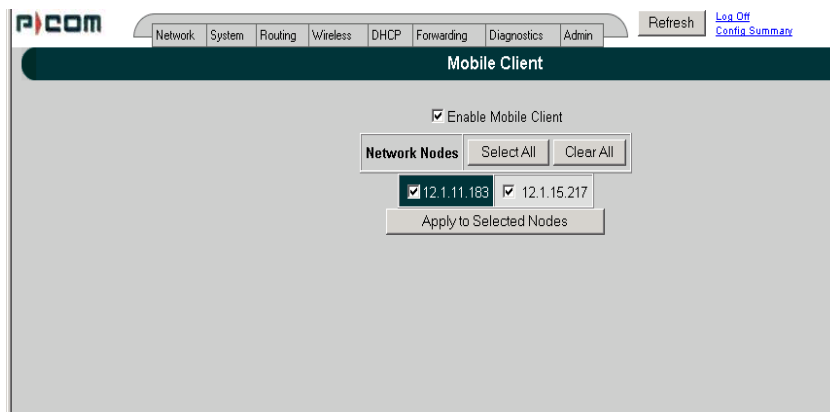


Figure 4-4: Enabling/disabling the SPEEDMesh client

- 2 To enable the SPEEDMesh client, select the **Enable Mobile Client** check box.
- 3 Select the nodes you want to enable for SPEEDMesh-enabled client mode node via one node, all nodes (via Select All) or unselect all nodes (via Clear All).
- 4 Click **Apply to Selected Nodes** to active the SPEEDMesh client(s).

Note: If you forgot to enable WEP security, see *B. Enabling WEP Security Between a SPEEDMesh-Enabled Client and SPEEDLAN 9200*, page 4-5.

Wireless menu

Choose one of the options from the **Wireless** menu:

- If you choose **Configuration**, you will be able to set the following radio parameters: SSID, wireless mode, channel, signaling rate, turbo mode, Tx power and preamble. For more information, see *Configuration*, page 3-38 for more details.
- If you choose **Tx Retries**, 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 3-41.
- If you choose **Max Throughput**, you will be able to set the Max Transmit Data Rate in Kb/s. For more information, see *Max Throughput (Regulating Bandwidth)*, page 3-43.
- If you choose **RTS/CTS** and enable RTS/CTS for a particular node, it will refrain from sending a unicast data frame until the node completes the "RTS/CTS handshake" with the receiving node. For more information, see *Request to Send (RTS) / Clear to Send (CTS)*, page 4-8.
- If you choose **Rx Threshold**, you will be able to set the threshold for each mesh router on the network. For more information, see *Receive (Rx) Threshold Parameter*, page 4-9 for details.
- If you choose **Blocked Links**, you will be able to block or unblock mesh routers. For more information, see *Blocked Links*, page 4-10 for more details.
- If you want to enter the number of times that a neighbor node can fail to reply to a neighbor discovery probe before it is declared unreachable, see *Link Expiration*, page 4-11.

Receive (Rx) Threshold Parameter

From a single mesh unit connected to a mesh network, you can set the receive threshold (given in dBm), for every mesh router in the network. The receive threshold specifies the minimum acceptable receive level for a datagram (defined for signaling rates, depending on the Wireless Mode you selected on the Wireless Configuration page). Any datagrams received below these levels will be discarded. This will provide better network stability for networks containing marginal links, since link state changes (and the corresponding routing changes) will be avoided for marginal links which are not capable of consistent communication.

By clicking the **Defaults** button, the values will go to their default values. If you enter a value of **0** (zero), you are turning the receive threshold parameter off.

P1COM | [Network](#) | [System](#) | [Routing](#) | [Wireless](#) | [DHCP](#) | [Forwarding](#) | [Diagnostics](#) | [Admin](#) | [Refresh](#) | [Log Off](#) | [Config Summary](#)

Rx Threshold

Rx Threshold is the minimum receive signal strength required to maintain a direct Mesh link. These settings will be applied to all routers in the Mesh network.

54 Mb/s	-		dBm
48 Mb/s	-		dBm
36 Mb/s	-		dBm
24 Mb/s	-		dBm
18 Mb/s	-		dBm
12 Mb/s	-		dBm
11 Mb/s	-		dBm
9 Mb/s	-		dBm
6 Mb/s	-		dBm
5.5 Mb/s	-		dBm
2 Mb/s	-		dBm
1 Mb/s	-		dBm

[Defaults](#)

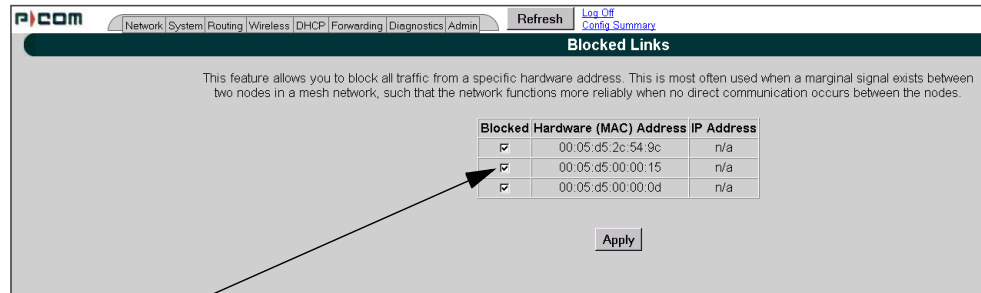
[Apply](#)

Figure 4-5: Rx Threshold page

The current Rx thresholds for your wireless mesh router(s) are listed in the Current Rx Thresholds section. Their signaling rates are also listed, as described above.

If you click **Default**, it will load the current default setting for the Configurator. Click **Apply** when finished.

Blocked Links



Select the checkbox under **Blocked** to block a mesh router. Leave it unselected when you want leave the mesh router unblocked.

Figure 4-6: Blocking Mesh Routers

This feature allows you to block all traffic from a specific hardware address. This is most often used when a marginal signal exists between two nodes in a mesh network, such that the network functions more reliably when no direct communication occurs between the nodes. To completely block a link you must perform the same action on the remote node.

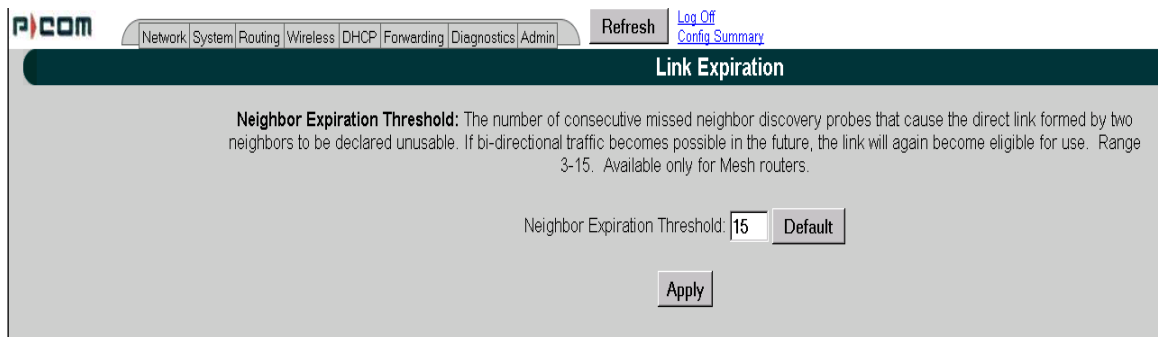
Note: If you blocked a mesh router, the next time it is rebooted it will remain blocked. If you want to unblock the router, make sure that the **Blocked** check box is not selected.

Note: Click **Apply** when finished.

Link Expiration

This page is only available for mesh routers.

To use this feature, choose **Link Expiration** from the **Wireless** menu. The following page will appear:



The screenshot shows the P1COM web interface. At the top, there is a navigation bar with tabs: Network, System, Routing, Wireless, DHCP, Forwarding, Diagnostics, and Admin. The 'Wireless' tab is selected. To the right of the tabs are buttons for 'Refresh', 'Log Off', and 'Config Summary'. Below the navigation bar is a dark blue header with the text 'Link Expiration'. The main content area has a light gray background. It contains a paragraph explaining the 'Neighbor Expiration Threshold' and a form field for setting this threshold. The form field is labeled 'Neighbor Expiration Threshold:' and has a text input box containing the value '15' and a 'Default' button. Below the form field is an 'Apply' button.

Neighbor Expiration Threshold: The number of consecutive missed neighbor discovery probes that cause the direct link formed by two neighbors to be declared unusable. If bi-directional traffic becomes possible in the future, the link will again become eligible for use. Range 3-15. Available only for Mesh routers.

Neighbor Expiration Threshold:

Figure 4-7: Link Expiration

Neighbor Expiration Threshold: The number of consecutive missed neighbor discovery probes that cause the direct link formed by two neighbors to be declared unusable. If bi-directional traffic becomes possible in the future, the link will again become eligible for use. The range for this parameter is 3-15. The default is 7.

After selecting a value for the parameter described above, select the nodes to which this value will be sent (via the **Select All** or **Apply to Selected Nodes** buttons). Then, click **Apply**.

Admin Menu

Remote Control

To remotely reboot or turn off the SPEEDLAN 9200 mesh routers, choose **Remote Control** from the **Admin** menu. The following page will appear.

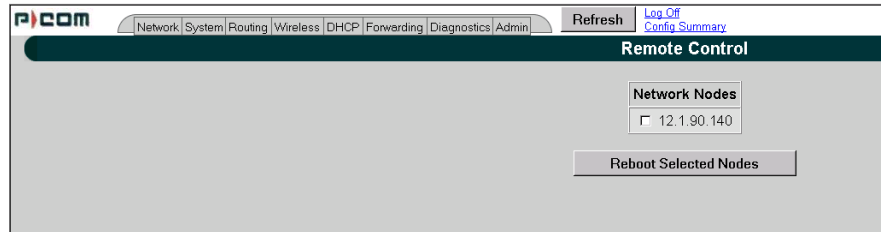


Figure 4-8: Remote Control for mesh mode

Select the mesh routers you want to reboot and click **Reboot Selected Nodes**. If there are remote nodes, select them and click **Select All** or **Clear All**.

Software Update

Note: The Software Update zip file (found on www.wavewireless.com/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 (.wnn) file to perform the update. After you have unzipped the file, make sure you extract the update file (.wnn) file to your desktop. Then, follow the directions below.

To update the software on the local router or on the remote mesh routers, choose **Software Update** from the **Admin** menu. The Software Update page will appear.

Updating the Local Router

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



Figure 4-9: Updating the software for mesh local router

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: All units are automatically rebooted after a successful upgrade.

Updating the Software on a Local Router and Remote Router

To update the software on a location router and on a remote router, choose it under the **Software Update** submenu (e.g., MeshNet).

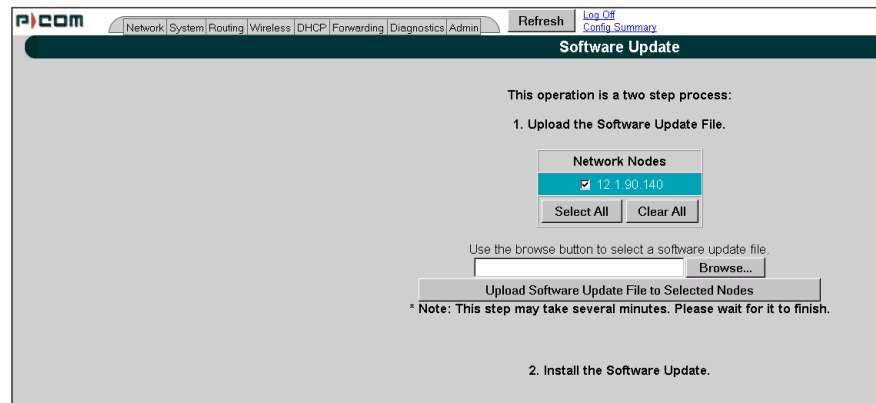


Figure 4-10: Updating the software for a local mesh and remote router

This operation is a two-step process:

- 1 Select the remotes 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.

Chapter 5

Basics of IP Addressing

Main sections in this chapter:

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



Basics of IP Addressing

IP Addressing is important because it tells the network how to locate the computers or network equipment connected to it. IP addresses are given so each computer or equipment on the network has a unique routable address. IP addressing provides the following information:

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

What is an IP address?

An IP address is a unique 32-bit identifier that contains:

- Four octets (e.g., decimal 192.0.2.56).
- Two sections: the network address and the node address (also known as the host address).

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

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

Internet Address Classes

Understanding this methodology is difficult; therefore, let's explain this in easier terms. The first octet(s) defines the "class" of the address, which is the only method to tell the size of the network (how big) and where the internet address belongs.

There are three main classes:

- Class A: 35.**0.0.0**
- Class B: 128.5.**0.0**
- Class C: 192.0.2.**0**

-non-bolded text = Part of network address

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

This specification simplifies the way routers handle the messages (packets) and speed up the forwarding process.

In fact, IP defines five classes:

- **Class A** addresses uses 1 octet for the network portion and 3 octets for the node (or host) section of the address. This provides up to 128 networks with 16.7 million nodes for each network.
 - First octet is assigned as network address
 - Remaining octets used for node addresses
 - Format: network, node, node, node
 - In IP address 49.22.102.70, "49" is network address and "22.102.70" is the node address—all machines on this network have the "49" network address assigned to them
 - Maximum of 16,777,216 node addresses
- **Class B** addresses uses 2 octets for the network portion and 2 octets for the node (or host) section of the address. This provides up to 16,384 networks with 64,534 nodes for each network.
 - First 2 octets are assigned as network address
 - Remaining octets used for node addresses
 - Format: network, network, node, node
 - In IP address 130.57.30.56, "130.57" is the network address, and "30.56" is the node address
 - Maximum of 65,534 node addresses
- **Class C** addresses use 3 octets for the network portion and 1 octet for the node (or host) section of the address. This provides 16.7 million networks with 256 nodes for each network.
 - First three octets are assigned as network address
 - Remaining octet used for node address
 - Format: network, network, network, node
 - In IP address 192.0.2.102, "192.0.2" is the network address, and "102" is the node address
 - Maximum of 28 or 254 node addresses

- **Class D**
 - Range is 224.0.0.0 to 239.255.255.255
 - Used for multicast packets (i.e., host sends out router discovery packets to learn all of the routers on the network)
 - Netmask = /32

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

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

Note: Public addresses can include a network address assigned from the network administrator or from the IP provider. Also, there is one network in each class that is defined for private use, allowing the creation of internal networks. These addresses are Class A: 10.0.0.0, Class B: 172.16.0.0, and Class C: 192.168.0.0.

Subnetting a Network

The increasing number of hosts and networks make large impractical address blocks that are not smaller than 255. In order to keep the IP address block small, so routers can manage them more efficiently, a smaller network definition is created. This is called a subnet. Subnets are intended to:

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

Default Subnet masks

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

Note: Subnet mask is bolded and corresponds to the network portion of the IP address.

What is a Subnet?

A subnet allows you to create multiple networks within one Class A, B, or C network. Each subnet contains a netmask that helps routers identify the subnet beginning and size.

What is a Subnet Mask?

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

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

Example of Subnetting:

For example, a Class C network contains three masked octets (255.255.255). The last octet (0) identifies nodes (i.e., computers).

If Router D is reading IP Addresses 192.0.2.1 (let's call this IP Address 1) and 192.0.2.64 (let's call this IP Address 2) on this Class C network, it would send IP Address 1 to Subnet A and IP Address 2 to Subnet B. The remaining nodes in each subnet (A through D) on this network can contain up to 254 pieces of network equipment (computers, printers, fax machines, bridges or routers, etc.).

Diagram of Subnetting a Network

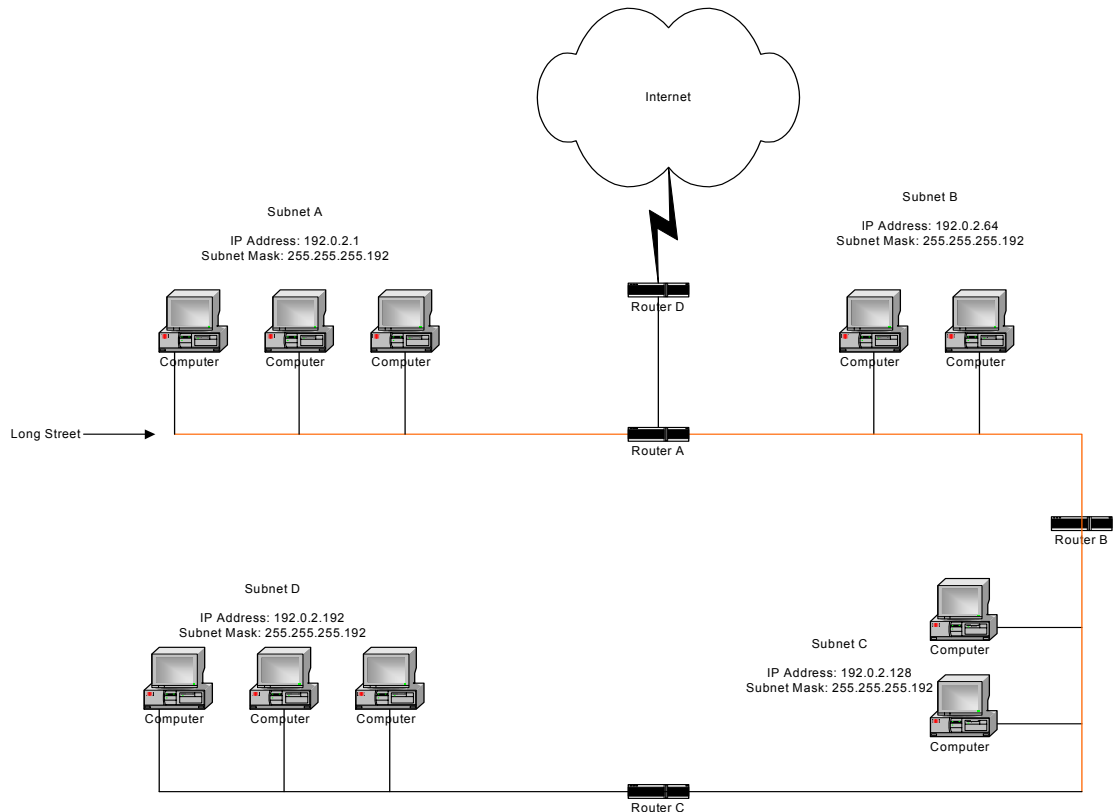


Figure 5-1: Subnetting diagram

Still confused?

An easier method to explain this concept is to use the classic "mailing" analogy used in IP addressing. Consider that this network, called Long Street, is four blocks long. There are 254 houses on Long Street, and each block contains 64 houses. Houses 1 to 63 reside on Block A. Houses 64 to 127 reside on Block B. Houses 128 to 191 reside on Block C. Houses 192 to 254 reside on Block D. Think of each block as a subnet. This

means that Blocks A, B, C, and D are all part of Long Street, which is also known as the network in this example. The mailman would organize the letters (or IP addresses for network equipment) by creating four piles (one for each block, or subnet). As soon as the mailman picks up pile A in his hand, he knows which block to turn on. This same reasoning applies to piles B, C, and D as well. Router D knows exactly which subnet to transfer (or turn) the packets to by reading its IP and subnet mask address. Note that each subnet on this network is 255.255.255.192. Why is 192 the last octet in the subnet mask and not 64? The last octet, 192, is the mask that allows 64 "houses" to reside on the street.

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

How does a network administrator assign an IP address?

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

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

- **Manual (static) Addressing - Is 'Manually Configure' option on Interfaces Parameters page of SPEEDLAN 9200 Configurator**
Each device connected to the Internet must have its own unique IP address. Also, if a computer is being used as a server, you will assign it a permanent IP address. This enables other computers to connect to it. Static addressing is also beneficial to users that need to maintain a "constant" connection to the Internet. This will enable users to easily access the IP address.
- **Automatic (dynamic) Addressing - Is 'Use DHCP' option on Interface Parameters page of the SPEEDLAN 9200 Configurator.**
A DHCP (Dynamic Host Configuration Protocol) server assigns the IP address to each computer as the computer connects to the network. If a computer moves to a new network (i.e., great for temporary employees or mobile users), it must be assigned a new IP address for that network. DHCP can be used to manage these assignments automatically. DHCP is described in further detail below.

What is DHCP?

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

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

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

Figure of DHCP Addressing

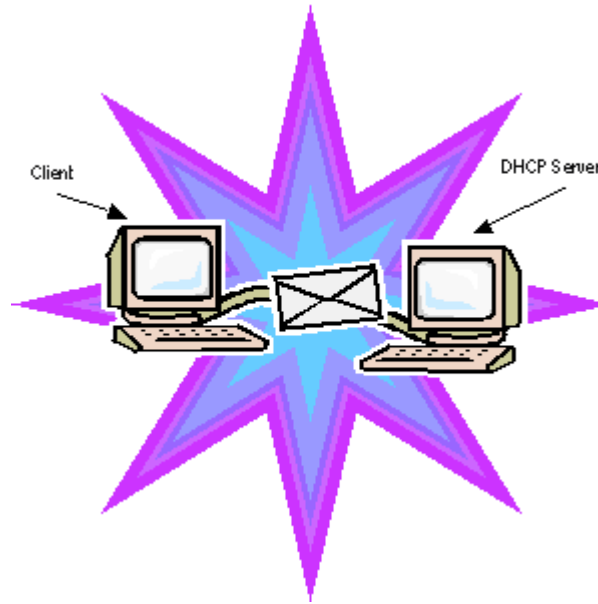


Figure 5-2: DHCP client and server

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

What is NAT?

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

Network Address Translation (NAT) occurs when there is a translation among an Internet Protocol (IP address) used within one network (designated as inside network) to a different IP addresses within another network (designated as outside network).

Network Address Translators (NATs) allow companies to decrease the number of global

IP addresses. This enables companies to communicate with other devices on the Internet with a single global IP address (or more than one IP address).

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

NAPT

What differentiates NAPT from NAT? NAPT (or Network Address Port Translation) not only translates the IP address but also the transport layer port. Thus, if an inbound packet was addressed to a web server port on 80, the NAPT device would translate and pass to the packet to the private network's web server. Without port translation, the NAT device has no means of knowing which host in the private network can pass packets to other devices. For an example see, *Diagram of Incoming NAT*, page 5-12.

Diagram of Outgoing NAT

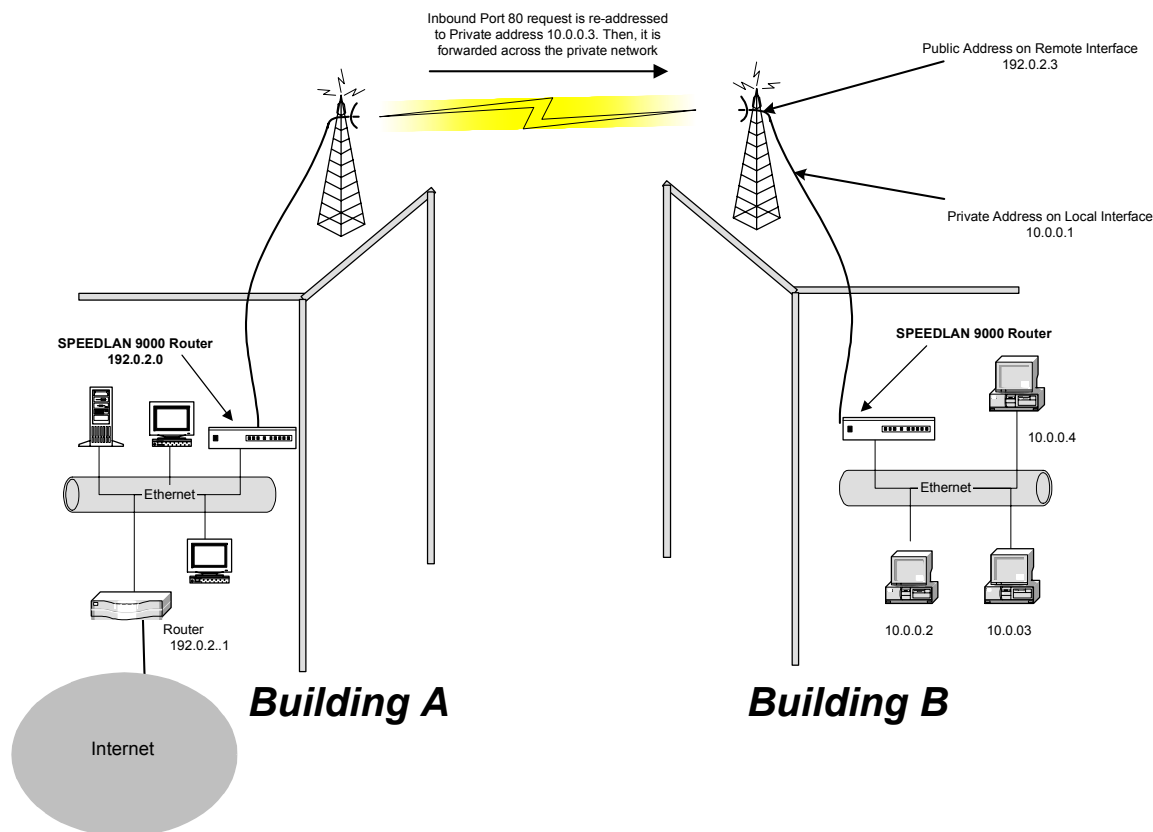


Figure 5-3: Outgoing NAT

As the packet is transmitted from the private network (in Building B) across the public network (public address in Building A and the Internet), the packet will be re-addressed as 192.0.2.3 (public address). When the packet returns to Building B, the packet will be re-addressed to the IP address of the private network by using the MAC address contained in the header to identify the destination.

Diagram of Incoming NAT

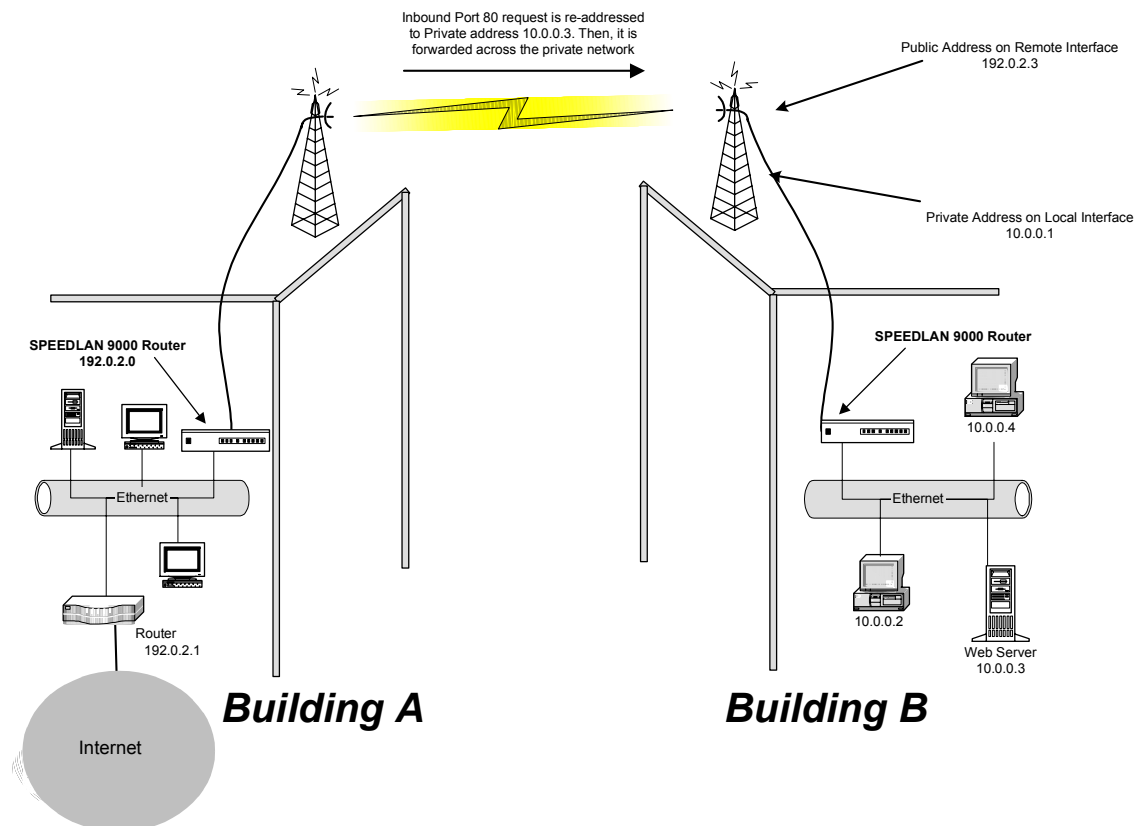


Figure 5-4: Incoming NAT

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

Basics of Routing

A router connects two or more networks or subnetworks together and decides which direction it should send each packet. A router is typically a gateway (where one network meets another). A router operates at the Network Layer of the OSI model. This means a router sends information based on the packet's IP address instead of the Ethernet (MAC) address (as in bridging).

Routing protocols use special metric algorithms when determining the best path for a packet to travel. All of this information is stored in a routing table. Some of this information includes hop count and destination information. The routing table also stores when the receiver gets the packet and lets the sender know that it was received.

Note: For more information about routing, see www.whatis.com, <http://www.techweb.com/encyclopedia/>, <http://www.computeruser.com/resources/dictionary/dictionary.html>, or search for "basics of routing" on the World Wide Web.

[illegible]

Glossary for Standard Data Communications



Glossary for Standard Data Communications

Advanced Encryption Standard (AES)

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 9200 products use an AES 128-bit encryption key.

Address Resolution Protocol (ARP)

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.

Alignment

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

Amplitude

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

Analog

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

Antenna

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

Antenna Gain

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

Attenuation

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

Attenuator

A device used to reduce the RF signal level.

Azimuth

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

Band

A portion of the electromagnetic frequency spectrum.

Bandwidth

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

Bit

An abbreviation for binary digits.

Bit Error Rate

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

Bridge

The function of a bridge is to connect separate networks together. This device operates at the DataLink Layer of the OSI model. Bridges connect different network types (such as Ethernet and Token Ring) or networks of the same type.

Byte

A data unit consisting of eight bits.

Cable

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

Channel

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

Classless Inter-Domain Routing (CIDR)

This is an abbreviated method of entering the netmask. For more information, see CIDR Table (For Netmask Information Purposes) in Chapter 3.

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

A CSU/DSU is a pair of devices that adapts a dead pair (i.e., an unbiased line) to transmit high-speed data signals. Of course, the pair is manageable and provides a status, but their main function is be a dead-line modem. Latest versions use digital signals over the dead line, but older models did not.

Channel Spacing

Channel spacing is the spectral space between RF channels; it may be in KHz or MHz, depending on the band.

Class (IP Network)

There are three main classes are: Class A, Class B, and Class C.

- Class A: Net, Node, Node, Node 35.**0.0.0** (last three octets are available for equipment)
- Class B: Net, Net, Node, Node 128.5.**0.0** (last two octets are available for equipment)
- Class C: Net, Net, Net, Node 192.168.1.**0** (last octet is available for equipment)

Coaxial Cable

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

Code Division Multiple Access (CDMA)

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

Common Management Information Protocol (CMIP)

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

Company name

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

Console

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

Crimp

Crimp the connector to secure the conductors.

Customer Premise Equipment (CPE)

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

Data Communication Equipment (DCE)

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

Data Terminal Equipment (DTE)

Hardware that provides for data communications. See also DCE above.

dBm

Decibels (dB) relative to 1 milliwatt.

dBw

Decibels (dB) relative to 1 watt.

Decibel (dB)

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

Diffraction

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

Digital Signal Processor (DSP)

A specialized computer chip designed to perform speedy and complex operations on digitized waveforms.

Direct Sequence (DS)

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

Direct Sequence Spread Spectrum (DSSS)

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

Dynamic Host Configuration Protocol (DHCP)

DHCP servers provide efficient use of IP addresses by assigning them dynamically or statically. DHCP is used on the wired interface of the 9000.

Digital Signal Processor (DSP)

A specialized computer chip designed to perform speedy and complex operations on digitized waveforms.

E1

An E1 is a full-duplex synchronous digital stream with a signaling rate of 2.048 Mb/s. The electrical characteristics of the digital interface are defined in the recommendation UIT-T G.703 (which by the way also defines it for a T1). Framing structure is defined in ITU recommendations G.704 and G.732. Finally, the only countries in the world where E1 streams are not regularly used are in U A and Japan.

Elevation

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

Encryption

The method of converting data into a form that cannot be understood by unauthorized people. Encryption is very important when using wireless communication because wireless circuits are easier to tap into than wired circuits. There is also strong encryption, which means ciphers are used to make uncoding the signal almost impossible, unless you have the decryption keys.

ESD

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

Ethernet

This is the most popular physical layer LAN technology in use today. Other LAN types include Token Ring, Fast Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and Local Talk. Ethernet is popular because it strikes a good balance between speed, cost and ease of installation.

Ethernet Switch

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

Fade Margin

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

Fading

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

Federal Communications Commission (FCC)

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

Firewall

A firewall protects resources in a private network from the users on outside networks. It can also restrict unwanted traffic from the private network to the outside. The firewall determines based on a set of rules whether packets should be forwarded to their destination.

Firmware

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

Forward Error Correction (FEC)

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

Framing

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

Frequency

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

Frequency Hopping (FH)

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

Fresnel Zone

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

File Transfer Protocol (FTP)

A protocol used to transfer files over a TCP/IP network.

Full Duplex

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

Gain

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

GHz

GigaHertz. Billions of Hertz.

Ground elevation

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

Half Duplex

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

Hertz (Hz)

A unit of measurement equal to one cycle per second.

Hexadecimal (Hex, or H)

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

Hop

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

Host

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

Hot-standby

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

Hub

This device on a network receives and repeats data to connected destinations on the network.

HyperText Transport Protocol (HTTP)

The communication protocol used to connect servers on the Web.

HyperText Transport Protocol Secure (HTTPS)

The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The session is managed by a security protocol.

Institute of Electrical and Electronics Engineers (IEEE)

A membership organization that includes engineers, scientists and students in electronics and allied fields. It was founded in 1963.

Interface

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

Interference

Unwanted signals that cause performance degradation or loss of information.

Internet

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

IP Address

This address tells the network how to locate the computers or network equipment connected to it. IP addresses are given so each computer or equipment on the network contains a unique address. There are two methods used when assigning an IP address:

- **Automatic (dynamic) Addressing**

A DHCP (Dynamic Host Configuration Protocol) server assigns the IP address to each computer as the computer connects to the network. If a computer moves to a new network (i.e., great for temporary employees or mobile users), it must be assigned a new IP address for that network. DHCP can be used to manage these assignments automatically.

- **Manual (static) Addressing**

Each device connected to the Internet must have its own unique IP address. Also, if a computer is being used as a server, you will assign it a permanent IP address. This enables other computers to connect to it. Static addressing is also beneficial to users that need to maintain a "constant" connection to the Internet. This will enable users to easily access the IP address.

ISM (Industrial, Scientific, and Medical Bands)

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

Isotropic

Uniform in all directions.

K²

This is a polling protocol used in star networks (line of sight). A base station polls the remote stations (Customer Premise Equipment) and tells when and where CPEs can transmit.

Kb/s

Thousands of bits per second.

KHz (KiloHertz)

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

LAN (Local Area Network)

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

Last mile

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

Latitude

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

LED

This is a light-emitting diode, which is a semiconductor, that sends out visible light when an electrical current moves through it. An electronic device that emits light with little generation of heat.

Line of Sight (radio) (LOS)

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

Loopback

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

Loss of Signal (LOS)

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

MAC address (MAC)

A MAC Address requires 12 hex-digits in groups of two that are separated by dashes or semicolons (i.e., 00:05:D5:12:AF:01).

MAN

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

Management Information Base (MIB)

The MIB is the definition of all standard objects that may be addressed inside a device. The most common protocol to retrieve the information associated to a specific object is SNMP.

MDS (RIP2 MD5 Authentication)

When RIP2 is used with an authentication algorithm, such as MD5, network security is increased since the destination receiving the RIP packet knows that it was generated by a reliable source (i.e., the actual sender of the packet). RIP2-MD5 authentication transmits the output of the authentication algorithm rather than the RIP2 authentication key. Therefore, the RIP2 authentication key is never transmitted over the network and cannot be heard by other routers. This means a router can determine exactly who sent the message and not assume which router sent it.

Mean Time Between Failure (MTBF)

This is defined by a specific set of calculations. The formula of the system longevity is based on the thermal, electrical and environmental stresses on each component.

MHz (MegaHertz)

Millions of Hertz.

Modulation

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

MOdulator-DEModulator (MODEM)

A device that converts a digital signal to analog, or vice versa, and is used to transfer data between computers over communications lines.

Mb/s

Million of samples per second.

Multi-path fading

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

Network Address Translation (NAT)

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.

Network

A set of connections that allow them to exchange data with each other, which enables multiple users to share to communicate data through the accepted path(s). Two or more locations tied together with equipment and communications channels.

Node

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

Noise

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

Obstruction

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

Octet

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

Outside Diameter (OD)

Outside diameter of pipe for mounting an antenna.

Packet

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

Part 15 (of FCC rules)

The section of the FCC Code of Federal Regulations defines the restrictions regarding the use of Spread Spectrum systems.

Passive Repeater

It is easier to explain this using an analogy of an RF reflecting device, like a mirror.

Path Length

The distance between two ends of a wireless system.

Path Loss

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

Path Profile

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

Personal Communication Services (PCS)

A lower powered, higher frequency competitive technology to cellular.

Personal Computer (PC)

Any laptop or desktop (e.g., Windows or a Macintosh).

PC Memory Card International Association (PCMCIA)

This is a standard card for connecting peripherals to portable computers.

Polarization

It's the orientation of the electrical vector on an electromagnetic signal. The vector can be polarized as needed either linear or mixed (i.e., circular).

Pole Height

This is the height of the antenna supporting structure.

Power Output

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

Processing Gain

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

Propagation

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

Protocol

A network protocol is the standard that allows computers to communicate with each other. A protocol defines how computers identify one another on the network, the form that the data should take in transit, and how this information is processed once it reaches its final destination. Protocols also define procedures for handling lost or damaged transmissions or "packets." IPX (for Novell Netware), TCP/IP (for UNIX, Windows NT, Windows 95 and 98 and other platforms), DECnet (for networking Digital Equipment Corp. computers), AppleTalk (for main Macintosh computers), and NetBIOS/NetBEUI (for LAN and Windows NT networks) are some of today's most popular networks.

Pseudo-random Noise code (PN code)

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

Public Switched Telephone Network (PSTN)

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

Quadrature Amplitude Modulation (QAM)

It's a high-density modulation that uses phase and amplitude modulation at the same time. It's used in OFDM, and modulators require a high SNR to provide a stable signal recovery rate.

Quadrature Phase Shift Keying (QPSK)

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

Radiation

The emission of energy from a generator to a transmitter.

Radiation Pattern

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

Radio Frequency (RF)

The frequency at which microwave systems transmit.

Received Signal Strength Indicator (RSSI)

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

Reflection

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

Refraction

The change on the energy's propagation direction as it travels through different density medium.

Reliability

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

Responsible personnel

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

RFC (Request for Comments)

RFCs are documents that explain specifications for types of technology. They primarily contain published tutorials that help people learn about the specific aspects of the Internet. For more information, see Internet Engineering Task Force (IETF) - <http://www.rfc-editor.org/rfc.html>.

RF Signal Level

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

Routing Information Protocol (RIP)

RIP determines a route based on the fewest hop count between the source and destination. RIP, a distance vector protocol, routinely sends broadcasting to its neighboring nodes. There are different classes of RIP:

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

Router

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

Rx (Receiver)

This is where the packet is going.

Server

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

Sidelobe

Sidelobes are the spurious emissions caused by the antenna's geometrical irregularities. They are significantly lower than the main lobe (i.e., common when around 20dB under the main lobe).

Signal level

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

Simple Network Management Protocol (SNMP)

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

Site ID (Unique)

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

SMTP (Simple Mail Transfer Protocol)

SMTP is the standard e-mail protocol used in the Internet. SMTP is a TCP/IP protocol, and it defines the message format and message transfer agent, which is used to store and forward the mail.

Spread Spectrum Technology (SST)

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

Star

A topology (in the K2 polling protocol category) that includes point-to-point or point-to-multipoint activity, as long as those routers are within line-of-sight of each other.

Subnet mask

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

Subnet

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

Symbol Threshold

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

System Gain

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

TCP (Transmission Control Protocol)

TCP is a user datagram type of protocol that ensure that the message was sent accurately.

TCP/IP (Transmission Control Protocol/Internet Protocol)

This is an Internet protocol, and it ensure that the data was sent accurately from one host to another.

Tx (Transceiver)

This is where the packet is coming from.

UDP (User Datagram Protocol)

A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.

WAN

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

Wired

A network interface connected by wire to other nodes in the network.

Wireless

A network interface that uses radio to communicate to other nodes in the network.

Appendices (A-F)

The Appendices include:

- Appendix A: Changing the Router's Topology Mode
- Appendix B: Passwords for the SPEEDLAN 9200 Configurator
- Appendix C: Declarations of Conformity and Regulatory Information
- Appendix D: SPEEDLAN 9200 Technical Specifications & Product Model Information
- Appendix E: Acronyms
- Appendix F: Firmware History
- Appendix G: Channels for IEEE 802.11x. This appendix lists the valid operating channels for FCC and IC (Canada).



Appendix A - Changing the Router's Topology Mode



Changing the Router's Topology Mode

This tutorial tells you how 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).

- 1** Enter the correct URL or IP address for the router in your web browser.
- 2** Enter the correct password and click **Login**.
- 3** After logging in, the Network Interfaces page will appear. Select the new mode (e.g., Mesh) from the **Interface Type** drop-down menu. Then, click **Apply**.
- 4** The system will reboot the router.

Appendix B - Passwords for the SPEEDLAN 9200 Configurator

This appendix provides the passwords needed for the
SPEEDLAN 9200 Configurator.



SPEEDLAN 9200 Configurator Passwords

There are five classes of users. The classes are as follows with their default passwords:

- Full Access (also known as a superuser): "wave_full"
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 9200 network)
- Wireless Read: "wave_wireless" (account for the wireless SPEEDLAN 9200 network)

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

Note: 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 3-74.

Appendix C - Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for P-Com's SPEEDLAN 9200 products.

This appendix contains the following sections:

- Safety Instructions
- Manufacturers Canadian Declaration of Conformity Statement
- European Telecommunications Standards Institute Statement of Compliance Information to User
- Radio Approval Table



Safety Instructions

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 9200 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 9200 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.

Manufacturer Information

Manufacturer/Importer Name: P-Com
7020 Professional Parkway East
Sarasota, FL 34240
Phone: 941-907-2300
Fax: 941-355-0219

Radio Approvals

To determine the correct device you are allowed to use in your country, refer to the tables below:

Radio Approval Table for Models SL920x

Country	Commission	Model SL920x & Certification Number
United States	FCC	KINSL9201, KINSL9202

Minimum Receive Sensitivity (in dBm) for SL920x

Frequency	dBm & Mb/s
5GHz OFDM	-65dBm @ 54Mb/s -82dBm @ 6Mb/s
2.4GHz OFDM	-65dBm @ 54Mb/s -82dBm @ 6Mb/s
2.4GHz DSSS	-80dBm @ 11Mb/s -87dBm @ 1Mb/s

Appendix D - SPEEDLAN 9200 Technical Specifications & Product Model Information

This appendix provides specifications and product model information for the SPEEDLAN 9200 products.



SPEEDLAN 9200 Technical Specifications

Appendix E - Acronyms



List of Acronyms

A

ANSI (American National Standards Institute)

ARP (Address Resolution Protocol)

ARPA (Advanced Research Projects Agency)

C

CDMA (Code Division Multiple Access)

CIDR (Classless Inter-Domain Routing)

CMIP (Common Management Information Protocol)

CPE (Customer Premise Equipment)

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

D

dB (Decibel)

dBm (DeciBels below 1 Milliwatt)

DCE (Data Communication Equipment)

Decibels (dB) relative to 1 milliwatt.

DHCP (Dynamic Host Configuration Protocol)

DOS (Disk Operating System)

DS (Direct Sequence)

DSP (Digital Signal Processor)

DSSS (Direct Sequence Spread Spectrum)

DTE (Data Terminal Equipment)

E

E1

ESD (Electro-Static Discharge)

FAQ (Frequently Asked Questions)

F

FCC (Federal Communications Commission)

FEC (Forward Error Correction)

FH (Frequency Hopping)

FTP (File Transfer Protocol)

G

GHz (GigaHertz)

GUI (Graphical User Interface)

H

Hex or H (Hexadecimal)

HTTP (HyperText Transport Protocol)

HTTPS (HyperText Transport Protocol Secure)

Hz (Hertz)

I

ICMP (Internet Control Message Protocol)

IEEE (Institute of Electrical and Electronics Engineers)

IMAP (Interactive Mail Access Protocol)

IP (Internet Protocol Address)

IP (Internet Protocol)

ISM (Industrial, Scientific, and Medical Bands)

K

K2 (Star Protocol)

Kb/s (Kbits/sec)

KHz (KiloHertz)

L

LAN (Local Area Network)

LED (Light-Emitting Diode)

LIU (Line Interface Unit)

LOS (Line of Sight)

M

MAC (Medium Access Protocol) address

MAN (Metropolitan Area Network)

Mb/s (MegaBytes per SECond)

MD5 (RIP2 MD5 Authentication)

MIB (Management Information Base)

MODEM (MOdulator-DEModulator)

MTBF (Mean Time Between Failure)

N

NAT (Network Address and Port Translation)

NAT (Network Address Translation)

O

OD (Outside Diameter)

P

PC (Personal Computer)

PCMCIA (PC Memory Card International Association)

PCS (Personal Communication Services)

PD (Public Domain)

PDA (Personal Digital Assistant)

PDF (Adobe's Portable Document Format)

PN (Pseudo-random Noise code)

POP (Post Office Protocol)

PPP (Point-to-Point)

PSTN (Public Switched Telephone Network)

Q

QAM (Quadrature Amplitude Modulation)

QPSK (Quadrature Phase Shift Keying)

R

RAM (Random Access Memory)

RF (Radio Frequency)

RF (Radio Frequency)

RFC (Request for Comments)

RIP (Routing Information Protocol)

ROM (Read Only Memory)

RSSI (Received Signal Strength Indicator)

Rx (Receiver)

S

SMTP (Simple Mail Transfer Protocol)

SNMP (Simple Network Management Protocol)

SST (Spread Spectrum Technology)

STD (Standard)

T

TCP (Transmission Control Protocol)

TCP/IP (Transmission Control Protocol/Internet Protocol)

Tx (Transceiver)

U

UDP (User Datagram Protocol)

USB (Universal Series Bus)

W

WAN (Wide Area Network)

WWW (World Wide Web)

Appendix F - Firmware History

This appendix lists history of any prior firmware notes.



There is no information to report at this time.

Appendix G - Channels for IEEE 802.11x

This appendix lists the valid operating channels for FCC and IC (Canada).



Channels for IEEE 5GHz OFDM (UNII upper band)

Channel Information		Regulatory Domains	
Channel Number	Frequency	FCC	
149	5.745 GHz	✓	
153	5.765 GHz	✓	
157	5.785 GHz	✓	
161	5.805 GHz	✓	
165	5.825 GHz	✓	

2.4GHz DSSS Channels

Channel Information		Regulatory Domains	
Channel	Frequency	FCC	
1	2412	✓	
2	2417	✓	
3	2422	✓	
4	2427	✓	
5	2432	✓	
6	2437	✓	
7	2442	✓	
8	2447	✓	
9	2452	✓	
10	2457	✓	
11	2462	✓	

2.4GHz OFDM Channels

Channel Information		Regulatory Domains	
Channel	Frequency	FCC	
1	2412	✓	
2	2417	✓	
3	2422	✓	
4	2427	✓	
5	2432	✓	
6	2437	✓	
7	2442	✓	
8	2447	✓	
9	2452	✓	
10	2457	✓	
11	2462	✓	

Product License Agreement

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

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

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

Software License Agreement

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

The following terms govern your use of the enclosed Software:

License Grant

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

Ownership

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

Copies and Adaptations

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

No Disassembly or Decryption

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

Transfer

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

Termination

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

Export Restriction

You agree that you will not export or re-export the PRODUCT in any form without the appropriate government licenses. Your failure to comply with this provision is a material breach of this AGREEMENT.

U.S. Government Restricted Rights

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

P-Com LIMITED WARRANTY STATEMENT

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

2. P-Com does not warrant that the operation of P-Com products will be uninterrupted or error free. P-Com products may contain remanufactured parts equivalent to new in performance or may have been subject to incidental use.

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

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

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

Return Policies and Warranties

Initial One Year Warranty Term

Each P-Com product is warranted against defects in material and workmanship for a period of one year from date of shipment. During the warranty period P-Com will, at its option, repair or replace products that prove to be defective.

If equipment fails, the Customer or Reseller shall notify P-Com and request a Return Material Authorization (RMA) number. For warranty service or repair, this product must be returned to P-Com. **All returns to P-Com MUST have a valid RMA number written clearly on the outside of the box or the shipment will be refused. The buyer shall pay all return shipping charges during the one-year warranty.**

Return for Credit

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

Limitation of Warranty

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

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

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

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

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

Exclusive Remedies

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

[illegible]

Index

A

Address Sharing 3-58

Admin menu 3-74

- Factory reset 3-76

- Permissions 3-75

- Software update 3-75

- User configuration 3-74

Alias IP 3-22

Authentication 3-34

C

Configuration

- changing the channel 3-39

- channels 3-38

- configuring a mesh node 4-6

- preamble setting 3-39

- setting the signaling rate 3-39

- turbo mode 3-39

- wireless modes (2.4 and 5.8GHz) 3-38

Configuration menu 3-7

- DHCP Server menu 3-44

- Logging On 3-10

- Network menu 3-19

- Routing menu 3-31

- Security alert 3-13

- System menu 3-25

Configuring in base station mode

- Authentication 4-3

- Configuring data and channel rate 4-6

- Interfaces 4-2

- Remotely controlling 4-10

- Upgrading software 4-10

Configuring in mesh mode 4-1

Creating an Advanced Service 3-55

D

DHCP Relay menu 3-51

DHCP Server Menu 3-44

- adding a Known Client 3-48

- adding a New DHCP Subnet 3-47

- adding DHCP Client 3-49

- adding known client 3-48

- adding new subnet 3-47

- configuring DHCP Relay 3-50

- setting Up DHCP 3-46

Diagnostics menu 3-68

- ARP table 3-71

ICMP 3-71

Interface statistics 3-69

E

Equipment features 1-6

F

Features 1-2

Firewall 3-63

Forwarding 3-51

Forwarding Menu 3-55

Internal Servers 3-60

Forwarding menu 3-51

1:1 NAT 3-62

Address sharing 3-58

Firewall 3-63

General NAT info 3-56

Internal servers 3-60

Services 3-53

Fowarding Menu 3-62

Firewall 3-63

IP Sessions 3-68

Services 3-53

H

Hardware configuration table 2-5

Indoor junction box 2-6

I

Installation Steps

Installation Diagram 2-21

Installation Steps for 9201/9204 2-9

Installation Steps for 9202/9203 2-15

Internal Servers 3-60

IP Sessions 3-68

ISP 1-3

M

Manual Configuration 3-2

Mobile client

addiing security 4-5

N

NAPT 3-62

NAT

Address Sharing 3-58

Network management 1-4

Network menu

TCP/IP 3-19

R

Router

changing the router's topology mode A-1

Common functionality 3-1

Mesh mode 4-1

Routing Menu

Authentication on RIP-2 MD5 3-34

Routing menu

Default gateway 3-32

Route table 3-36

RTS/CTS 4-8

Static route 3-37

S

Security

authentication on a mesh network 4-4

enabling encryption between a PDA/laptop and SPEEDLAN 9200 routers 4-5

enabling encryption between SPEEDLAN 9200 routers 4-4

WEP 4-4

Setting Up DHCP and DHCP Relay 3-45

SNMP 3-26

SPEEDMesh-enabled 4-5

SPEEDMesh-enabled client

enabling/disabling 4-6

System menu

Host name 3-29

Password 3-30

Reboot 3-31

Version 3-29

V

Virtual Addresses 3-23

W

WEP 4-5

types of WEP keys 4-5

