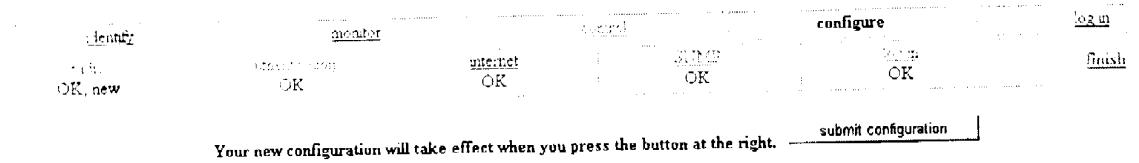
WaveNet IP

Configure



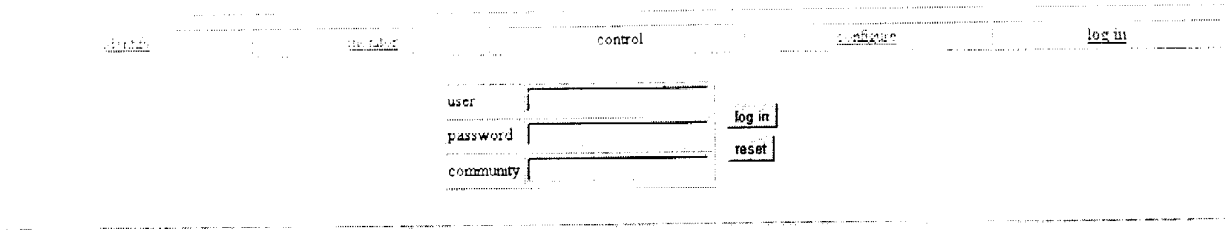
13. Reconfigure the PC using an IP address and subnet mask consistent with the router's new internet configuration.

14. Confirm that log in and SNMP security configurations allow access as intended.

15. Select identify and record the IP Addresses and Station (MAC) Addresses of the Ethernet and Radio interfaces, and the Hardware and Software Identification information. These are generally useful for troubleshooting, maintenance, and the remote router radio interface MAC Address is needed if the central router authentication feature will be used.

WaveNet IP

Log In

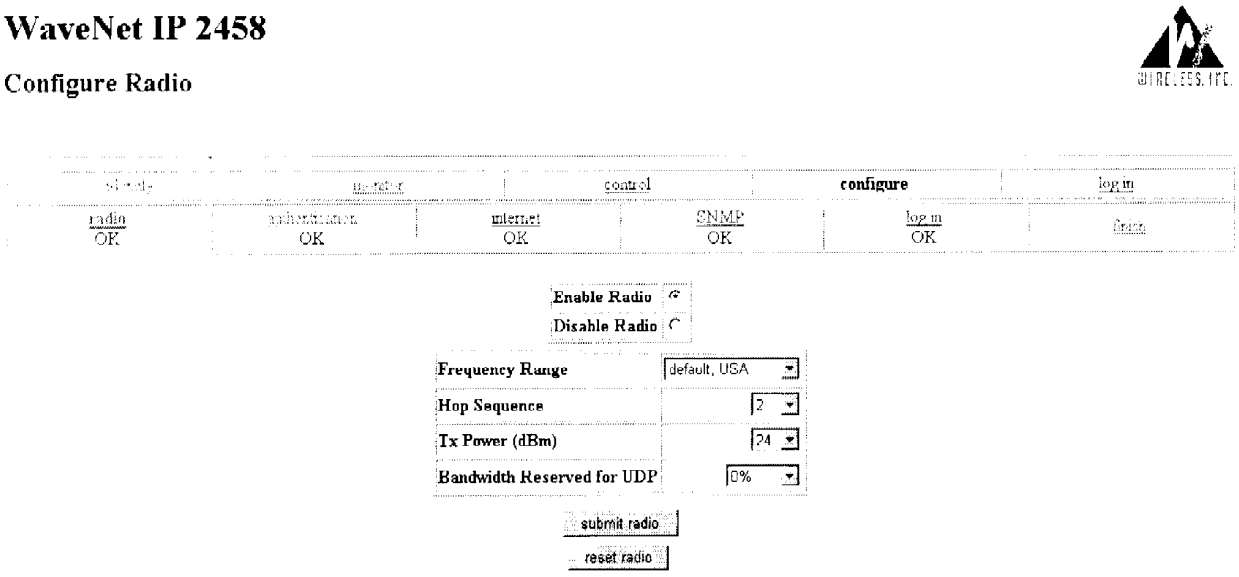


For more information, consult the Wireless, Inc. Web Page

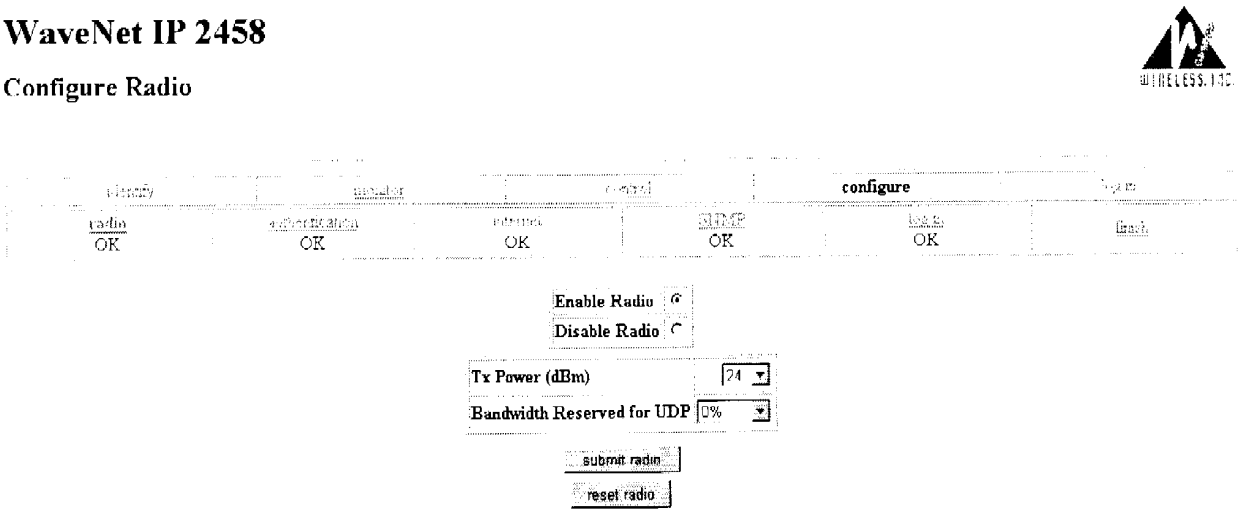
Configure Radio

Performing radio configuration is required in order to deploy the router.

Configure Radio screen on a central:



Configure Radio screen on a remote:



Frequency Range

This is available on central routers only. The default value is the United States FCC-defined ISM band (2.403-2.481 GHz / 5.770-5.848 GHz). A selection of other (subset) ranges is available to meet the regulatory requirements of countries that do not follow the FCC rules. A remote router will dynamically set its Frequency Range to match that of the of the central unit with which it associates.

RF Net ID and Hop Sequence

Enter the Hop Sequence (central units only) parameter from the network planning information. A remote router will dynamically set its Hop Sequence to match that of the of the central unit with which it associates.

Tx (Transmit) Power

Select the desired value from the pull-down list. The range of values is +15 to +24 dBm.

Meeting any regulatory transmitter output power and/or EIRP requirements is the installer's responsibility. The formula for EIRP is given below:

$$EIRP_{dBm} = \text{Tx Power}_{dBm} + \text{Tx Antenna Gain}_{dBi} - \text{Tx Antenna Cable Loss}_{dB}$$

For example, to meet the FCC EIRP limit of +36 dBm (4W) using a 16 dBi sector antenna with a 1 dB loss antenna cable, the transmit power must be set to +21 dBm or lower. See Appendix C for maximum power settings under FCC rules for each provided antenna.

Bandwidth Reservation for UDP

The Bandwidth Reservation for UDP parameter is used to prioritize UDP protocol packets vs. non-UDP packets over the radio interface. Since voice-over-IP traffic is typically carried over the UDP protocol, this allows for the system to deliver voice packets with bounded delay, regardless of non-voice traffic levels. If this parameter is set to *none*, then there is no special handling for UDP packets. If this parameter is set to a value other than *none*, then two priority channels are created, one for UDP packets and one for non-UDP packets. Data from each channel will be given priority, until the amount of data from that channel reaches the specified percentage of total radio channel capacity:

Parameter Value	UDP Bandwidth	Non-UDP Bandwidth
none	N/A	N/A
low	50%	50%
medium	63%	37%
high	75%	25%
very high	88%	12%

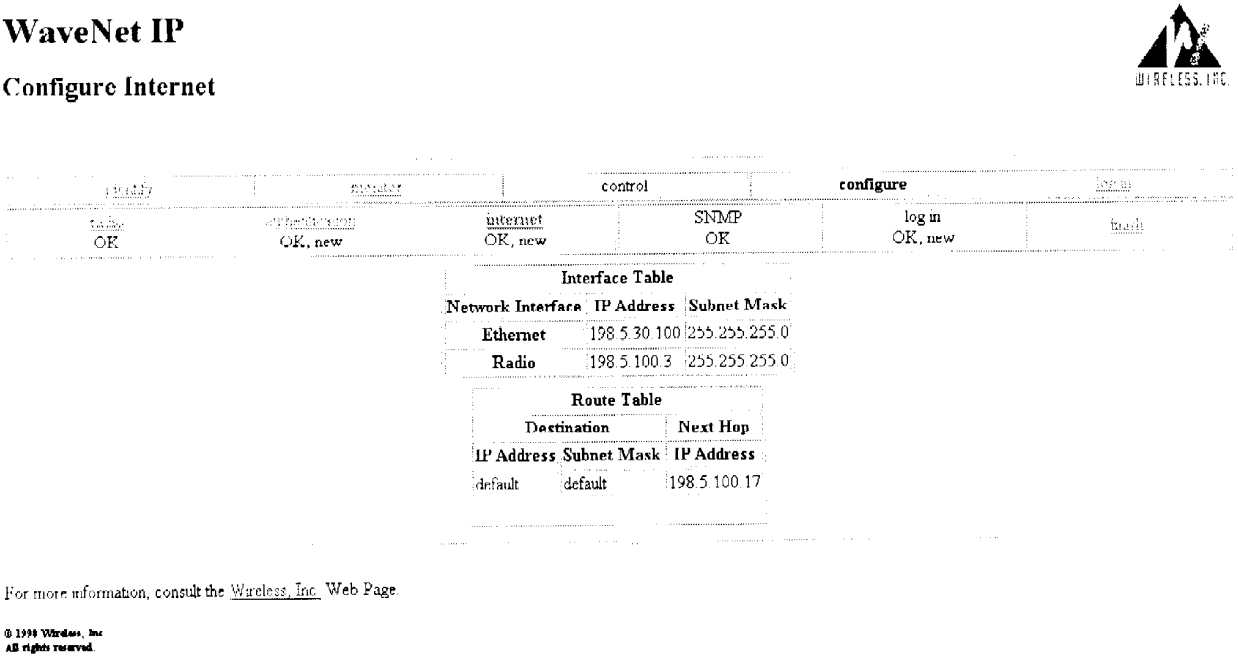
The 88% maximum for UDP packets ensures that non-UDP management data packets (HTTP, Telnet, or FTP) can always be delivered, regardless of the prioritized UDP packet load. When one of the priority channels has no packets to send, then the other priority channel is allowed to use the total radio bandwidth.

Radio Enable/Disable

In order to establish a connection or pass data over the radio interface, *Enable* must be selected. Selecting *Disable* will prevent radio link transmissions and receptions, and the radio self-test LED will be off. The rest of the configuration and installation instructions assume that *Enable* is selected.

Configure Internet Parameters

Performing internet configuration is required in order to deploy the router. The default address established by using the reset switch on the router board should not be used beyond the initial router configuration process.



WaveNet IP

Configure Internet

WIRELESS, INC.

control | configure

		internet	SNMP	log in	
OK	OK, new	OK, new	OK	OK, new	

Interface Table

Network Interface	IP Address	Subnet Mask
Ethernet	198.5.30.100	255.255.255.0
Radio	198.5.100.3	255.255.255.0

Route Table

Destination		Next Hop
IP Address	Subnet Mask	IP Address
default	default	198.5.100.17

For more information, consult the Wireless, Inc. Web Page.

Interface Table

Update the Interface Table with the new values for the IP Address and Subnet Mask for the Ethernet and Radio interfaces. Subnet masks must have binary values consisting of a block of contiguous ones followed by a block of contiguous zeros.

Route Table

Update the Route Table with the addresses of the networks that the router will route packets to, from the network planning information. A maximum of 64 routes may be entered. The columns to enter are:

- Destination Network IP Address (or "default")
- Destination Network Subnet Mask (or "default", when using "default" destination)
- Next Hop IP Address (address of next router on the local Ethernet or radio network)

Configure SNMP

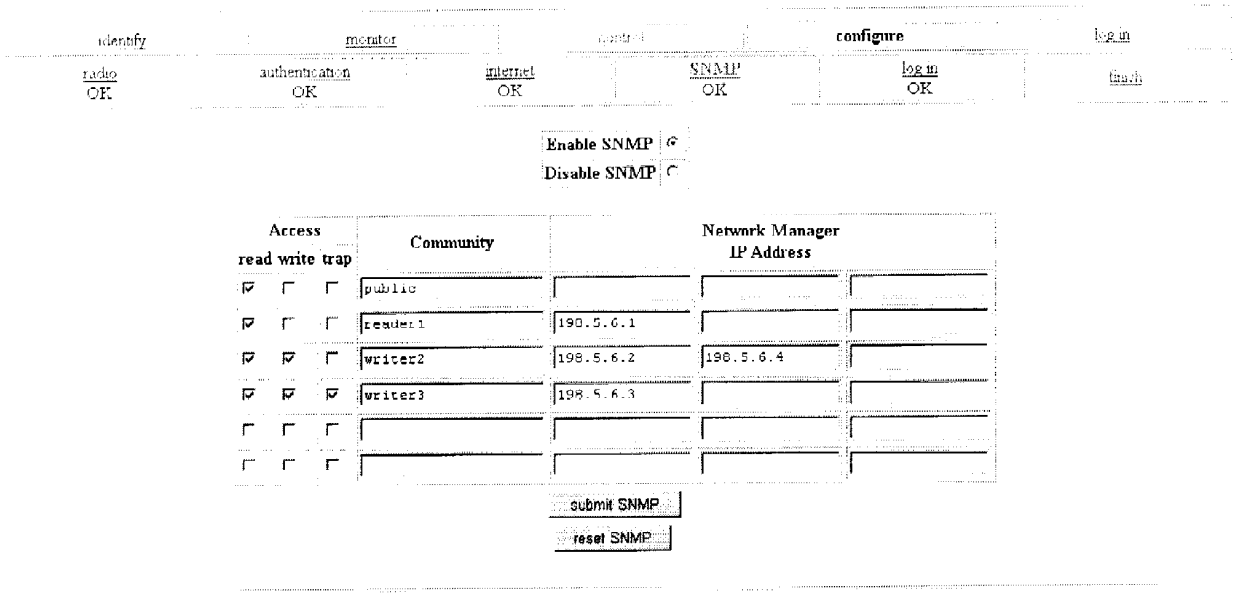
Performing SNMP configuration is optional. If SNMP is *Enabled*, then authorized users can access all monitoring variables and/or selected configuration variables. Variables that may be configured are limited to the normal industry practices for routers and radio-specific parameters. Users may also access a subset of MIB variables through the Web browser interface, upon supplying a valid Community name (from a valid IP address) to log in through the Web browser interface. This applies even if they do not have a Web browser network log in user name and password.

Units are shipped from the factory with a community named "public" which has Read access. This allows users to view all configuration information. Read access for the community named "public" can be removed, thus preventing unauthorized personnel (those without username and password access) from viewing any configuration information.

The SNMP Community Name can be used to provide read-only or read/write access to a specific user or group of users. You can add a community name, and assign the desired level of access (read-only or read/write), via the SNMP configuration page. Once you have submitted the configuration change, you can enter the newly assigned community name in the space provided on the log in page. You will then have access to the unit at the level assigned to that community. You can then give that name to a particular user, or to a group of users.

WaveNet IP

Configure SNMP



For more information, consult the Wireless, Inc. Web Page.

Community Table

The Community Table allows access to the SNMP Read and Write functions based on Community names (which serve as SNMP passwords). Community names must consist of alphanumeric, hyphens, underscores, and/or periods. If one or more Network Manager IP Addresses are specified, then read and write requests will only be accepted if the IP source address from the SNMP packet matches one of the addresses listed.

If Traps are selected, then the router will send SNMP Traps to the specified IP address(es).

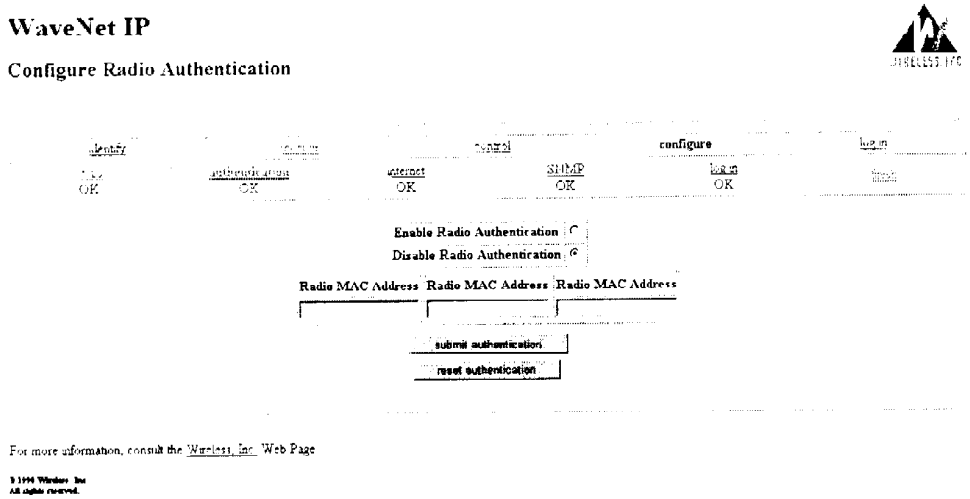
The factory default setting is to allow Read access for the Community "Public" only, from any NMS; if this access is not desired, SNMP should be *Disabled*, the Read Access box should be de-selected, or the Community name should be changed to another value.

Configure Radio Authentication

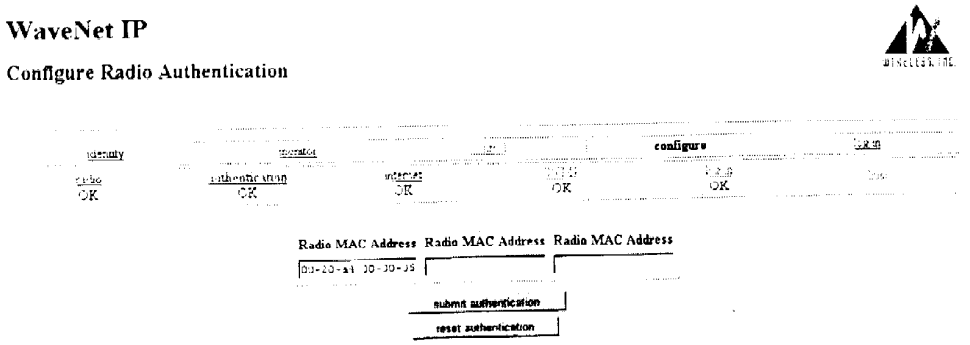
Performing authentication configuration is required on remotes, and is optional on centrals. This feature only allows the remote router to form a radio link with one of several specified central routers, and when *Enabled* on a central router, only allows authorized remote routers to form a radio link with the central router. The authentication step only occurs at connection establishment time (when remote, or central, is first powered on), and therefore cannot be used to terminate an existing connection. The authentication table consists of a list of allowed router radio interface MAC addresses. Authentication is disabled on the central by factory default

Note that authentication on all remote routers must be reconfigured if a new central router replaces the existing central router, unless the MAC addresses of the potential spare central units are known in advance; in such case the MAC address of the spare central(s) should be entered in each remotes' authentication table. When using redundant centrals, make sure that the MAC addresses of each of the redundant centrals appears in each remotes' authentication table.

Configure Radio Authentication screen for a central:

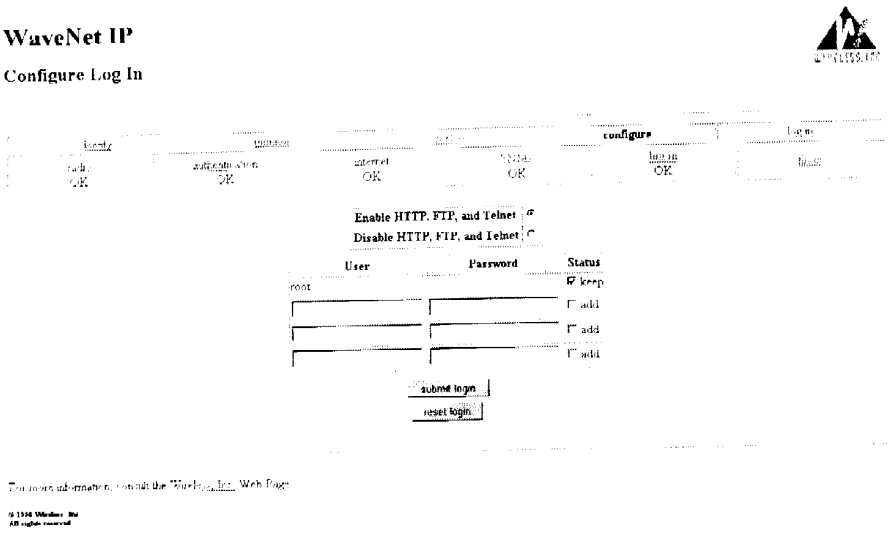


Configure Radio Authentication screen for a remote:



Configure Log In Security

Configuring log in access is usually recommended, except when extraordinary levels of security are required. If this is not configured, then it will not be possible to Telnet, or perform Web browser or FTP based management operations over the network.



User/Password Table

User names and passwords can be established for those allowed full access to the router management functions through the Web browser interface or through FTP. These fields may contain alphanumeric, plus the following symbols: *$-_.+!**.

Enable/Disable FTP and HTTP

Network access to the Web browser management pages (HTTP) and FTP can be *enabled* or *disabled*. If *enabled*, then user and password log in values will be checked against the values entered into the User/Password table at log in time before full access is granted. To add a new user, enter the user name and password (minimum 8 characters), and select the *add* checkbox. The user will be prompted to confirm the password. To delete a user, de-select the *keep* checkbox next to the entry.

Note that limited access to SNMP-accessible variables will be allowed through the Web browser interface if the user supplies a valid SNMP community name at log in time. Access to SNMP variables will be restricted to read and/or write access depending on the community name provided and the IP address of the Network Management Station. Configuration Web pages will only display those fields that can accessed given the security restrictions based on the community name.

If network log in is disabled, then reconfiguration of many of the router functions will require physical access to the setup switch on the router board within the enclosure.

Using FTP, a user can read and write any file on the router. Misuse can cause router operations to cease, so it should used with care. This is normally only needed to initially obtain a copy of the router's enterprise MIB from the router's flash file system, to save or restore a copy of one or more of the router's configuration files, or to update the router with new software.

5 Installation

This section assumes that the network and site planning have been completed, and that the pre-installation configuration has been completed. If any of these steps has not yet been completed, they should be undertaken prior to the physical installation of the routers.

Note: *This system is intended for installation by professional radio equipment installers only. It is the responsibility of the installer to program the transmit power level to comply with FCC EIRP limits or other applicable regulatory requirements.*

Install The Router

Mounting the Enclosure

The following procedure will prepare the cables for mounting.

1. If the data/power cable is not already attached to the enclosure, attach the weather-seal at the router end of the cable to the enclosure as shown in Figure 3. The power and Ethernet connectors should be disconnected from the board within the enclosure. The cable should be coiled and disconnected from power and data sources.

2. Secure a pulling line to one of the holes at the top of the enclosure, if the unit is to be hoisted into position.

3. Attach the grounding lead to the enclosure grounding lug, and coil the grounding wire.

After selecting the location for the enclosure, perform the following procedure to attach the enclosure to the mast using the standard mounting kit that came with the unit (see Figure 10). The standard mounting kit accommodates mast sizes from 1.5-2.5 " (3.8-6.3cm). An optional mounting kit is available that accommodates mast sizes from 1.5-4.5 " (3.8-11.4cm).

1. Attach the top mounting bracket and U-bolt using the supplied nuts (no washer is needed). Note that this bracket should be securely tightened to the mast, as it must support the entire weight of the unit. Place a loose washer over the end of each U-bolt; these will make contact with the enclosure after it is hung on the U-bolt.

2. Pull or hoist the coiled data/power cable, grounding wire, transmit coordination cable (if present), and the router together as a unit to the installation point. Do not rely on the weather-seals to support the weight of the cables. Remember to allow room to mount the antenna above the enclosure.

3. Hang the enclosure on the U-bolt, and secure each side to the top mounting bracket (with washer) with a supplied washer, lock washer, and nut.

4. Secure the bottom of the enclosure to the mast with the remaining U-bolt, securing each end of the U-bolt with a supplied washer, lock washer, and nut. The bottom bracket is only used to prevent the enclosure from swinging away from the mast; it is not intended to support the weight of the enclosure.

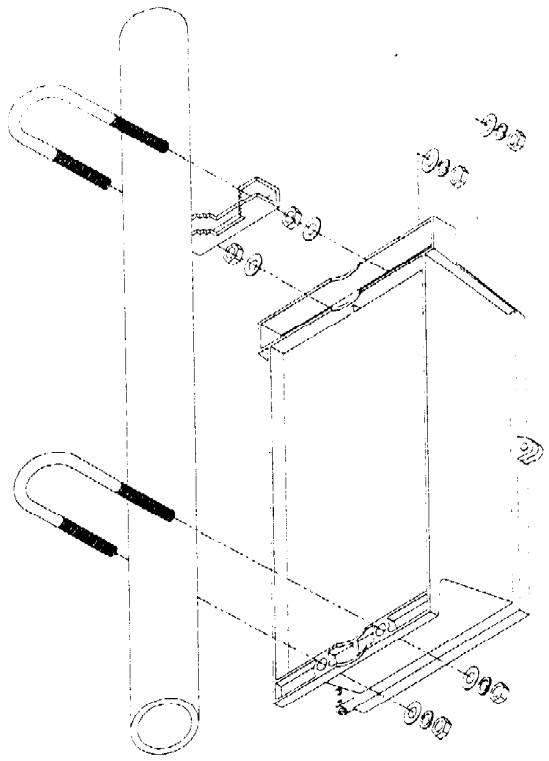


Figure 9 Mounting Enclosure

Secure The Cabling

1. Secure the data/power cable and grounding wire to the mast, mount, or tower as close to the enclosure as possible so there is minimal weight on the weather-seals. Tie-wraps or cable ties can be used. The weather-seals should not be used to support the weight of the cable. Continue down the mast, mount, or tower, securing the cables every meter (three feet). Run the cable under any horizontal bridges, securing the cable to the bridges. If the cable is run through conduit, take care to prevent the cable jacket from scraping on the edge at the entrance to the conduit. It may be necessary to remove or protect the RJ-45 connector if it is to be pulled through conduit.

2. Attach the grounding wire to a properly designed grounding system (see *Lightning Protection and Grounding System* section of Chapter 3).

3. Create a drip loop in the cable, and then run the data/power cable through the wall of the building using a wall/roof feed-through. Wall/roof feed-throughs have one or more openings and a boot, clamp, and galvanized plate to secure the cable to the wall. If lightning protection equipment is used (highly recommended for lightning-prone areas), it should be attached at the entry point to the building as described in Chapter 3.

Indoor Power Connection

Terminate the power cable at the power supply. Either lead of the power cable can be connected to either terminal of the transformer. Attach the transformer (if used) to the wall supply, or otherwise connect the conductors to the power source.

Mount the Antenna

Warning: To avoid excessive exposure to RF energy, WaveNet IP 2458 antennas should be installed and serviced with the primary power disconnected from the WaveNet IP 2458 unit. When power is applied to the unit, the installer must keep at least 44 inches (112 cm.) away from the feed point of the antenna to comply with FCC RF exposure limits. The antennas must be mounted such that the general population will not come within 44 inches of the feed point. This is normally accomplished by installing the unit at an elevated altitude on a roof-top or mast.

1. If the antenna cable is not captive to the antenna, attach it to the antenna connector prior to mounting the antenna. Tighten the connectors firmly by hand, or by using a special slip-jaw pliers made for this purpose. Protect the exposed cable connectors to ensure that the connections are weatherproof. The preferred way to seal this connection is using a cold shrink insulator (such as 3M brand #8447-3.2) inserted over the cable prior to attaching to the antenna port. The alternative method is to first wrap electrical tape around the connectors, completely covering them, and then completely wrap the connectors with water-resistant putty tape (such as Scotch™ brand 33).

2. Pull or hoist the antenna and cable assembly to the installation point. For central site sector antennas, determine the direction that the antenna should point before attaching the antenna mounting hardware; for a remote site directional antenna, align the antenna to the approximate direction of the central site by using a compass, or by actual sighting. Attach the antenna to the mast, using the mounting hardware and instructions included with the antenna. For remote site directional antennas, tighten the mounting hardware only as much as needed to support the antenna until the aiming process is completed (below).

3. Attach the antenna cable to the female N connector on the bottom of the router enclosure. Be careful not to damage the coaxial cable by bending it too much. Be sure not to bend the coaxial cable at too small a radius when connecting it between the enclosure and the antenna. Weatherproof the connection to the enclosure.

Internal Router Cable Connections

1. Loosen the screws on the enclosure door and open the door.

2. Connect the Ethernet and power connectors to the board.

3. After the router boots-up, verify that the router and radio self-test indicators remain lit.

Aiming the Directional Antenna (Remote Routers Only)

Warning: When aligning the directional style of antennas, always align and adjust these antennas from the rear, and avoid RF exposure from the front of the antenna. The installer must keep at least 44 inches (112 cm.) away from the front of the feed point of the antenna to comply with FCC RF exposure limits.

1. Attach the positive lead of a digital volt meter (DVM) to the Signal Quality test point on the router board (see Figure 2), and attach the negative lead to the edge of the enclosure or other source of ground, using alligator clip leads. If the remote router is able to establish a radio connection with the central router, then a voltage greater than one volt will be shown on the DVM. Note that it may take up to a minute or two for the radio connection to be established, after the self-test completes. If the radio connection does not come up, verify that the antenna is pointed in the correct direction, and re-orient it if necessary, again waiting up to a minute or two for the radio connection to be established.

2. Assuming that a directional antenna is being used (typical case), the antenna aim should be varied slightly in all directions (as allowed by the mounting hardware) to find the strongest radio signal. In the case where a directional antenna is used at each end of a link, then each antenna may have to be adjusted (alternately) a number of time to achieve optimal signal strength. The RSSI level will change in proportion to a change in receive signal level. Each time the antenna is moved, it will take up to one second for the DVM to indicate the new signal strength. The following table shows approximate values for the received signal strength based on the RSSI voltage value.

Receive Level $_{dBm}$	-90	-85	-80	-75	-70	-65	-60	-55	-50
RSSI $_{volts}$ Central	1.25	1.55	1.70	1.90	2.20	2.55	2.90	3.25	3.55
RSSI $_{volts}$ Remote	1.30	1.60	1.75	2.00	2.30	2.65	2.95	3.35	3.65

3. After a path with a strong signal is established, tighten the antenna mounting hardware, disconnect the DVM, close the enclosure door, and tighten the door screws. If desired, a pad lock can be attached to the enclosure door.

Configuring Other Customer Equipment

Workstations and Other End-Nodes

If the router is attached directly to the end-station network, i.e. there is no intervening router, then the end-stations that need to communicate through the router need to know the IP address of the router's Ethernet interface. One or more of the following configuration choices are typically available based on the specifics of the end-station equipment:

- enter the address of the *WaveNet IP 2458* Ethernet interface as the default gateway address,
- add the address to the table of available routers, or
- enter the address into the route table as the next hop for one or more specified remote networks

Routers

In some installations, the router is connected to the end-stations via another router, such as a separate site router or a Novell® NetWare® or Microsoft® Windows® NT™ server system acting as a site router. In these cases, the site router needs to know all of the networks that can be reached through the radio network.

Network Management Stations

Any standard SNMP Network Management System (NMS) can be used to monitor and control the *WaveNet IP 2458* network and individual routers. The routers generally support the applicable objects from MIB-II.

WaveNet IP 2458 has an enterprise MIB provided in standard ASN-1 format. The enterprise MIB can be found in the router's file system as "F:/PUB/wn2458.mib". It can be FTP'd from the router and loaded into the NMS's MIB database to allow access to the router's device-specific variables. The description fields in the enterprise MIB document the contents of each variable. Generally, treat the routers and their associated networks like any other network to be managed.

A listing of the *WaveNet IP 2458* enterprise MIB can be found in Appendix A.

Verifying Internetwork Connectivity

Central Sites

The goal of this section is to verify connectivity between a new central site router and the central site network equipment. Connectivity between central and remote sites is normally verified when a remote is installed.

From a PC connected to the central site network, *ping* the IP addresses of the central router's Ethernet interface and radio interface. If either of these fails, recheck the internetwork configuration on the router including:

- IP addresses of Ethernet and radio interfaces
- Subnet masks of both interfaces
- Route table entries

If the configuration is correct, then verify the physical connection to the router. If communications cannot be established to the router, then it may be necessary to use the setup switch on the router board inside of the enclosure to reset the router's internetwork configuration to a known state (see Chapter 4).

Remote Sites

From a remote site end-station, attempt to *ping* to the IP address of a device located at another site. If a *ping* response is received, then internetwork connectivity is confirmed. Check (and correct, if necessary) the internetwork configuration (including Ethernet Type II framing) of the end-station and any intermediate routers, and retry the operation. If this fails, try a *traceroute* to see how far the packet gets; check for mis-configured internetwork parameters including route table entries.

If this is not effective, then configure a dedicated PC as a node on the network shared by the Ethernet interface of the *WaveNet IP 2458* router. Be sure to configure the following PC network parameters:

- IP address
- Subnet mask
- Use IP address of remote router's Ethernet interface as default gateway

Connect the router's Ethernet interface to an isolated network containing just the PC using a separate hub or a crossover modular jack assembly.

Issue *ping*s in the following order to determine the source of the connectivity problem. If there is a failure then consider the possible problem sources listed for each step.

Action	Upon Failure, Verify:
ping the router's Ethernet interface	♦ IP address, subnet mask, or default gateway on PC ♦ IP address or subnet mask of router's Ethernet interface (on router) ♦ Physical Ethernet link (hub and/or cable) to remote router
ping the remote router's radio interface	♦ IP address or subnet mask of router's radio interface on router ♦ radio interface is *Enabled*
ping the central site *WaveNet IP 2458* router's radio interface	♦ IP address or subnet mask of central router's radio interface ♦ Physical radio link
ping the central site *WaveNet IP 2458* router's Ethernet interface	♦ IP address or subnet mask of central router's Ethernet interface

If communications cannot be established to the router, then it may be necessary to use the setup switch on the router board inside of the enclosure to reset the router's internetwork configuration to a known state (see Chapter 4).

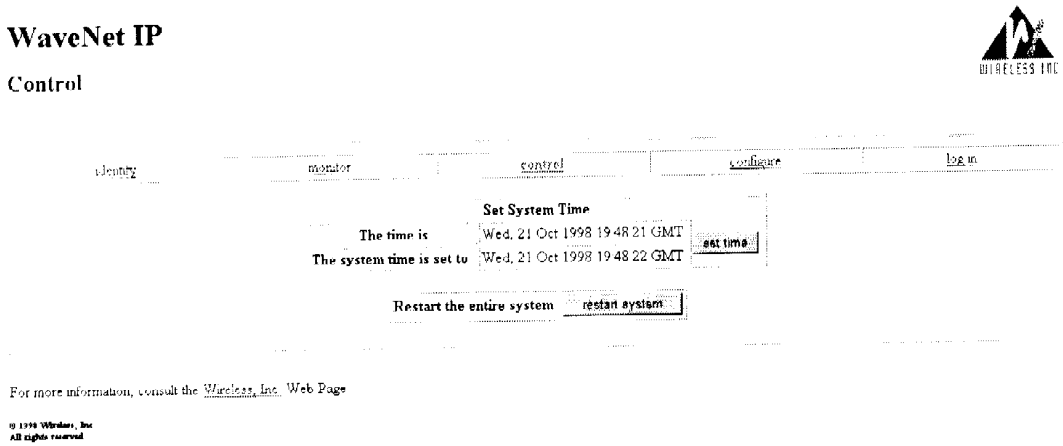
If all of these are successful, then verify the route tables of the *WaveNet IP 2458* central or remote. If the route tables are correct, then the problem is likely outside of the *WaveNet IP 2458* network.

6 Network Operation

Control Operations

The control management page is used to set the system time to the current time, as understood by the computer that the Web browser is running on. The system time is expressed relative to Greenwich Mean Time (GMT).

The control page can also be used to reset the *WaveNet IP 2458* unit. Note that this operation will take the router and radio off-line for approximately 2.5 minutes.



Adding and Removing Remotes

Adding a Remote Router to an Existing Network

1. Configure and install the remote router as described in previous chapters.
2. Add routes to the networks accessed through the remote router into the central router's route table.
3. Add routes to any other central site router or external router as needed.
4. If authentication is being used on the central router, add the remote router's radio interface MAC address to the central router's authentication table.

5. Verify connectivity to the remote router from the central site by *ping*'ing stations on the remote network. If this fails, try doing a *traceroute* to find where the connection fails, and/or successively *ping* each router interface working forwards from the central site router Ethernet interface.

6. If network log ins are permitted, verify that this works.

7. If an SNMP NMS is being used, add the remote to the NMS's database.

Removing a Remote Router from an Existing Network

This procedure can be used if the authentication feature is being used at the central unit.

1. Remove the remote router's radio interface MAC address from the authentication table.

2. If the remote router is currently connected to the central and network log ins are enabled, then log in to the remote router and perform a restart system operation from the control page to disconnect the remote router's radio connection. It should now fail to connect since it will no longer succeed with the authentication process. (Ignore this item if the *Terminating Connectivity to a Remote* procedure was followed in Step 1.)

3. Remove the route table entries for the remote router from the central router and any other external routers.

4. If an SNMP NMS is being used, remove the remote router from the NMS's database.

Moving a Remote Router Between Co-Located Central Routers

1. Add a route table entry for the remote router into the new central router's table.

2. If authentication is being used, add the remote router's radio MAC address to the new central router's authentication table.

3. Modify the remote router's route table entries.

4. Modify the remote router's radio configuration, including RF Net ID and Hopping Sequence.

5. Delete the remote router's route table entry and authentication table entry (if used) from the old central router's tables.

6. Modify the route table entries for the remote router in any external routers being used.

7. log in to the remote router to verify connectivity.

8. If an SNMP NMS is being used, update the NMS's database with the remote router's new information.

Using FTP to Archive or Modify Configurations

It may be desirable to archive a copy of a router's configuration for record keeping, or to restore in case of hardware failures. It may also be desirable to copy all or part of one router's configuration to another router. This might be done to insure consistency of data (e.g. security or routing parameters), or else as a short cut to reduce configuration time. These objectives can be accomplished by using FTP to retrieve one or more of a router's configuration files, which can be restored to the same unit or another unit when desired. Note that the internal structures of the data located within the configuration files may change between different software versions, therefore configuration files should only be stored/restored between units having the same version of software. Note that it may be necessary to *cd* to the router's file system root (F:) prior to accessing files.

The router's configuration files are located in the router's file system as follows:

- Radio Configuration Parameters: F:/RADIO/ylconfig.dat
- Authentication Table: F:/RADIO/ylassoc.dat
- Log in User Names and Passwords: F:/MPN/passwd
- Interface IP Addresses and Subnet Masks: F:/MPN/inet
- Route Table Entries: F:/MPN/routes
- SNMP Community Table: F:/SNMP/config
- MIB-II System Group Data: F:/SNMP/nov

FTP'ing configuration files onto a router should be done with care, as errors in the copying process may render the router inoperable pending significant recovery processes.

Monitoring and Trend Analysis

Central and remote routers can be monitored through either the Web browser or SNMP agent interfaces.

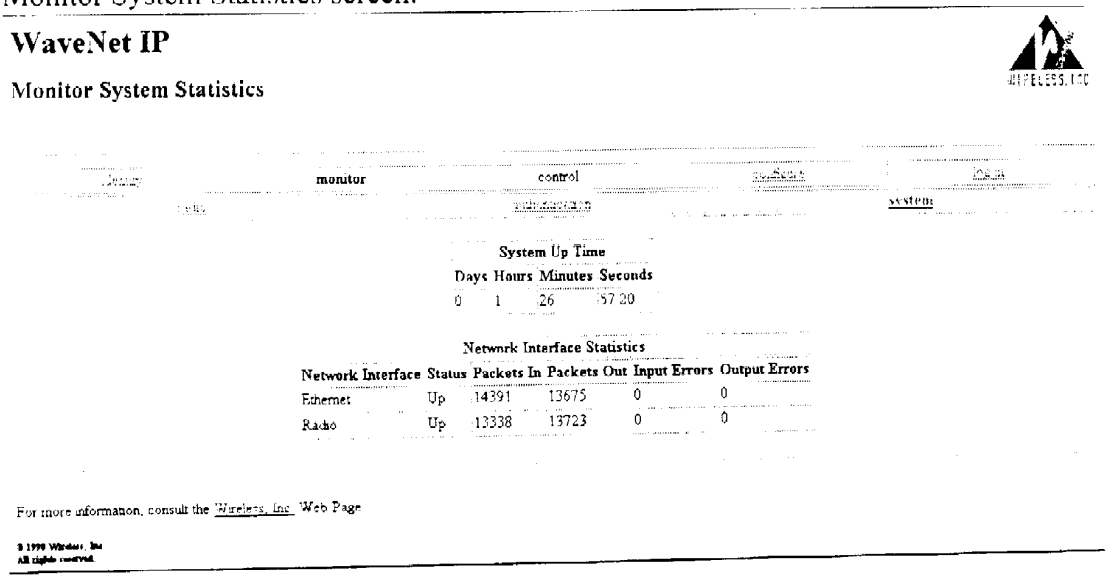
SNMP Network Management Stations

All monitorable statistics are available through SNMP queries. In addition to MIB-II variables, product-specific variables are available through the *WaveNet IP 2458* enterprise MIB (see Appendix A), which can be FTP'd from *F:/PUB/wn2458.mib* in the router's file system. Most commercial SNMP Network Management Stations have the ability to sample variables over time and display trends and/or raise alarms based on defined thresholds. In addition, applicable MIB-II traps are supported, and can be used to raise alarms on the network management station.

Web Browser Interface

A subset of the SNMP-accessible statistics is available through the Web browser interface. These statistics can be read by doing a network log in using either a user name and password, or by specifying a valid community name that is allowed SNMP read access, and then selecting monitor. Statistics can be repeatedly sampled by using the reload/refresh feature included with the Web browser. System, Radio, or Authentication statistics can be selected.

Monitor System Statistics screen:



WaveNet IP

Monitor System Statistics

monitor control system

System Up Time

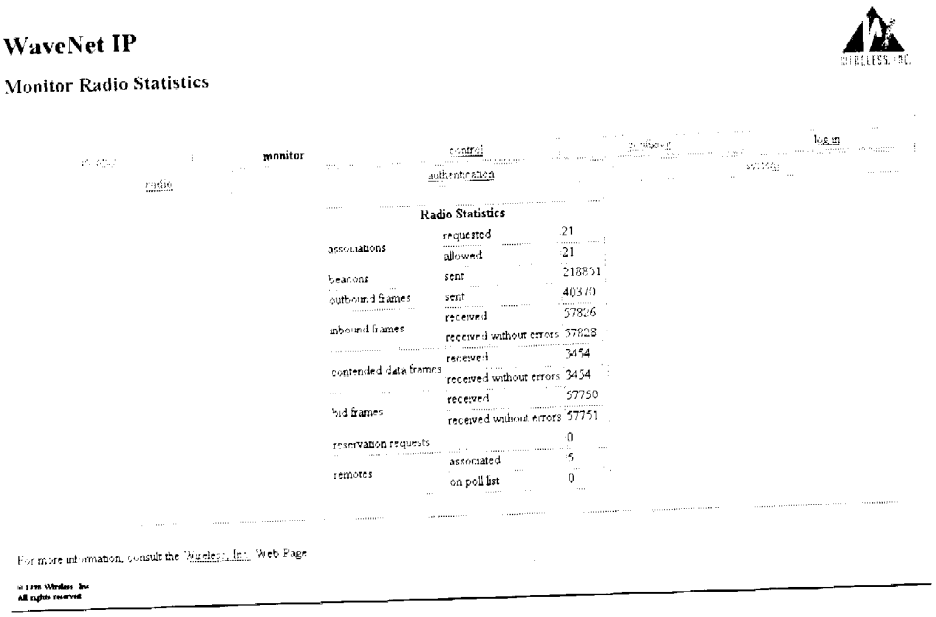
Days	Hours	Minutes	Seconds
0	1	26	57.20

Network Interface Statistics

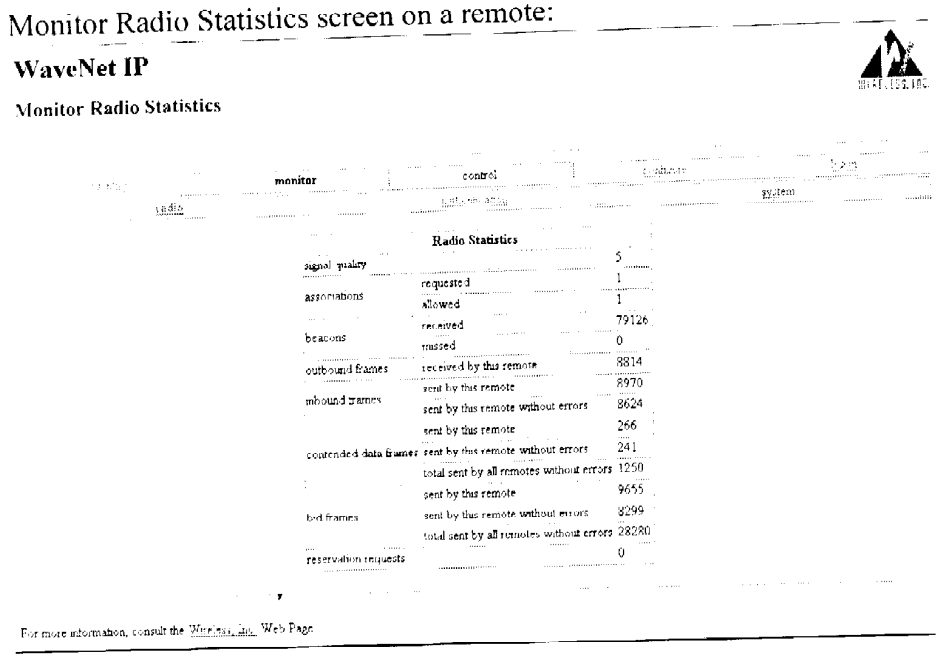
Network Interface	Status	Packets In	Packets Out	Input Errors	Output Errors
Ethernet	Up	14391	13675	0	0
Radio	Up	13338	13723	0	0

For more information, consult the Wireless, Inc. Web Page

Monitor Radio Statistics screen on a central:



Monitor Radio Statistics screen on a remote:



Monitor Radio Statistics

Performance monitoring and troubleshooting of the radio link can be accomplished using radio statistics.

The following provides a definition for each radio statistic on a central: