WaveNet Access 3500
Operations Manual

Version 1.0

Copyright

Trademarks

WaveNet is a registered trademark of Wireless, Inc.

Novell and NetWare are registered trademarks of Novell, Inc.

Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape Navigator is a trademark of Netscape Communications

Scotch is a trademark of 3M Corporation.

All other product names or service names are trademarks of their respective owners.

Electromagnetic Interference

This device complies with ETSI EN 301 021 radio certification requirements. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: Any user changes or modifications not expressly approved by Wireless, Inc. could void the user's authority to operate this equipment.

Customer Support: (408) 727-8383 Monday through Friday, 8 am to 5 pm PT

At all other hours, for emergencies, call 408-327-0876 (Worldwide), or 888-323-8885 (US only)

Contents

Chapter 3 - Pre-Installation Configuration

Chapter 4 - Installation

Chapter 5 - Network Operation

Chapter 6 - Maintenance

Chapter 7 - Specifications

Appendix A - Messages and Traps

Preface

WaveNet® Access 3500 is a wireless access router system that can be used to link up to hundreds of remote Ethernet LANs to a single central site location. The WaveNet Access 3500 has voice prioritization and user selectable bandwidth reserved for voice, which allows it to integrate seamlessly with your VoIP network. Along with providing full-duplex operation, special care has been taken in the design of this product to minimize latency, the number one concern when deploying VoIP networks.

The WaveNet Access 3500 operates in the 3.4 GHz to 3.6 GHz licensed bands. The band is split; the 3.5 to 3.6 GHz frequency range is used for the downstream (Central transmitting to Remote) traffic, and the 3.4 to 3.5 GHz range for upstream (Remote transmitting to Central) traffic.

A system designed using the WaveNet Access 3500 provides a cost-effective, highly reliable alternative to existing copper based wireline alternatives such as ISDN and digital leased lines connecting LAN computer networks to the Internet, private IP networks, or into an intranet.

In addition, WaveNet Access 3500 VoIP support allows seamless integrated voice and data communications. As IP evolves and new protocols are added to support real time traffic, it is anticipated that VoIP will be implemented in wide area networks.

Purpose of this Document

This document contains the information and procedures necessary to plan, configure, install, operate, test, and maintain WaveNet Access 3500 systems.

Intended Audience

This document is intended for personnel who install, operate, and support WaveNet Access 3500 equipment. This includes network administrators as well as those who plan and install the radio links. Network administrators should have experience planning, installing, and operating internetwork equipment and networks.

How this Document is Organized

The information in this document is ordered to match the chronological flow of tasks needed to plan and deploy a network. The chapters are organized in the following sequence:

- "Preface," contains overall document information.
- "Functional Description," explains the functions of the WaveNet Access 3500 system.
- "Network and Site Planning," explains details regarding the planning that should be completed prior to system deployment.
- "Pre-Installation Configuration," explains how to complete the configuration of the routers to the extent possible prior to the actual physical installation.
- "Installation," explains how to physically install the routers.
- "Network Operation," explains how to add or remove Remotes, how to use FTP to modify the network configuration, and how to monitor and tune network performance.
- "Maintenance," explains how to determine performance degradation and replace failed units.
- "Specifications," gives the electrical, mechanical, and environmental specifications.
- Appendix A, "Messages and Traps," contains an abbreviated listing of the common messages and traps that may be generated by the routers.
- Appendix B, "List of Antennas Compliant with ETSI Type Certification," lists characeristics of antennas that may be used with the WaveNet Access 3500 system on Central radios.
- Appendix C, "Grounding Practices and Lightning Protection Information," gives information on accepted grounding and lightning protection practices.
- Appendix D, "Radio Statistics," lists and defines all the radio statistics.
- Appendix E, "WaveNet Access 3500 MIB," gives a listing of the MIB.

Terms

Table 1 lists the terms and abbreviations commonly used throughout this document.

Table 1. Terms

Term	Description
WaveNet Access 3500	The complete system consisting of Central and Remote radio access routers, antenna subsystems, and management systems, as deployed in a point-to-multipoint network
ATPC	Automatic Transmit Power Control
Central Unit	The unit located at the backbone network connection in the WaveNet Access 3500 system. It performs radio transmission and reception with multiple Remote units, protocol processing, and communications with a Central site network or device. A Remote unit is referred to as “the Central” for short.
CIDR	Connection Identifier. The CIDR value is returned to the connecting program after connect processing has established a session and must be used on subsequent requests to the resource.
EIRP	Effective Isotropic Radiated Power
ETSI	European Telecommunications Standards Institute
FRU	Field replaceable unit
Inbound Frames	Frames sent from Remote to Central
ISP	Internet Service Provider
kbps	kilobits per second (1×10^3 bits per second)
MAC	Media Access Control, which is the protocol used to allocate data transmission time on the radio channels.
MTU	Maximum Transfer Unit. The maximum number of bytes that an Internet Protocol (IP) datagram can contain. Also defined as the largest amount of data that can be transmitted in a single frame for a particular network interface.
NMS	Network management system that controls the operation, administration and maintenance of the WaveNet Access 3500 System
Outbound Frames	Frames sent from Central to Remote
pps	Packets per second
Remote Unit	The units located at the end customer networks in the WaveNet Access 3500 system. A Remote unit performs radio transmission and reception with a Central Unit, performs protocol processing, and communicates with a remote site network or device. A Remote unit is referred to as “the Remote” for short.
RSSI	Receive Signal Strength Indication

Table 1. Terms (Continued)

Term	Description
UI	User Interface
UDP	User Datagram Protocol. A packet-level protocol built directly on the Internet Protocol layer. UDP uses application-to-application programs between host systems.
VoIP	Voice over IP

1 Functional Description

This chapter contains a functional description of the WaveNet Access 3500 router, and contains the following sections:

Introduction

WaveNet Access 3500, a point-to-multipoint wireless access router, offers a low-cost alternative to ISDN, leased lines and Frame Relay for Internet and intranet connectivity. There are three versions of the router:

- Central Router with external antenna
- Remote Router with external antenna
- Remote Router with integrated antenna

The Central router and the Remote router with external antenna have the same appearance. The Remote with the integrated antenna does not have a connector for the external connector and has a shell covering the integrated antenna. The different versions of the WaveNet Access 3500 router are shown in Figure 1-1

Central Router and
Remote Router with External Antenna

Remote Router with Integrated Antenna

Figure 1-1. WaveNet Access 3500 Routers

WaveNet Access 3500 is capable of supporting hundreds of remote networks from a single central location. Radio operation is in the 3.4 GHz to 3.6 GHz bands.

A functional summary of the WaveNet Access 3500 is shown in Table 1-1.

Table 1-1. WaveNet Access 3500 Functional Summary

Parameter	Value
Radio Data Rate	4600 kbps
Effective Data Rate	3250 kbps
Frequency Band	3.4 GHz - 3.6 GHz licensed
Channel Size	1750 kHz
Mode	Point-to-Multipoint, Full-Duplex
Distance	5 km line-of-sight (10 km maximum)
Data Protocols	IP (v4), ICMP, ARP, TCP, FTP, SNMP, RIP, RIP II
Data Interfaces	Ethernet (10BASE-T, RJ-45)
Remotes Per Central Radio	30
Repeaters	No
Management Interfaces	Web browser based UI, SNMP Monitor/Configure, Maintenance Port
Diagnostics	Power on self test (POST) tests memory, CPU, configuration parameters, software load BNC connector for RSSI levels 9-pin circular MIL connector (for Palm PDA device (with Palm OS 2.0 or above) to monitor radio LEDs

The system consists of Central and Remote routers. The entire wireless router unit is contained within a single outdoor enclosure. The Remote routers are typically mounted on the roof or side of a building and connect into the remote site Ethernet with a standard 10BASE-T connection. Central site routers are typically mast-mounted on top of tall buildings or on hilltops. Up to eight Central units can be co-located at each central site, allowing incremental deployment of network capacity at the central site.

The Central router physically transmits to all Remotes that it serves, in a point-to-multipoint manner. The Central router functionality ensures that data is only delivered to the correct remote site Ethernet. The Remote router physically transmits only to the Central router, in a point-to-point manner. The router functionality at the Central router determines if the data should be routed over its Ethernet link or to another Remote router that it serves.

Configuration

Figure 1-2 shows how a single Central site network might be constructed as part of an Internet Service Provider network, or corporate intranet. The Remotes and Centrals are connected to local routers or local computer systems through Ethernet. It is also possible for the Central to have no local connections, functioning only as a router for traffic between Remotes. The NMS can be connected by means of the Central or Remote sites. More than one NMS may be used simultaneously on the network.

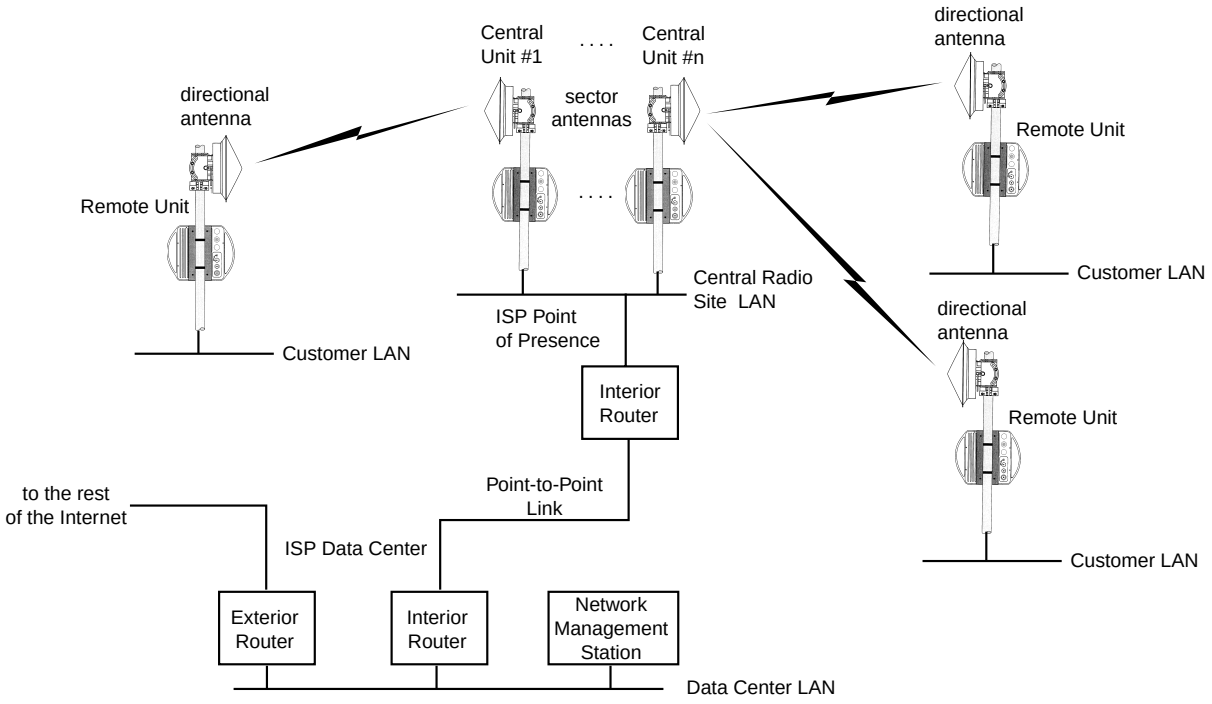


Figure 1-2. Radio Network Example

The network configuration limits are:

- Up to eight Central units per central site location
- Up to 30 Remote units per Central unit (240 per central site)
- Central to Remote line-of-sight distances of up to 10 km

Theory of Operation

The WaveNet Access 3500 system is licensed band wireless point-to-multipoint data communications system. It is intended to provide reliable data transmission between remote location networks and devices and a central location. The system is tailored to provide internetworking communications, but could be extended for use with other transaction-oriented data traffic. The system accepts IP datagrams of up to 1500 bytes from central and remote site networks and devices, and routes these packets between central and remote site networks and devices in a manner consistent with typical industry internetwork access routers.

Outbound Packets

Packets flow from the Central router to the Remote routers in the outbound channel. Packets destined for all Remotes share this channel. Each Remote router examines each packet, and accepts those that have the correct radio network address (RF Net ID as defined by the Central radio's MAC address) and are addressed to its radio interface station address. Normally these packets are either received locally by the Remote router (for router management functions), or forwarded to the Remote router's Ethernet network based on the packet's destination IP address and the contents of the Remote router's Route Table. If there is no Route Table entry matching the packet's IP network address, the packet is discarded. Packets are transmitted on the outbound channel based on the order in which the Central router receives them, except when Bandwidth Reserved for UDP is greater than zero. In this case, packets carrying voice are sent ahead of data packets, regardless of the order in which they are received.

When Bandwidth Reserved for UDP is greater than zero, the maximum MTU size is reduced from 1500 bytes to 770 bytes, to reduce latency of voice packets.

Inbound Packets

Packets flow from the Remote routers to the Central router in the inbound channel. Packets destined for the Central router from all Remote routers share this channel. The Central router acts on these packets in the same manner that the Remote routers act on packets from the outbound channel. When one Remote router addresses a packet to another Remote router, the packet is first transmitted to the Central router, which in turn transmits it to the destination Remote router.

Reservation Requests

When a Remote router initially has one or more packets to transmit to the Central, it signals its need to transmit by placing a *reservation* request in the inbound contention channel. This channel is divided into slots, which are shared by all Remote routers. It is possible that more than one Remote will attempt to transmit in the same slot (a *collision*), and as a result either one or the other

Remote will succeed in transmitting its request, or else neither will succeed. If the Remote does not receive an acknowledgment that it can transmit its packet(s), it retries the reservation request. The number of slots available is sufficient to ensure that no Remote router is consistently blocked from making reservation requests due to collisions.

When the Central router receives a reservation request from a Remote router, it adds the Remote router to its *polling* list. The Central router polls each Remote router on its polling list in a round-robin manner. When a Remote router receives a *poll request* from the Central router in the outbound channel, it responds by transmitting one data packet in the inbound channel.

Protocol

To make efficient use of the radio channel, media access control (MAC) and link layer communications protocols are implemented. This protocol permits reliable data transport and multiplexing of multiple logical connections between the Central and the Remotes, insuring that the system will continue to function well even in periods of peak demand.

Data and Unit Capacity

In a cellular deployment, up to four Central units may be co-located at any single central site, provided each Central unit is connected to an antenna that covers no more than a 90° arc (sector). The resulting raw system capacity is:

4600 kbps * 4 = 18.4 Mbps.

The usable (or effective) capacity (after factoring in radio protocol overhead) is:

3250 kbps * 4 = 13 Mbps.

In a non-cellular deployment, up to six Central units may be co-located at any central site, provided each Central unit is connected to an antenna that covers no more than a 60° arc (sector. The resulting raw system capacity is:

4600 kbps * 6 = 27.6 Mbps.

The usable (or effective) capacity (after factoring in radio protocol overhead) is:

3250 kbps * 6 = 19.5 Mbps.

The number of Remotes supported by the system is determined by the amount and type of traffic created by the end devices, the maximum delay permitted, and the throughput desired. The actual capacity can only be determined after the traffic characteristics of the attached devices and networks is known.

User Interface

The WaveNet Access 3500 has a Web browser based User Interface (UI), which is the primary configuration interface. It can be accessed using any popular Web browser such as Netscape Navigator and Microsoft's Internet Explorer. The UI can also be used to monitor and control each WaveNet Access 3500 in a network, both locally and remotely.

The browser UI provides the interface necessary to fully configure the WaveNet Access 3500 (radio parameters, routing information, and so on). The UI also provides easy access to a number of radio statistics and other useful parameters.

In addition, a Palm PDA device (with Palm OS 2.0 or above) interface, connected to the circular 9-pin round connector on the router, provides a user interface for reading the radio LEDs and RSSI levels.

Network Management System

The WaveNet Access 3500 system can be monitored and controlled with a network management system (NMS). This system provides the capability to monitor and control the network from any internetwork-connected location. The system can be monitored and generally managed using standard NMS platforms (for example, HP PC or Unix-based OpenView, SunNet Manager, or IBM NetView/6000). Customers who already use an NMS system will be able to integrate day-to-day operational management of WaveNet Access 3500 systems in a manner consistent with their other managed networks and devices.

Radio Subsystem

The radio subsystem is actually two subsystems: one for the Central unit and one for the Remote unit. The Central unit transmits in the 3.50-3.60 GHz band, and receives in the 3.40-3.50 GHz band. The Remote unit transmits in the 3.40-3.50 GHz band, and receives in the 3.50-3.6 GHz band. The radio subsystem (including its MAC layer) is required to provide a reliable channel over a maximum distance 10 kilometers (assuming a line-of-sight path), although it is recommended that for frequency reuse purposes that systems be engineered for a maximum radius of 5 kilometers.

When service demands are below system capacity, the system is generally able to transmit IP datagrams with a round-trip delay of under 80 ms.

The radio link operates at a raw rate of 2300 kbps full-duplex, which provides inbound and outbound channels, each operating at a raw data rate of 2300 kbps. The outbound and inbound channels can operate in excess of 70% efficiency.

Networking Support

The system acts as a metropolitan area access router between branch networks and a central network and each other. It is intended to support real-time packet data and non real-time applications.

Network Management

SNMP

The system contains a network management function, which monitors and controls the WaveNet Access 3500 network. The network management function is provided by a combination of an SNMP agent on each unit and an SNMP Network Management System (NMS) that can query and set parameters by communicating with the agents, as well as accept traps from the agents that can in turn be presented as alarms to the NMS user.

The network management function provides the following control capabilities:

- Configuring the software
- Setting parameters associated with the operation of the system
- Configuring hardware parameters
- Resetting system components
- Enabling and disabling Remote units
- Other operational actions.

The network management function provides the following monitoring capabilities:

- Monitoring RF connection quality
- Recording statistics and events
- Displaying status and alarms
- Assistance in fault location and correction

All local and remote management functions are be available through SNMP gets, sets, and traps, except for establishing SNMP community names, which for security reasons can only be done through local access to the units. Routine monitoring and control functions are available through standard NMS applications, generally available on common NMS platforms.

Maintenance Interface

Certain maintenance functions, such as monitoring radio statistics, are available through the Maintenance Interface, a 9-pin circular MIL connector that connects to an external Palm PDA device (with Palm OS 2.0 or above). The Maintenance

Interface is in fact an access point to the operating system's (VxWorks) shell. The shell is also available through Telnet, although Telnet access is user name and password protected, while there is no security on the maintenance interface.

Installation

The Remote and Central units are mounted outside, near the antenna, to reduce RF antenna lead losses.

Normally, a line-of-sight path of no more than 5 kilometers is required to ensure a good RF connection between the Central and Remote; however, greater or lesser distances may be supported based on the quality of the path and level of interferers.

Security

Security provisions exist at several levels, allowing a highly secure network to be deployed. Specific security features include:

- A proprietary physical layer protocol protects the decoding of data from raw radio transmission
- An authentication feature (when enabled) prevents unauthorized Remote units from accessing radio network
- Static route tables ensure that remote sites only receive packets destined for their local networks
- Passwords and community names restrict management operations to authorized users

Due to these features, the radio network is more secure than the typical wireline networks that link to it (Ethernet, PPP links, and so on). To ensure user application security, normal industry security practices should be employed (such as the use of firewalls and application-level encryption).

The objective of the authentication feature is to verify that a Central only allows authorized Remotes to synchronize with it, and that a Remote does not enter normal operation until the Central authorizes it to do so. It is assumed that only actual WaveNet IP 3500 units can succeed in communicating valid packets, due to the proprietary radio PHY and MAC layers, and that MAC addresses are unique to specific physical units.

A Remote only synchronizes with a Central that is configured on the same channel as the Remote. After a Remote synchronizes with the Central, the Remote sends the Central an Authentication Request. The Central is configured to either approve requests from all Remotes (when Radio MAC Authentication is disabled at the Central), or a fixed list of Remotes (when Radio MAC Authentication is enabled at the Central). The Central responds to the Remote with an approval if the MAC address of the Remote is recognized by the Central,

or else it replies with a disapproval. The Remote retries this operation if it receives no response in a certain number of seconds. If a Remote receives a disapproval, it pauses for a time period of a minute or more and then retries the operation.

No encryption of any data is provided.

Management

There are three basic management facilities included with each router:

- HTTP/HTML server providing embedded management Web pages
- SNMP MIB-II and WaveNet Access 3500 enterprise MIB support
- FTP upload and download of configuration data files and system software

Configuration and monitoring of individual routers can be accomplished, both locally and remotely, using the Web pages served from within the router itself. In-depth network monitoring can be accomplished using an SNMP network management station (NMS), using both the standard MIB-II variables as well as device-specific variables included in the supplied WaveNet Access 3500 enterprise MIB. The router contains a non-volatile FLASH file system. Configuration data and system software are stored in various files that can be accessed by means of FTP. No special management applications are required to use these facilities.

Network administrators can enable or disable access to these facilities, and can limit access by use of passwords or SNMP community names.

2 Network and Site Planning

This chapter details the planning that should be completed prior to system deployment, starting with application requirements such as geographical service area and performance levels. Next, a determination is made regarding router physical site locations and number of routers required. Finally, configuration requirements for individual routers are decided. This chapter contains the following sections:

Establishing Requirements

The following subsections give information to help you plan the objectives, security provisions, and reliability of the system.

Service Area, Capacity, and Performance

Prior to planning the physical network topology, one should establish the design objectives for the network. While the exact information needed varies from network to network, the following items represent the type of information compiled at this stage:

- A physical map showing the desired coverage boundaries for remote sites, and locations of network backbone access points, central data centers, and any other high-bandwidth connectivity sites.
- Locations of all known remote sites (both wireless and wireline) should be marked on the map, and approximate numbers of potential remote sites should be indicated by area.
- Locations of network management centers should be indicated.
- Good potential central site locations (tall buildings, communication towers, hill tops) and major line-of-sight obstacles should be indicated.
- Typical and worst-case performance requirements should be determined for the remote sites, including the network bandwidth needed (in IP packets per second), and the corresponding percentages of time that a given Remote will be demanding service (as opposed to being idle). If inbound and outbound directions are significantly unbalanced, the numbers for both directions should be estimated. These numbers are best determined empirically by measuring existing network traffic, when possible.

Security

A special tool is required to access the router enclosure, which provides physical security.

Also, care should be taken in planning the network locations of management centers so that SNMP community names and FTP/HTTP/Telnet passwords are not sent over untrusted network links external to the WaveNet Access 3500 radio network.

Determine who will be allowed to access which level of management information from which routers, and select community names, user names, and passwords accordingly. FTP/HTTP/Telnet passwords should only be provided to the network management staff allowed to reconfigure the routers, including making changes to passwords and SNMP access writes. SNMP community names with write access allows limited reconfiguration rights, but does not

include the rights to change users, passwords, or community names. SNMP community names with read access do not allow any system configuration changes to be made, but do allow viewing of system usage and error statistics.

Reliability and Availability

Highly available configurations can be implemented at the cost of deploying redundant hardware routers. Redundant units (and antennas) can be added at the central sites and/or remote sites, depending on the availability needs of the applications.

Mean Time Between Failure (MTBF)

Central and Remote units each have a hardware MTBF exceeding 60,000 hours.

Mean Time to Repair (MTTR)

The units have no field serviceable parts, so field repair is accomplished through swapping a failed unit with a good unit. If connectivity between Central and Remote units is monitored centrally, failures can easily be detected within 15 minutes (or better, if needed). To swap a failed Radio and Router Module assembly with a good one and re-configure the unit should require less than 15 minutes, if a spare unit is available and if a person capable of installing a unit is in the presence of the unit. If no skilled personnel are at the site of the failure, travel time must be added, and there will typically be time involved in obtaining physical access to the unit. A software update and possible subsequent reconfiguration of the unit normally requires less than 30 minutes.

Planning the Network

The following subsections are designed to help you in planning and designing the overall network.

Location of Central Sites

The choice of central site locations is critical for obtaining the highest possible level of system performance. There are several technical considerations for choosing good central site locations, including:

- Clear line-of-sight (LOS) paths must exist from the central site to the remote sites
- Distances between central and remote sites must allow for good radio path margins
- The number of Remotes to be supported must be within the capacity of central site routers

- Access to power and network links to backbone networks or data centers exist.

It is highly recommended that the services of experienced local radio equipment installers be obtained.

Number of Central Routers

Up to eight Central routers may be co-located at any one central site. The number of routers to be used is based on the total network traffic capacity to be supported from the site, network architecture, and the geographical locations of the remote sites. It may be desirable to increase the number of Central routers (beyond the number needed to meet the capacity requirements) in order to allow the use of higher gain sector antenna to increase the radius of the coverage area.

Antenna Considerations

Each Central router forms a radio network separate and distinct from any other Central router's network. As such, the installer is free to use whatever types of antennas make the most sense for each Central router, given the required geographical coverage area for each Central radio network. It is allowable to connect more than one antenna to one router's transmit or receive ports. One antenna may be connected to multiple routers' receive ports, or using a splitter/isolator, to multiple routers' transmit ports.

Sectored antennas for Central units typically provide between 12 and 17 dBi gain, and typically cover between a 30° and 120°azimuth. For example, to cover 360° of azimuth using 90° azimuth 16 dBi antennas, one would typically use at least four Central routers, each connected to its own sector antenna. Because each Central radio forms an independent radio network, sectors may overlap to provide the desired amount of network capacity to any geographical area. To allow for the ability to rebalance Remote routers between multiple central site routers, it may be desirable to implement overlapping sectors, where each Remote router is within the beam pattern of more than one Central router. For example, using eight 90° sector antennas allows each Remote router to be configured to communicate with one of two different Central routers. In this case, if one Central router becomes too heavily loaded, some of its Remote routers can be reconfigured to use the other Central router.

To determine the distance obtainable from various combinations of transmit power and antennas used, first calculate the total RF path available (after allowing for path margins). Note that the gain of the Central antenna should be the gain at the lowest point utilized on its azimuth/elevation, which is typically 1 to 4 dB lower than its maximum gain.

Central Site Antennas

Table 2-1 shows the basic specifications of the central site external antenna.

Table 2-1. Central Site Antenna Specifications

Parameter	Value
Gain and Beamwidth	12 dBi, 90°, Horizontal and Vertical polarization (separate antenna for each polarity) 16 dBi, 60°, Vertical polarization
Mounting	Pole mount capability: 4.43cm-11.4cm (1.75"-4.5") mast.
Azimuth and Elevation Adjustment	The Central antenna provides up to 15° downtilt.
RF Interface	N-Type female connector.

The antenna is connected to the unit with cables normally no longer than 1.8 meters. The receive antenna attached to a Remote unit can be aimed by monitoring the RSSI interface and adjusting the antenna for maximum RSSI voltage.

Remote Antennas

Table 2-2 shows the basic specifications of the remote site antenna.

Table 2-2. Remote Site Antenna Specifications

Parameter	Value
Gain and Beamwidth	9" x 9" 20 dBi, 20° integrated panel antenna. Horizontal and Vertical polarization (separate antenna for each polarization). 20 dBi, external 18-inch parabolic dish, Horizontal and Vertical polarization 23 dBi, external 24-inch parabolic dish, Horizontal and Vertical polarization
Mounting	Pole mount capability: 4.43cm - 11.4cm (1.75"-4.5") mast.
Azimuth and Elevation Adjustment	The Remote antenna provides up to 15° downtilt (external antenna only).
RF Interface	N-Type female connector (external antenna only).

A list of antenna characteristics compliant with ETSI type certification is available in Appendix B, "List of Antennas Compliant with ETSI Type Certification."

Plan Connectivity Between Central Sites

Multiple Central units typically share a single point-to-point link (backbone) to the central site, NMS, and server resources located at the ISP Data Center. The central site may simply be a relay point into a backbone network, in which case an exterior router connects to the Central and provides a WAN link perhaps using VSAT, point-to-point narrowband radio, or copper cable connection. Other point-to-point links may be used to connect several central sites together, or to connect high traffic Remotes (such as server locations) into the network.

Whenever possible, it is desirable to locate a central site at a backbone network point of presence or the central data server site. It is sometimes possible to arrange for Central routers to share a communications tower or building roof-top with existing wireless backbone equipment.

Because the line-of-sight requirements for WaveNet Access 3500 central sites are often more stringent than for point-to-point radio sites, it may not be possible to locate the WaveNet Access 3500 central sites at existing backbone network access points. WaveNet Access 3500 central sites can be connected to a backbone network by a large range of point-to-point network link products, such as WaveNet Link Ethernet Extender, made by Wireless, Inc., spread spectrum products that operate in the 2.4 GHz to 5.8 GHz range, as well as many choices of licensed radio modems operating in millimeter band ranges (see Figure 2-1).

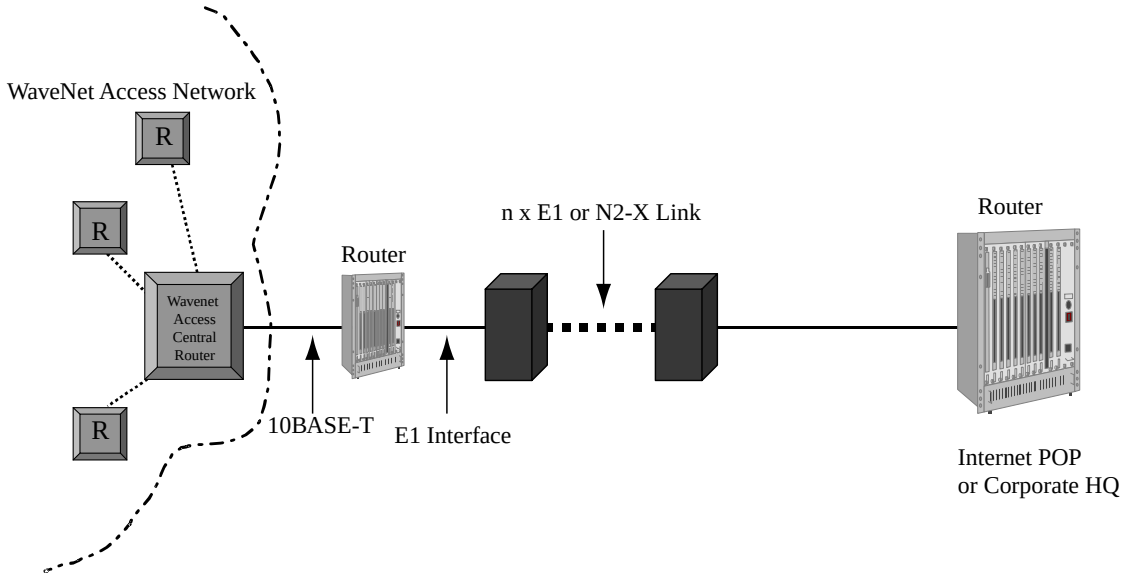


Figure 2-1. Backhaul to Network Access Point

A central site with four Central routers can typically be supported by a full-duplex point-to-point backbone connection at 4 * 2.048 Mbps (8.192 Mbps), while a central site with eight Central routers may require a link speed of 8 * 2.048 Mbps (16.384 Mbps) (full-duplex).

Where there are a small number of WaveNet Access 3500 central sites, it is simplest to connect each site directly to the backbone network. Where there are many central locations (such as in an extensive cellular configuration), it may make most sense to connect central locations together into a ring or mesh network, which in turn is connected to the backbone network (see Figure 2-2).

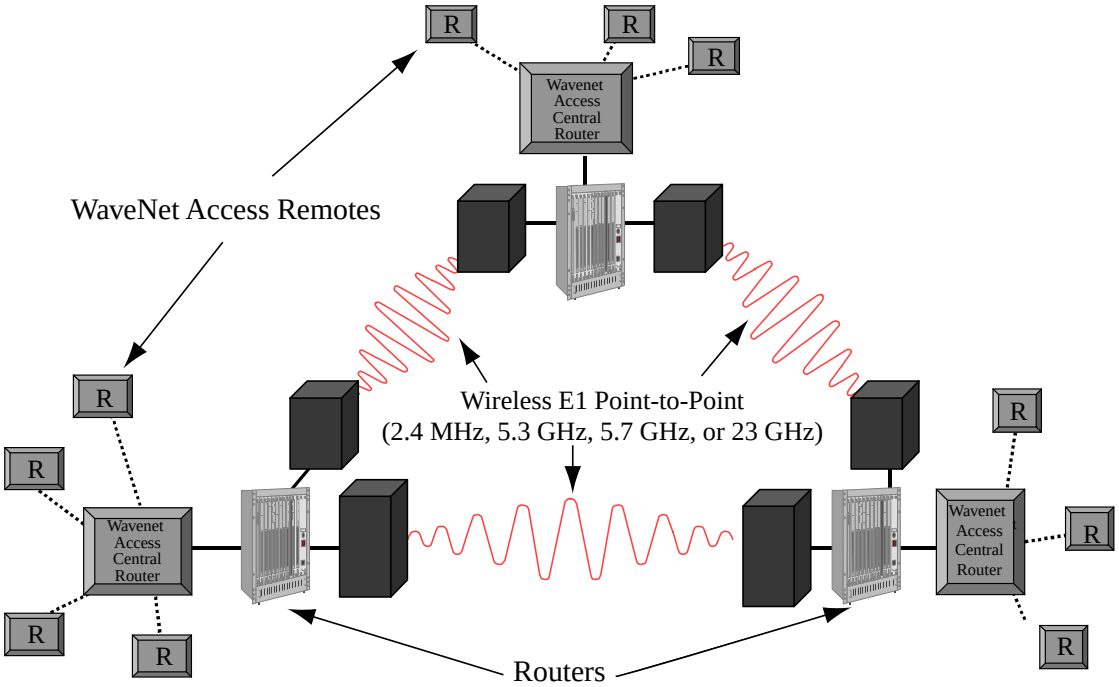


Figure 2-2. Central Sites in Ring Network

Repeater Configurations

It is possible to use two Remote routers in a back-to-back configuration to act as a repeater between two central sites located in different directions from the repeater location (see Figure 2-3). Note that this configuration can use a dedicated Central router (as shown) for maximum bandwidth, or can share the same Central router as other Remotes if there is limited traffic between the networks.

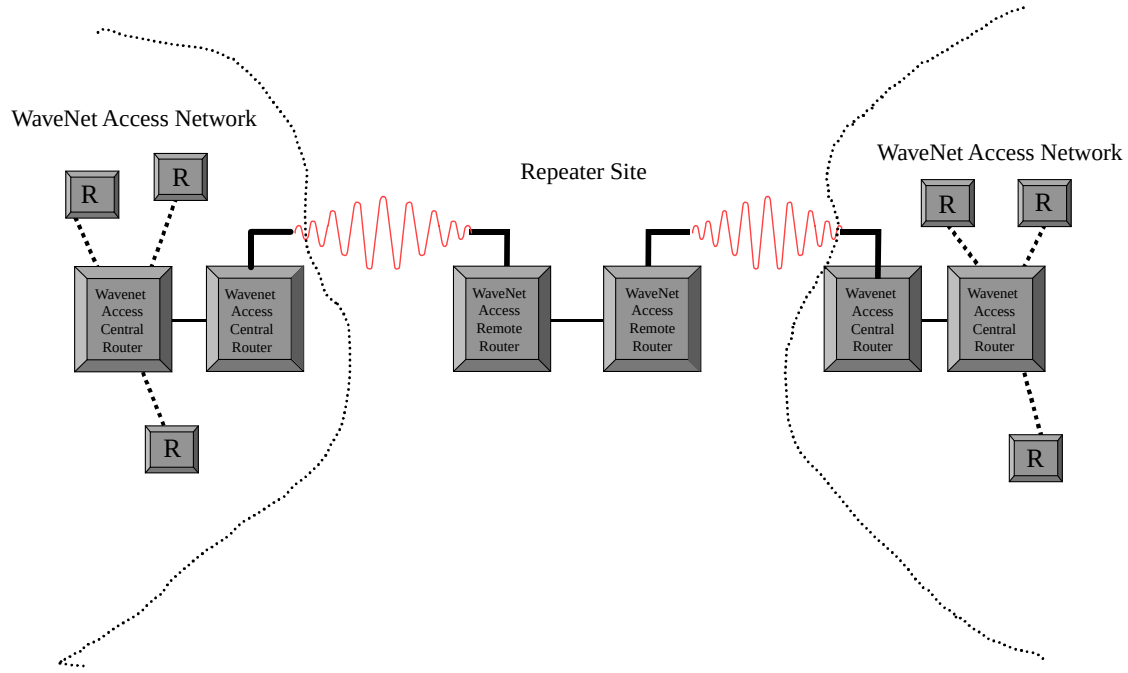


Figure 2-3. Repeater Using Back-to-Back Remote Routers

Alternatively, a single remote site located beyond the range of the system can be connected to a Remote router (within range) by using any pair of WaveNet Access products (see Figure 2-4).

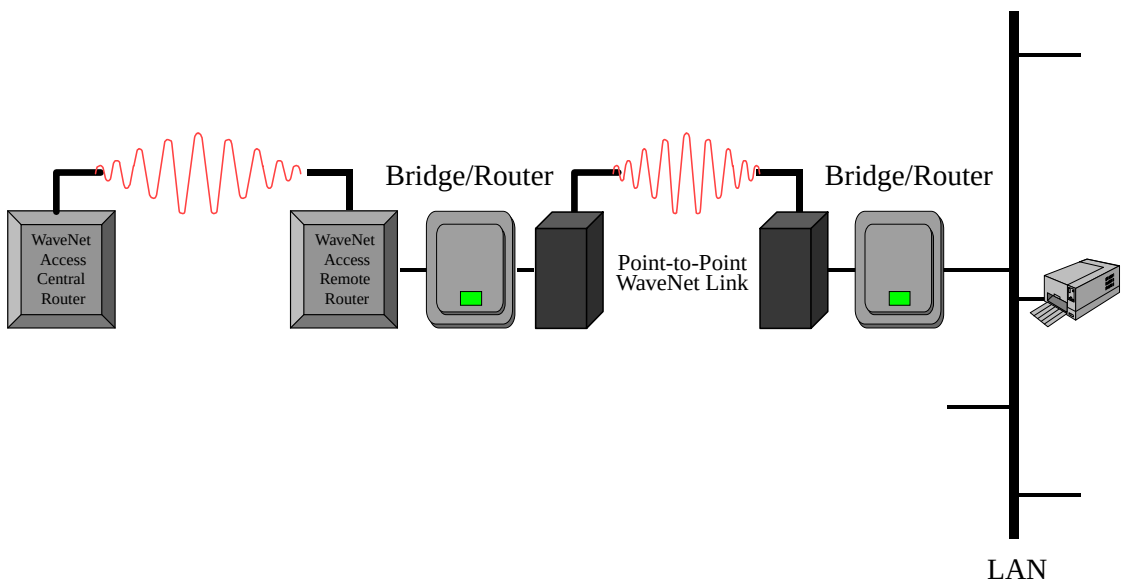


Figure 2-4. Repeater Using Point-to-Point Radio Link

Plan Connectivity Between Co-Located Central Routers

When there are many remote sites served from multiple Central routers located at a single central site, the easiest way to administer the routing between the radio networks is to use an external router connected to the central site that knows the routes to all of the remote sites. It is likely that there is already a backbone router at the central data center that could perform this function. In this way, there are only two route tables to be updated when adding or deleting a Remote router: the table belonging to the external router, and the table belonging to the Central router on the radio network for that Remote router.

The alternative approach is to configure a route for each remote site in the route tables of every central site router that needs connectivity with that remote site. This can be practical when Remote routers are added and deleted from the network infrequently, or when the number of Central and Remote routers is small. In this case, only an Ethernet hub is needed to link the Ethernet interfaces of the Central routers.

Plan IP Network Addressing

The radio interfaces on a given Central router and its associated Remote routers form a unique IP network (or subnetwork), and need to be assigned the same network address, with unique host addresses within the network. This requires allocating a radio IP network address for each Central router. To avoid consuming IP addresses for the radio network, it is allowable that you use addresses in the private range of Class C addresses 192.168… The Ethernet

interfaces on each Central and Remote router are assigned host addresses within their Ethernet networks. If the central site is connected to the backbone network by a router (recommended when there are multiple central site routers), then an IP network address must be assigned for the central site router's Ethernet network. It is a good practice to record the IP address planning information with the network map.

Plan Routing Information

The Central and Remote routers each contain a Route Table that controls how packets are routed between its Ethernet and radio networks. It is not necessary to add explicit routes for packets destined for the network addresses of either the radio or Ethernet network, because the router will infer these routes from the IP addresses and subnet masks for these interfaces. A Destination IP Address value of "default" will apply to all packets other than those addressed to the local networks of the Ethernet and radio interfaces or those with explicit Route Table entries. The Route Table entries contain:

- Destination Network Address
- Subnet Mask For Destination Network
- Next Hop IP Address (address of next router on the local Ethernet or radio network)

It is common for the Remote router's default route to have the Next Hop IP Address be that of the Central router's radio interface.

For a Central router, there is typically a route to each remote LAN. Where the Central router connects to a backbone network router, it is common for the Central router's default route Next Hop IP Address to be the backbone router's interface on the Central router's Ethernet network.

When there are four co-located central site routers, and packets must be routed between the multiple radio networks, each central site router needs route table entries for all remote networks. Alternatively, a separate Ethernet router (not a WaveNet Access 3500 router) can be used at the central site to route packets between the Central routers, allowing each Central router to only need routes to its own remote networks.

Route table entries (other than the default route) apply the subnet mask for the routing decision. Each route table entry can use a unique subnet mask, and CIDR and supernetting are supported.

Planning Individual Sites

This section details the planning that should be done prior to installing equipment at each specific site. Whenever possible, it should be completed prior to actual installation, especially for central site locations. Experienced installers may be able to accomplish these steps at actual remote site installation time if they carry stocks of the various cable, power, and installation material options.

Location of WaveNet Access 3500 Router

The WaveNet Access 3500 router is a single outdoor enclosure, designed to be mounted on a 1.75 - 4.5" (4.45 - 11.43 cm) mast. The router is typically installed on a communications tower, on top of a building, or on the side of a building. The router is connected to indoor data and power sources through a custom combined data and power cable. The key factors in selecting the specific installation location are good line of sight between central and remote antennas.

Power Supply Requirements

The router board incorporates switching power supply circuitry that converts an AC or DC power source to the appropriate operating voltages required by the router and radio assemblies. Figure 2-5 shows one of the power supply configurations that supplies power to the router and radio assemblies. It consists of an AC to 24V DC adapter, AC power cord, and DC power cord with spade lugs that connect to the data/power cable.

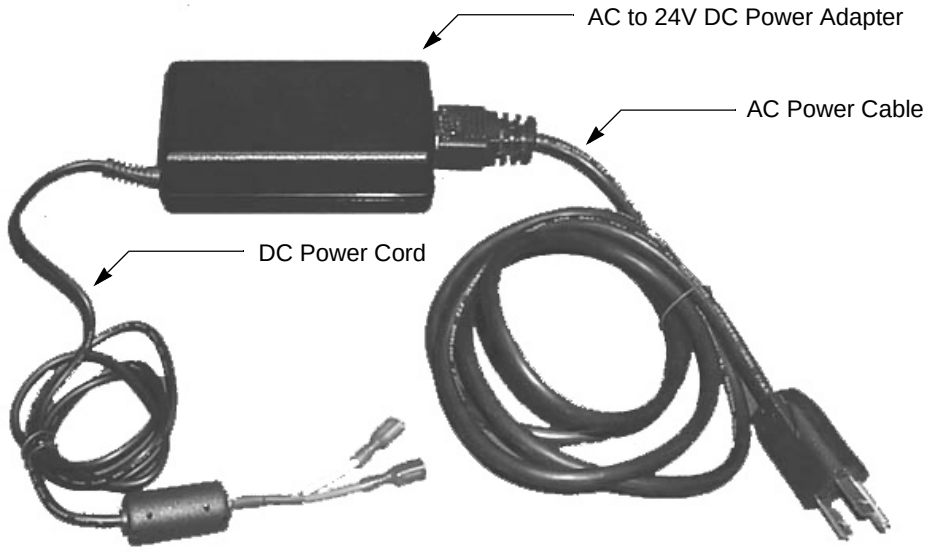


Figure 2-5. AC to DC Power Supply

Note: The primary power interface connection at the 4-pin power connector has transient protection devices across the active pins to provide a level of protection against near by lightening strikes (as does the Ethernet interface).

AC Power Input

The router power supply pins can accept an AC input voltage in the range from 14 to 29 VAC. This voltage may be supplied directly to the connector, or an external step-down transformer may be used. There is an existing approved unit that accepts 103 to 265 VAC, 50/60 Hz, and outputs 14 to 29 VAC for the router.

DC Power

The router is designed to operate with ±20 to ±41 VDC applied directly to the power pins. Voltages of ±45 to ±56 VDC may be used if they are first limited with an external voltage limiter. The limiter is intended to be mounted indoors, and has 6-32 threaded input and output terminal studs. To connect to the studs, use crimp-on lug terminals designed to mate with a #6 screw terminal. Connect the input wires to the ±45 to ±56 VDC source and the limited output (±20 to ±41 VDC) to the router power connector pins.

Power Supply Input Fuse

The router board incorporates a 5 X 20 mm type fuse on the input to the power supply. The fuse is factory replaceable without the need for special tools (such as a soldering iron).

An extra fuse is shipped with each unit. The fuse is contained in a plastic bag that is placed in the shipping container with the WaveNet Access 3500.

Note: The fuse may be replaced only at an authorized repair depot or at the factory.

Power Consumption

The WaveNet Access 3500 router consumes 25 Watts (maximum).

Power Cable

A cable that combines Ethernet and power is provided to ease cable pulling. Provisions for grounding and surge suppression are made within the router units, and must also be considered by the installer at the point that the data and power cables enter the indoor environment

The power sources should be rated to deliver 40 VA. Consult Table 2-3 for the acceptable voltage levels at the indoor end of the power cable. Table 2-3 shows the allowable input voltage ranges for each power option using various length power cables:

Table 2-3. Power Supply Options

Cable Length	Power Options			
	110 VAC Transformer	220 VAC Transformer	± 24 VDC (Native)	± 48 VDC Limiter
0 m. (0 ft.)	88-136	176-265	±20 to ±41	±42 to ±60
25 m. (82 ft.)	88-136	176-265	±21 to ±41	±42 to ±60
50 m. (164 ft.)	88-136	176-265	±22 to ±41	±42 to ±60
100 m. (328 ft.)	103-136	206-265	±23 to ±41	±42 to ±60

Antennas and Antenna Cables

There are three types of antennas: central, external remote, and integrated remote. External antennas are typically mounted above the routers, sharing a common mast. The antennas typically come with their own mast mounting hardware. The remote and central antennas usually come with female N connectors, and require separate cables with male N connectors on both ends. The antenna connection cables should be less than six feet in length, although longer cables can be used.

Note: Long antenna cable runs cause substantial loss of signal.

Central antennas are designed for sector coverages of either 60° or 90°. Remote integrated antennas have a 20° beam, and external remote antennas are in the form of a 18-inch or 24-inch dish.

Figure 2-6 shows how the routers and antennas mount on the antenna mast and how the cables are connected.

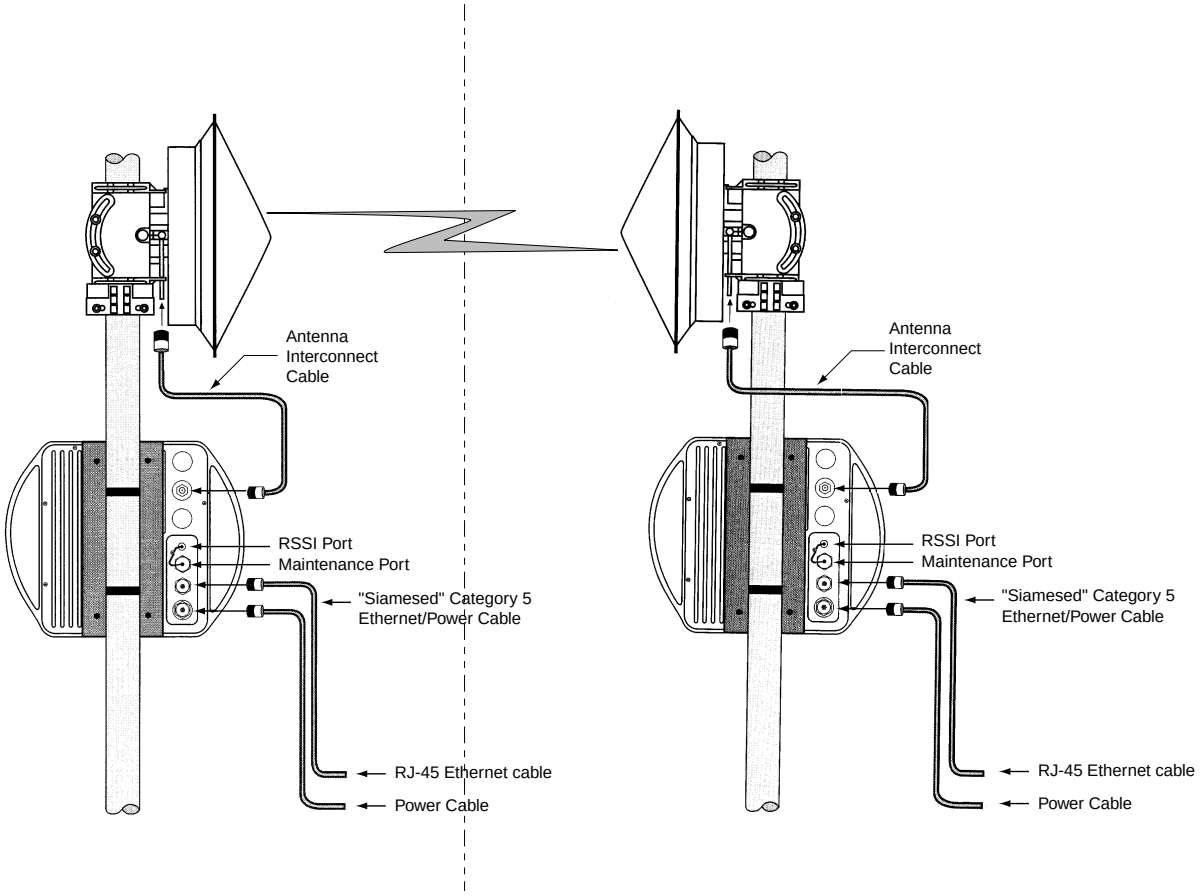


Figure 2-6. Typical Deployment of 3500 Router in a Point-to-Point Configuration

Data and Power Cable

The cables connecting the router to the indoor Ethernet equipment and power sources are combined into a single physical cable that can be split at both the router and the indoor ends. The cable and its connectors are shown in Figure 2-7.

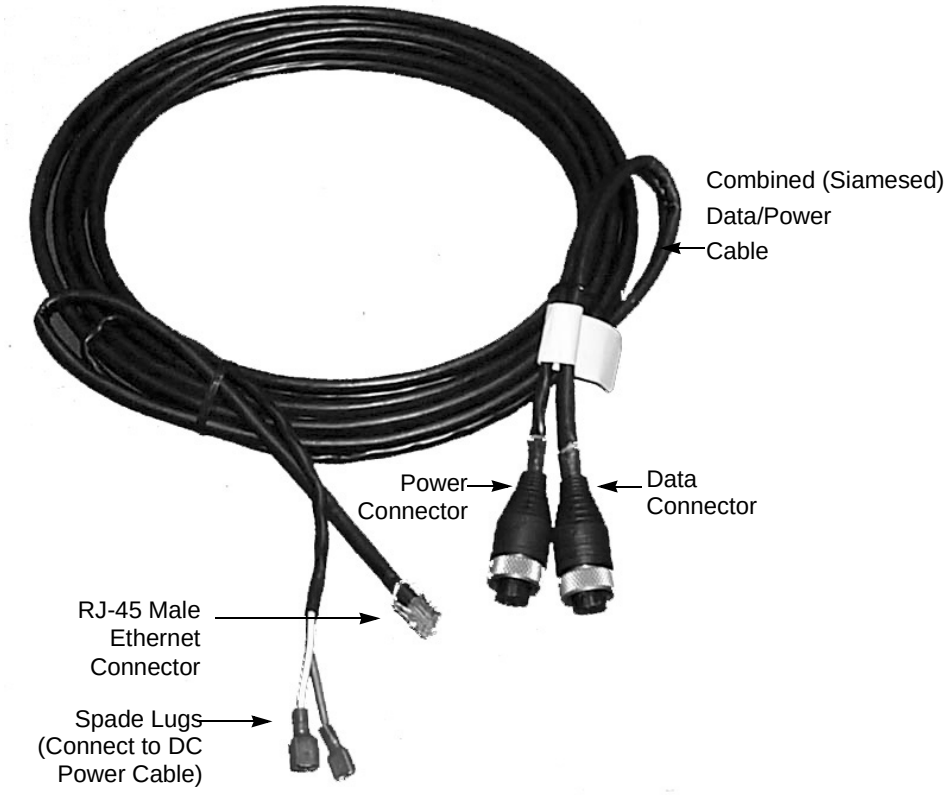


Figure 2-7. AC to DC Power Supply

The cable has an outside plant (OSP) rated polyethylene jacket and is gel-filled to prevent water from entering the cable. The jacket material does not generally meet indoor flammability regulations, and should be terminated or coupled to indoor-rated cable if the indoor cable runs are lengthy. Consult fire and electrical safety regulations for the rules that apply to each installation site[1]. The cable length from the indoor termination to the WaveNet Access 3500 can be up to 100 meters. The data cable distance can be increased (if needed) by using an Ethernet hub/repeater for the 10BASE-T connection.

1. The U.S. National Electrical Code requires that OSP cable be terminated within 50 feet of entering a building.

The power section of the cable consists of a single twisted-pair of #16 AWG conductors. It is designed to be connected to an AC or DC source that meets the specifications described above. It comes terminated on the router end with a 4-pin circular MIL connector, and is unterminated at the power source end, since this typically connects to screw terminals or wire mating crimp connectors.

The data section of the cable consists of four twisted pairs of #24 AWG conductors meeting Category 3 specifications, gel-filled, and surrounded by foil and braid shields. The cable comes terminated on the "inside" end with an RJ-45 connector wired according to the EIA/TIA T568B standard. The "outside" end is terminated with an 8-pin circular MIL connector. To terminate the indoor end at a punch-down block or lightning suppressor, the installer can cut off the connector and strip the jacket, shields, and conductors as needed. The router connector locations are shown on Figure 2-8.

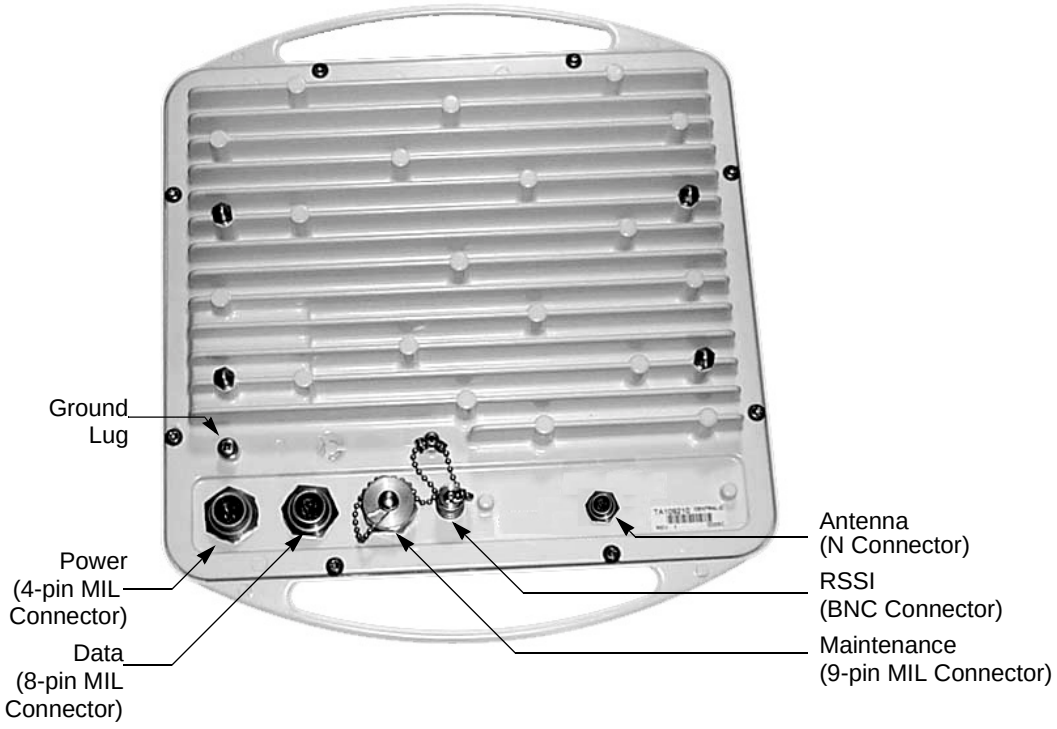


Figure 2-8. Central Router Connector Locations

Lightning Protection and Grounding System

Grounding is vitally important to protect indoor equipment and personnel from lightning strikes to the outdoor routers, and to generally ensure correct operation of the radio and digital circuitry. If a high-quality ground is not available at the planned installation site, it should be constructed prior to equipment installation.

To construct a good ground, ground rods should penetrate the earth to a depth of about two meters (six feet). Where the ground is in rocky terrain, make sure that the ground rods penetrate into loose soil. In sandy soil, use more ground rods to make sure that the ground has sufficient contact with water bearing material.

Use #4-#6 AWG wire to connect each ground rod to the equipment to be grounded. The cables should be free of sharp bends. Each ground cable should be at least two meters in length with at least one meter separation between each.

Refer to local and national electrical codes to determine acceptable grounding methods.

The router enclosure should be directly connected to ground to ensure that it functions correctly.

To protect indoor equipment and personnel from lightning strikes to the router or antenna, the data and power portions of the combined data/power cable should be individually protected by the use of lightning suppression equipment at the point where the cables enter the building.

The data portion of the cable has a foil/braid shield that should be directly connected to ground, and the individual conductors should be connected to appropriate lightning suppression equipment, which is in turn connected to ground. Since only conductors 1 (white/orange), 2 (orange), 3 (white/green), and 6 (green) need to be connected to the indoor equipment, only these conductors need be connected to the lightning suppression equipment. The other conductors should terminate prior to entering the building, and ideally should be connected directly to ground.

Although the cable shield is grounded to the enclosure at the weather seal, this ground is not sufficient to provide lightning protection to indoor equipment and personnel.

The power portion of the cable has two conductors, both of which should be connected to an appropriate lightning suppression unit at the point of entry into the building.

To protect the router itself from a lightning strike, it could be placed within a larger metal enclosure that is grounded, and internally contains lightning suppression equipment for the data, power, transmitter coordination, and

antenna leads. Alternatively, lightning protection equipment could be installed in the close vicinity of the router, such that only very short cable runs exist between the lightning protection equipment and the router.

For additional information on grounding practices and lightning protection, refer to Appendix C, “Grounding Practices and Lightning Protection Information.”

3 Pre-Installation Configuration

This chapter contains the procedures to follow that allow you to complete the configuration of the routers to the extent possible prior to the actual physical installation. It contains the following sections:

- "Terminate The Data/Power Cable"
- "Configure Router"

The configuration procedures make it possible to verify the operation of the unit in a controlled environment, prior to dealing with the unique aspects of the installation site. While it is recommended to complete these steps prior to of the physical installation process, it is possible to execute these procedures as part of physical installation, if necessary.

Terminate The Data/Power Cable

If the combined data and power cable to be used in the installation is available, it is best to use it for the procedures in this chapter. If it is not available, then a separate test cable should be prepared.

The power portion of the cable is terminated on the router end with a 4-pin circular MIL connector. The wire leads on the indoor end can be directly attached to the power supply (if it provides screw terminals), or they can be connected to the supply using crimp-on connectors. Either of the wire leads can be connected to either of the power supply terminals for either AC or DC power sources.

The data portion of the cable is terminated on the indoor end with an RJ-45 connector wired according to the EIA/TIA T568B standard as shown in Table 3-1. The outdoor end is terminated with a eight-pin circular MIL connector.

Table 3-1. RJ-45 Connector Pinout

RJ-45 Pin	10BASE-T Standard T568B	10BASE-T Crossover
1	White/Orange	White/Green
2	Orange	Green
3	White/Green	White/Orange
4	(Unused)	
5	(Unused)	
6	Green	Orange
7	(Unused)	
8	(Unused)	

Figure 3-1 shows the physical layout of the RJ-45 connector.

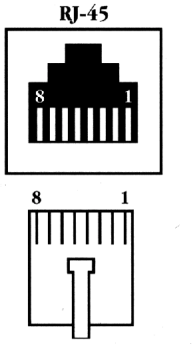


Figure 3-1. RJ-45 Physical Connector

If the indoor end is connected directly to an Ethernet hub, the cable can be used as is. If the indoor end is terminated at a punch-down block, make sure that the wire colors are connected to the block as shown in Table 3-1 for the T568B standard mapping onto the RJ-45 positions as defined for that punch-down block.

If the indoor end is connected in a point-to-point configuration directly to another Ethernet DTE (such as a PC or DTE-configured interface of a bridge or router) without the use of a hub, the 1/2 and 3/6 conductor pairs must be crossed-over as shown in the "10BASE-T Crossover" column of Table 3-1. This is best accomplished by connecting two standard cables to a dual modular jack terminal box, making the crossover between the two jacks within the terminal box. This avoids the possibility of confusing normal and crossover wired cables.

The RJ-45 connector used for the indoor end of this cable is designed for large-diameter round cables. If the cable is cut and re-connectorized, be sure to use an appropriate RJ-45 connector, rather than those that are commonly available for use with indoor telephone cable. Alternatively, use a modular jack terminal box or punch-down block to terminate the cable to avoid the possibility of a bad connection.

Configure Router

The router is configured using the Web browser over the Ethernet interface. In the following procedures, underlining designates Web page links. The configuration information is stored in the router in non-volatile memory, so you can remove power form the router and transport it without losing any of the information.

Equipment Needed

- A PC with a 10BASE-T Ethernet interface , Netscape Navigator 3.0 (or later) or Microsoft" Internet Explorer 4.0 (or later), and *ping* and *traceroute* utilities.
- A 10BASE-T Ethernet hub (disconnected from any other devices), or 10BASE-T cross-over dual modular jack terminal box.
- One 10BASE-T patch cable
- One WaveNet Access 3500 combined data/power cable

PC Internetwork Configuration

- IP address: 10.0.0.xxx (where xxx is any number between 2-254)
- Subnet mask: 255.0.0.0
- Gateway address 10.0.0.1 (factory default)

Router Configuration Procedure

1. Ground the router enclosure at the grounding lug (see Figure 2-8) or any other point.
2. Connect an antenna or attenuator to the antenna port on a Central or a Remote enclosure.

Note: There must always be a load on the transmit antenna port when power is being supplied to the unit. Failure to do so may cause damage to the radio interface.

---

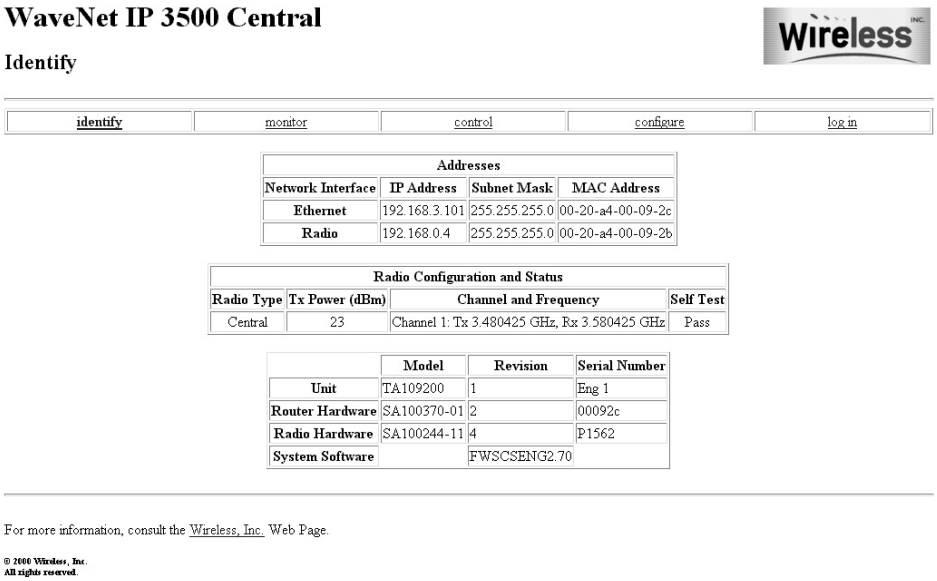
3. Connect the data cable between the router and the Ethernet hub (or cross-over modular jack terminal box).
4. Connect the power cable to the power supply.
5. Connect the power supply to the power source.
6. Wait one to two minutes for the router to initialize.
7. After the router initializes, the following parameters are temporarily set to the values shown below.
   - IP address of Ethernet interface: 10.0.0.1; subnet mask: 255.0.0.0
   - IP address of Radio interface: 172.16.0.1; subnet mask: 255.255.0.0

   Note: These values do not overwrite the values displayed on the internet configuration screen, but are displayed on the identify page.

   ---

8. Connect the PC to the Ethernet hub (or cross-over modular jack terminal box).

9. From the PC's Web browser, enter the router's IP address (URL) "10.0.0.1" and confirm that the router's **Identify** page is displayed, as shown in Figure 3-2.



WaveNet IP 3500 Central

Identify

identify | monitor | control | configure | log in

Addresses			
Network Interface	IP Address	Subnet Mask	MAC Address
Ethernet	192.168.3.101	255.255.255.0	00-20-a4-00-09-2c
Radio	192.168.0.4	255.255.255.0	00-20-a4-00-09-2b

Radio Configuration and Status			
Radio Type	Tx Power (dBm)	Channel and Frequency	Self Test
Central	23	Channel 1: Tx 3.480425 GHz, Rx 3.580425 GHz	Pass

	Model	Revision	Serial Number
Unit	TA109200	1	Eng 1
Router Hardware	SA100370-01	2	00092c
Radio Hardware	SA100244-11	4	P1562
System Software		FWSCSENG2.70	

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

Figure 3-2. Identify Page (Central)

Note that no network login is required whenever the router's Ethernet interface IP address is 10.0.0.x, where x=1-254.

Note: IP addresses in the range 10.0.0.1-10.0.0.254 should not be used except for temporary initial configuration.

---

10. Select **configure**.

The **Configure** page appears, as shown in Figure 3-3.

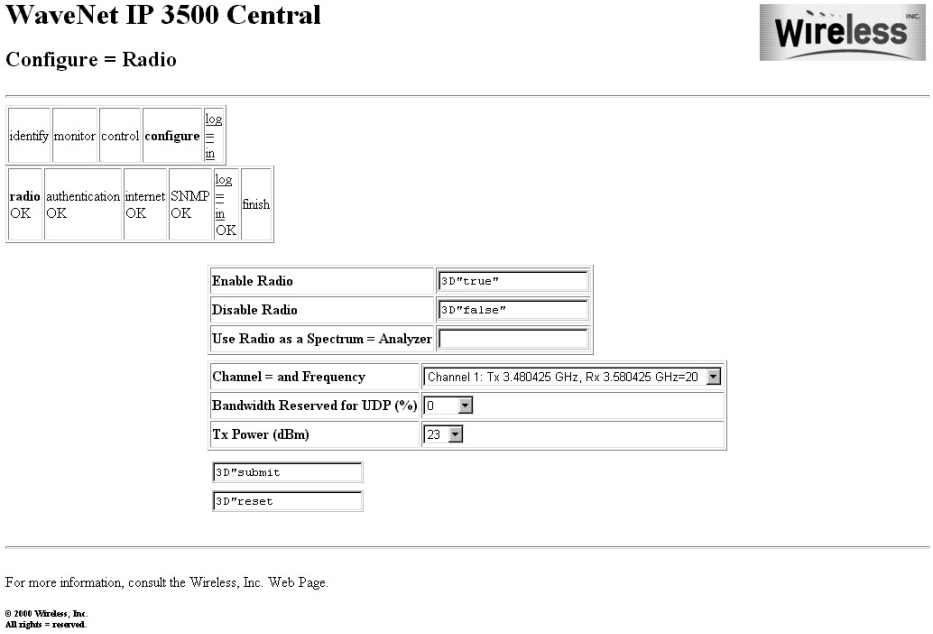


Figure 3-3. Configure Page

Within the **Configure** page, there are several subpage links. Select the link to each page in succession to configure or verify the configuration of the router. Note that on each configuration page there is a **reset** button, which resets the parameters to the values that were present upon entering the page. After making configuration changes on a page, click **submit**. After completing all of the desired configuration, select **finish**. Each of the subpages configure the parameters described in the bulleted list below.

- **radio**: Enable/Disable Radio, Channel Number, Bandwidth Reserved for UDP (%), and TX Power (dBm)
- **authentication**: Enables/Disables Radio Authentication (Central only); Radio MAC Address table
- **internet**: Ethernet and Radio IP Addresses, Subnet Masks, Route Table
- **SNMP**: Enable/Disable SNMP, Access Table
- **log in:** Enable/Disable HTTP, FTP, and Telnet Access, Set User Names and Passwords

For a detailed description of each of these subpages, see "Configure Subpages" on page 3-8.

11. **Click finish** on the **Configure Radio Authentication** page.

If your configuration contains errors, the **Configure** page appears as shown in Figure 3-4, indicating that there are configuration errors. The page or pages that are in error are so indicated on the page. If this happens, you must return to the page with errors, correct the errors, and click **finish** again.

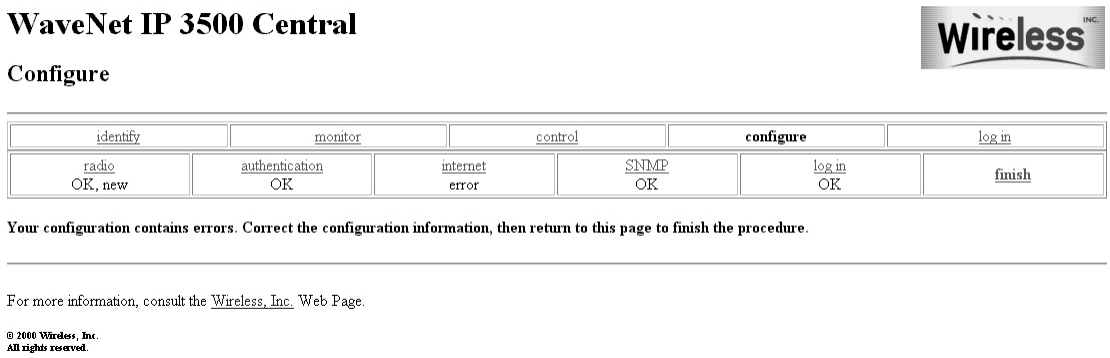


Figure 3-4. Configure Screen (with errors)

12. After you achieve an error free configuration, click **submit configuration** to make the new configuration active.

No configuration changes will take effect until this action is performed. Pending changes that have been configured but not submitted are saved so that they can be submitted at a later time.

13. Reconfigure the PC using an IP address and subnet mask consistent with the router's new Internet page (see the **Configure Internet** page).

14. Confirm that security configurations on the **Log In** and **Configure SNMP** pages 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, and maintenance. The Remote router radio interface MAC Address is needed if the Central router authentication feature is used.

Note: You must select a user name and password during initial configuration. once you change the unit's IP address, login will be invoked, and a user name and password will be required.

Configure Subpages

This section contains details about the parameters in each of the **Configure** subpages.

Configure Radio Subpage

Radio configuration is required in order to deploy the router. Click **radio** on the **Configure** screen to display the **Configure Radio** subpage, as shown in Figure 3-5.

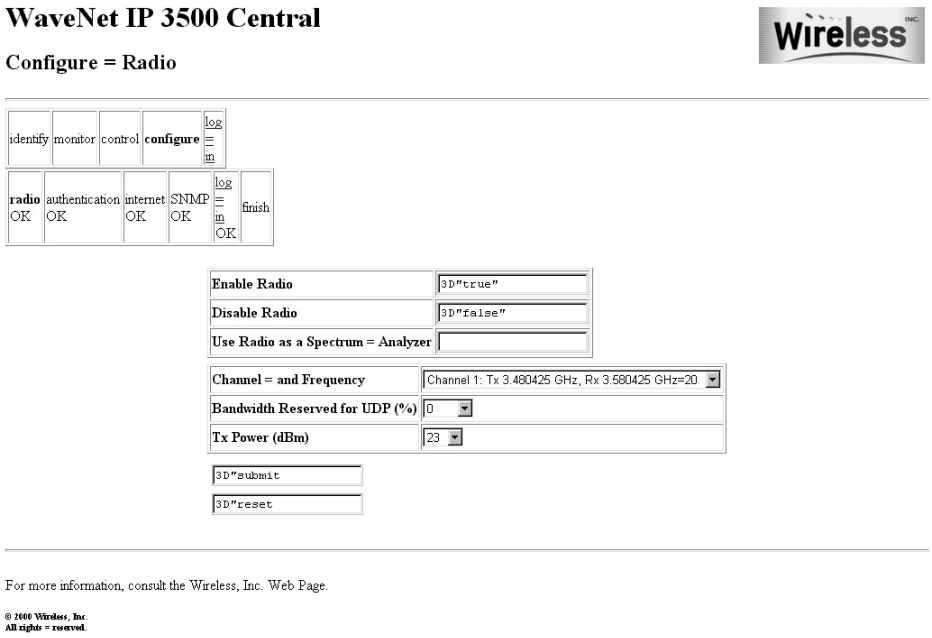


Figure 3-5. Configure Radio Subpage

Radio Enable/Disable

1. Click **Enable Radio** to establish a connection or pass data over the radio interface.
2. Click **Disable Radio** to prevent radio link transmissions and receptions.

CAUTION: If you disable a radio, a local Ethernet connection must be used to re-enable it, which requires a visit to the radio site.

The rest of the configuration and installation instructions assume that the radio is enabled.

Using the Radio as a Spectrum Analyzer

This allows you to display RSSI levels in dBm for each of the 8 channels available to the unit. The RSSI levels will be presented as peak-hold values, where the highest level on each channel will be retained and displayed at each sample period.

Channel and Frequency Selection

Each Central router transmits in the 3.50 to 3.60 GHz band and receives in the 3.40 to 3.50 GHz band. Eight consecutive channels are used, each with a bandwidth of 1.75 MHz. When setting up a central site, it is important to set up adjacent sectors with channel separation between sectors, and to set the channel for each Remote to match the channel of the Central with which it communicates.

Use the **Channel and Frequency** drop-down list in the **Configure Radio** subpage to select the appropriate channel and frequency for each Central and Remote radio for each sector, based on the explanations and descriptions that follow.

There are three basic ways to co-locate routers at a central site and assign channels:

1. Four co-located routers in a cellular deployment

Four Central units can be co-located, provided 90° antennas are employed. The adjoining sectors can use the same polarization and the RF channel of each Central should be two channels away from the adjoining sector.

Figure 3-6 shows how the sectors and channel numbers are set up for a single hub with four co-located Central units.

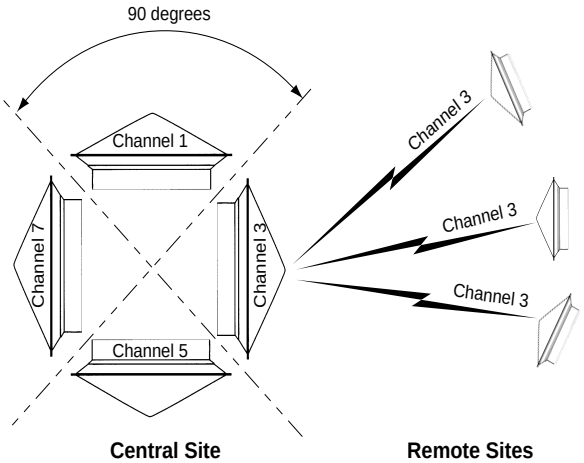


Figure 3-6. Channel Configuration for Central Hub and Remote Radios

In a densely populated city, a service provider will most likely want many central hub sites to properly cover the whole city. The diagram below shows how different channels and polarizations are used to properly cellularize a network.

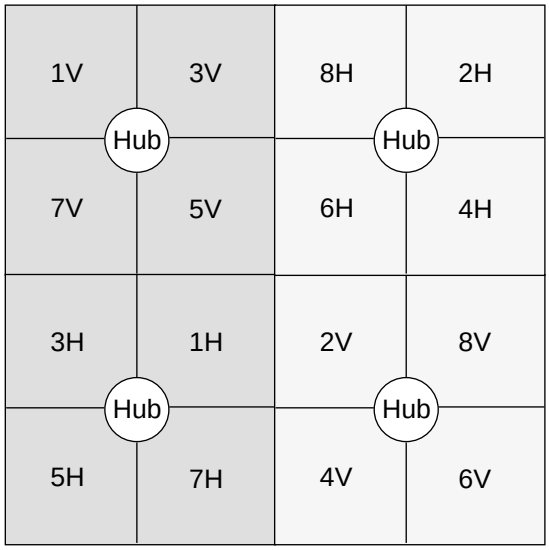


Figure 3-7. Cellular Topology With Channel and Polarization Assignments

In a rural or sparsely populated area, a non-cellular deployment might be best. In this configuration, only one cell tower is installed, with up to eight Central routers for metropolitan coverage.

2. Six co-located routers in a spot deployment model

Six Central units can be co-located, provided 60° antennas are employed. The adjoining sectors can use the same polarization, and the RF channel of each Central should be three channels away from the adjoining sector.

3. Eight co-located routers in a spot deployment model

Eight Central units can be co-located, provided 60° antennas are employed, with the antennas are deployed as two rings of four antennas each, with some amount of vertical separation between the rings. The antennas contained within each ring should be offset by 45°, such that an antenna in the lower ring does not have an antenna from the upper ring directly above. The adjoining sectors within each ring can use the same polarization, and the RF channel of each Central should be three channels away from the adjoining sector.

Bandwidth Reserved for UDP (%)

This is configurable on Central routers only. A Remote router dynamically sets its **Bandwidth Reserved for UDP (%)** parameter to match that of the of the Central unit with which it associates.

The **Bandwidth Reserved for UDP (%)** parameter is used to prioritize UDP protocol packets vs. non-UDP packets over the radio interface. Because 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 **0**, then there is no special handling for UDP packets. If this parameter is set to a value other than **0**, then two priority channels are created, one for UDP packets and one for non-UDP packets. Data from each channel is given priority, until the amount of data from that channel reaches the specified percentage of total radio channel capacity (see Table 3-2).

Table 3-2. Bandwidth Reservation

Parameter Value (%)	Bandwidth Reserved UDP	Bandwidth Reserved for Non-UDP
0	No Priority	No Priority
50	50%	50%
62.5	62.5%	37.5%
75	75%	25%
87.5	87.5%	12.5%

The 87.5% 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, the other priority channel is allowed to use the total radio bandwidth.

Tx (Transmit) Power

Select the desired value from the pull-down list. The range of values is +15 to +23 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) = TX Power (dBm) + Tx Antenna Gain (dBi) – Tx Antenna Cable Loss (dB)

For example, to meet the ETSI 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.

Configure Radio Authentication Subpage

Click **authentication** on the **Configure** page. The **Configure Radio Authentication** subpage appears, as shown in Figure 3-8.

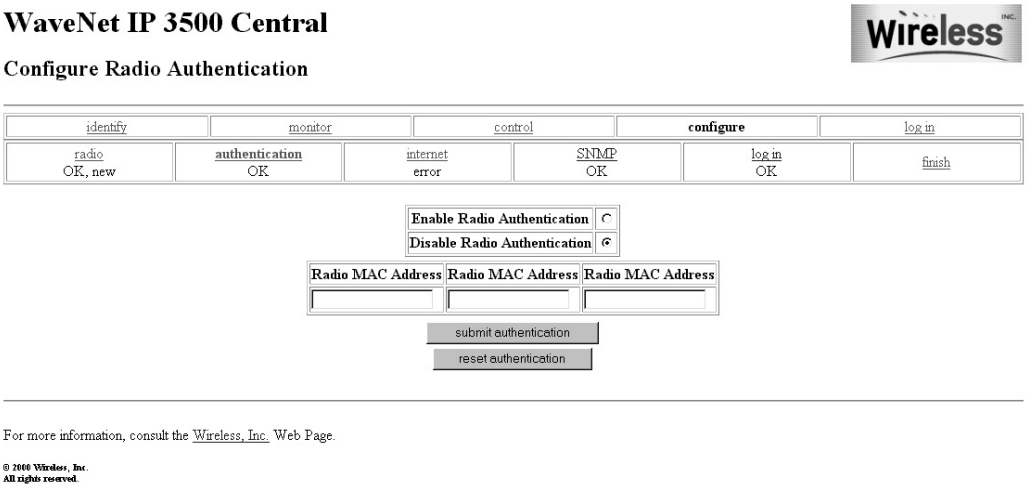


Figure 3-8. Configure Radio Authentication

Performing authentication configuration is not 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. When **Enable Radio Authentication** is selected on a Central router, only authorized Remote routers can 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 of the Remote router's authentication tables. When using redundant Centrals, make sure that the MAC addresses of each of the redundant Centrals appears in each Remote's authentication table.

Internet Subpage

Click **internet** on the **Configure** page. The **Configure Internet** subpage appears, as shown in Figure 3-9.

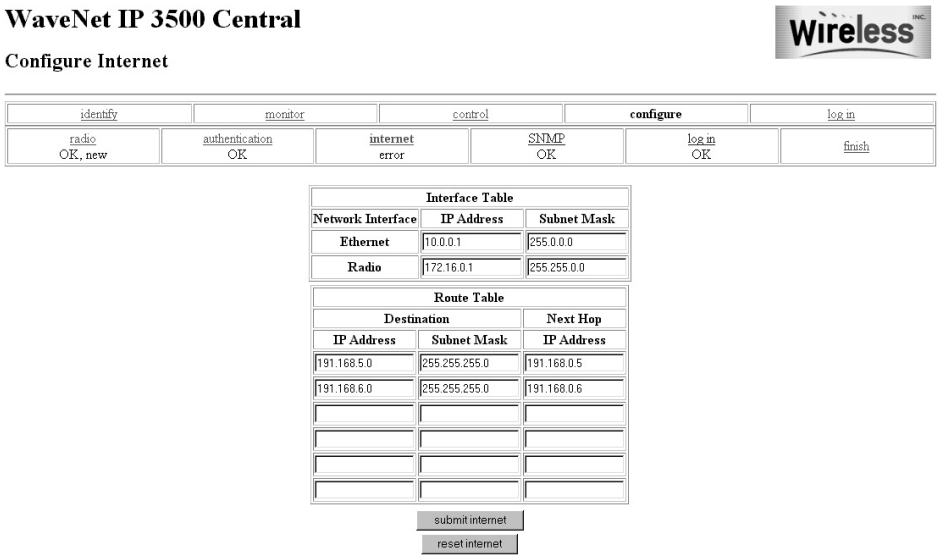


Figure 3-9. Configure Internet Subpage

Performing Internet configuration is required in order to deploy the router. The default address established when the router board powers up should not be used beyond the initial router configuration process.

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 to which the router will route packets based on 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)

SNMP Subpage

Click **SNMP** on the **Configure** page. The **Configure Internet** subpage appears, as shown in Figure 3-10.

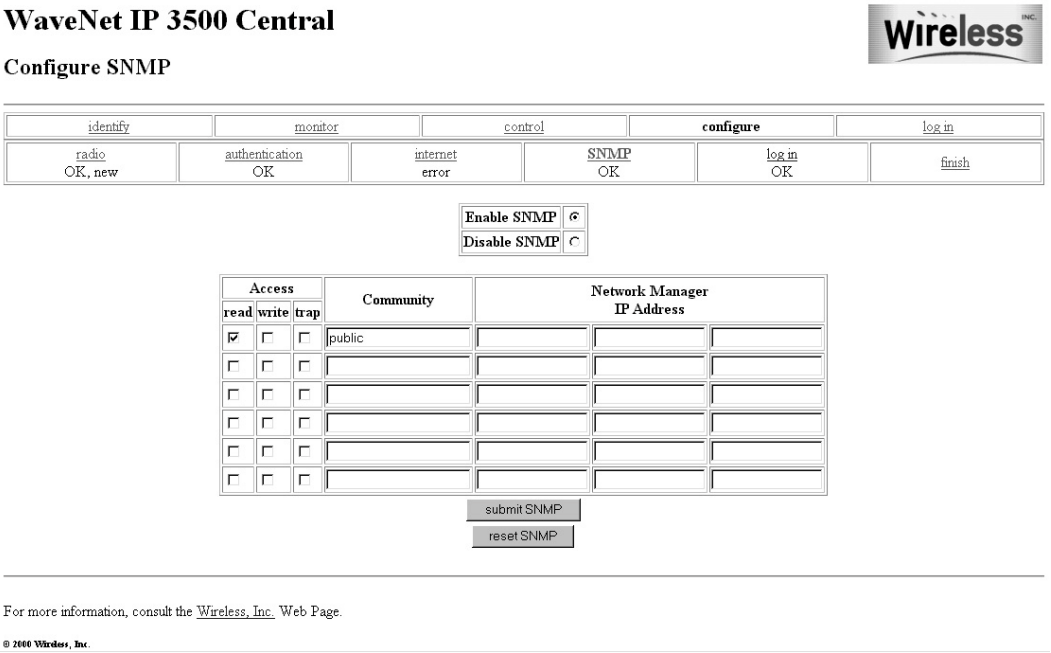


Figure 3-10. Configure SNMP Subpage

Performing SNMP configuration is optional. If **Enable SNMP** is selected, 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.

Note: Units are shipped from the factory with a community named "public," which has Read access. This allows users to view all configuration information through SNMP. Read access for the community named "public" can be removed, thus preventing unauthorized personnel from viewing SNMP variables (router/radio configuration information, etc.).

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), through 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, and give that name to a particular user, or to a group of users.

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 are only accepted if the IP source address from the SNMP packet matches one of the addresses listed.

If a **Trap** box is selected, the router sends 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, **Disable SNMP** should be selected, the **Read** access box should be de-selected, or the Community name should be changed to another value.

Log In Subpage

Click **log in** on the **Configure** page. The **Configure Log In** subpage appears, as shown in Figure 3-11.

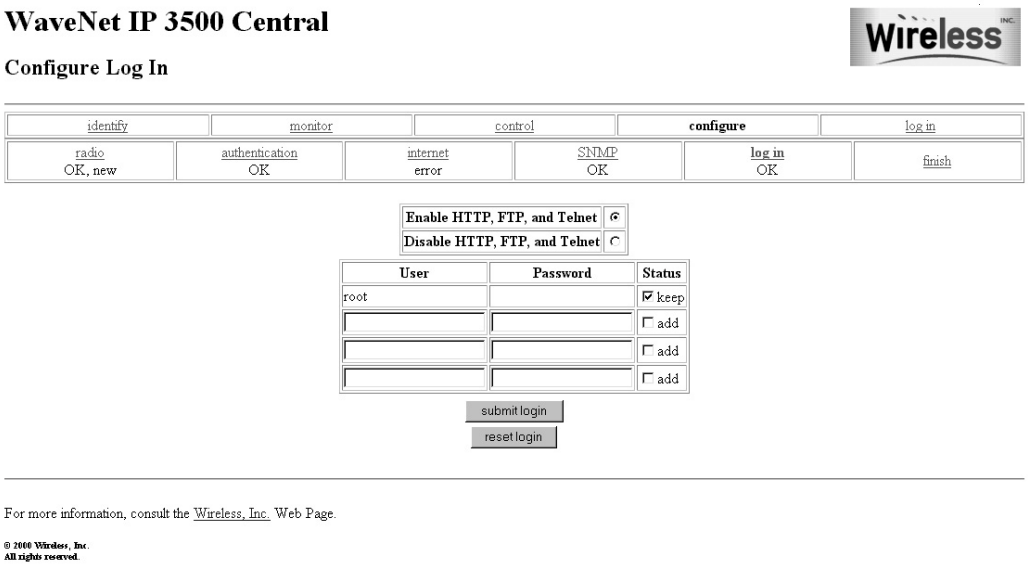


Figure 3-11. Configure Log In Subpage

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

Enable/Disable FTP, HTTP, and Telnet

Network access to the Web browser management pages (HTTP), FTP, and Telnet can be enabled or disabled. If **Enable HTTP, FTP, and Telnet** is selected, user and password log in values are 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 eight characters), and select the **add** checkbox. The user is 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 is allowed through the Web browser interface if the user supplies a valid SNMP community name at log in time. Access to SNMP variables is 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 only display those fields that can accessed given the security restrictions based on the community name.

Using FTP, a user can read and write any file on the router. Misuse can cause router operations to cease, so FTP should used with care. FTP 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.

Telnet access is protected by the same passwords configured for FTP and HTTP access to the unit. The maintenance console can be accessed by opening a Telnet session to the unit. Misuse of the console interface could damage the integrity of the system software and/or configuration.

Note: This interface should not be used except under the direction of Wireless, Inc. support staff.

If **Disable HTTP, FTP, and Telnet** is selected, then access to the unit through the Web browser (HTTP), FTP, and Telnet is denied, regardless of user and password log in values entered at log in time. To regain access requires that the router be reset. The router must also be reset to return to the unit to factory defaults. See "Verifying Internetwork Connectivity" on page 4-8 for instructions on resetting the router.

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 symbols, plus the following symbols:
$-_.+!.*

4 Installation

This chapter explains how do perform and verify the physical installation of the router. It consists of the following sections:

- "Install the Router and Antenna"
- "Configuring Other Customer Equipment"
- "Verifying Internetwork Connectivity"

This chapter 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 ETSI EN 300 019-2-4 V2.1.2 (1999-09) EIRP limits or other applicable regulatory requirements.

Install the Router and Antenna

To install the router and antenna, you must perform the following tasks:

- Prepare the cables
- Secure the router to the mast
- Mount the Antenna
- Connect and secure the outdoor cables
- Connect the indoor cables
- Aim the antenna

Preparing the Cables

The following cables and wires are needed for installation:

- Antenna cable
- Data/Power cable
- Grounding wire

Follow these steps to prepare the cables for mounting:

1. The power and Ethernet connectors should be disconnected from the router and from power and data sources.
2. Verify that each cable is terminated with the proper connector.
3. Attach the grounding lead to the enclosure grounding lug, and coil the grounding wire.

   The grounding lug location is shown in Figure 4-1.

Figure 4-1. Grounding Lug Location

Securing the Router to the Mast

To secure the router to the mast, you must first attach the outdoor pole mount adapter bracket to the mast, then secure the router to the mounting bracket.

Follow these steps to secure the router to the mast:

1. Install the outdoor pole mount adapter bracket to the mast using the supplied metal hose type clamps.
2. Align the four mounting studs on the router with the bracket holes and move the router against the bracket so that the studs protrude through to the back side of the bracket.
3. Push down the latches on the bracket so that they secure the studs and hold the router firmly in place.

Mounting the Antenna

Follow these steps to mount the central or remote antenna:

WARNING! To avoid excessive exposure to RF energy, WaveNet Access 3500 antennas should be installed and serviced with the primary power disconnected from the WaveNet Access 3500. When power is applied to the unit, the installer must keep at least 12 inches (30 cm.) away from the feed point of the antenna to comply with RF exposure limits. The antennas must be mounted such that the general population will not come within 12 inches of the feed point. This is normally accomplished by installing the unit at an elevated altitude on a roof-top or mast.

---

1. Attach the antenna cable to the antenna connector prior to mounting the antenna.
2. Tighten the connector firmly by hand, or by using special slip-jaw pliers made for this purpose.
3. Protect the exposed cable connector to ensure that the connection is 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 connector, completely covering it, and then completely wrap the connectors with water-resistant putty tape (such as Scotch brand 33).

4. Pull or hoist the antenna and cable assembly to the installation point.

   For central site directional 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.

5. 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 (see "Aiming Directional Antennas" on page 4-6).

6. Attach the antenna cable to the female N connector on the bottom of the router enclosure.

CAUTION: Be careful not to damage the coaxial cable by bending it too much when connecting it between the router and the antenna. Weatherproof the connection to the router.

Connecting and Securing the Outdoor Cables

Follow these steps to connect and secure the outdoor cabling:

1. Attach the 8-pin circular MIL connector on the Ethernet cable to the router Ethernet connector.

2. Attach the 4-pin circular MIL connector on the power cable to the router power connector.

3. Attach the ground wire to the grounding lug on the router

4. Secure the data/power cable and grounding wire to the mast, mount, or tower as close to the router as possible so there is minimal strain on the cable.

   Tie-wraps or cable ties can be used. The cable connectors should not be used to support the weight of the cable.

5. Continue down the mast, mount, or tower, securing the data/power cable and grounding wire 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.

6. Attach the grounding wire to a properly designed grounding system (see "Lightning Protection and Grounding System" on page 2-17, and Appendix C, "Grounding Practices and Lightning Protection Information."

7. Create a drip loop in the cable, and then run the data/power cable through the wall of the building using a wall or roof feed-through.

   Wall and roof feed-throughs have one or more openings and a boot, clamp, and galvanized plate to secure the cable to the wall.

8. Attach lightning protection equipment (highly recommended for lightning-prone areas) at the entry point to the building as described in "Lightning Protection and Grounding System" on page 2-17.

Connecting the Indoor Cables

Follow these steps to connect the indoor cables:

1. 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; otherwise connect the conductors to the power source.

2. Terminate the data cable at the appropriate punchdown block, Ethernet hub, or PC Network Interface card.

   See "Terminate The Data/Power Cable" on page 3-1 for further details.

3. After the router boots up, attach the Palm PDA device (with Palm OS 2.0 or above) to the 9-pin maintenance connector on the router to verify that the router and radio self-test indicators are correct.

Aiming Directional Antennas

Now that the router has booted up and is operational, you may proceed to aim the antenna.

WARNING! When aligning directional antennas, always align and adjust them from the rear to avoid RF exposure from the front of the antenna. The installer must keep at least 12 inches (30 cm.) away from the front of the feed point of the antenna to comply with RF exposure limits.

A Central radio continuously transmits, so you always have a signal from a Central with which to align a Remote's directional antenna. A Remote radio only transmits when it has data to send.

When it is necessary to use a directional antenna on a Central radio (such as a point-to-point link configuration), there are two methods that can be used to align the Central's antenna:

- Monitor the RSSI voltage[1] on the Remote end while the antenna on the Central is aligned.
- Monitor the RSSI voltage on the Central while the central antenna is aligned.

The latter method requires the Remote to transmit on each dwell. To accomplish this, you can use 15,000 byte pings (with zero millisecond wait) from the Central to the Remote to cause the Remote to transmit. Once the Remote is transmitting, you can align the antenna. This method is valid if only one Remote is transmitting to the Central during alignment.

The following antenna alignment procedure can be used on Remotes and Centrals:

1. To check the RSSI level, attach the positive lead of a digital volt meter (DVM) to the center conductor of the BNC connector on the enclosure, and the negative lead to the outer ring of the BNC connector (ground).

   If the Remote router is able to establish a radio connection with the Central router, 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 router 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.

[1] The RSSI voltage is available at the BNC connector on the router and is also available at the Monitor RSSI Subpage (see "Monitor RSSI Subpage" on page 5-6)

2. Vary the directional antenna aim 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, each antenna may have to be adjusted (alternately) a number of times to achieve optimal signal strength. The RSSI level changes in proportion to a change in the receive signal level. Each time the antenna is moved, it takes up to one second for the DVM to indicate the new signal strength. Table 4-1 shows approximate values for the received signal strength based on the RSSI voltage value.

Table 4-1. Received Signal Strengths

Receive Level (dBm)	-90	-85	-80	-75	-70	-65	-60	-55	-50
Central RSSI (volts)	0.593	0.695	0.800	0.905	1.011	1.117	1.221	1.329	1.432
Remote RSSI (volts)	0.585	0.685	0.788	0.889	0.986	1.088	1.190	1.292	1.397

3. After a path with a strong signal is established, tighten the antenna mounting hardware and disconnect the DVM.

Configuring Other Customer Equipment

Workstations and Other End-Nodes

If the router is attached directly to the end-station network (there is no intervening router), 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 Access 3500 Ethernet interface as the default gateway address at the PC or another router
- Add the address to the table of available routers at the PC or another router, or
- Enter the address into the route table at the PC or another router as the next hop for one or more specified remote networks

Routers

In some installations, the router is connected to the end stations through 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 Access 3500 network and individual routers. The routers generally support the applicable objects from MIB-II.

WaveNet Access 3500 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/wn3500.mib". It can be FTP'd from the router and loaded into the NMS 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 Access 3500 enterprise MIB can be found in Appendix E, "WaveNet Access 3500 MIB".

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.

Follow these steps to verify the connectivity:

1. 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

2. If the configuration is correct, verify the physical connection to the router.

3. If the physical connection is correct, and communications still cannot be established to the router, it may be necessary to reset the router's internetwork configuration to a known state.

4. To reset the router, remove router power and short pin 7 to pin 9 on the maintenance connector prior to re-applying power, then hold the short for 30 seconds after power is applied. After the short is removed, the router is reset

and the router IP address is set to a known value (10.0.0.1). See Figure 4-2 for the maintenance connector pin locations.

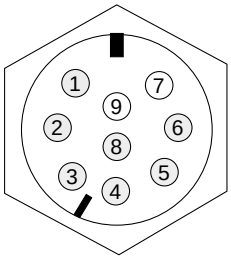


Figure 4-2. Maintenance Connector Pinout

Remote Sites

Follow these steps to verify connectivity:

1. From a remote site end-station, attempt to *ping* to the IP address of a device located at another site.
2. If a *ping* response is received, internetwork connectivity is confirmed.
3. If a *ping* response is not received, 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.
4. If this fails, try a *traceroute* to see how far the packet gets.

   Check for misconfigured internetwork parameters including route table entries.
5. If this is not effective, configure a dedicated PC as a node on the network shared by the Ethernet interface of the WaveNet Access 3500 router. Be sure to configure the following PC network parameters:
   - IP address
   - Subnet mask
   - Use the IP address of Remote router's Ethernet interface as the default gateway
6. Connect the router's Ethernet interface to an isolated network containing just the PC using a separate hub or a crossover modular jack assembly.
7. Issue *ping*s in the order shown in Table 4-2 to determine the source of the connectivity problem.

Table 4-2. Ping Order to Determine Connectivity Problems

Action	Upon Failure, Verify the Following
ping the router's Ethernet interface IP address, subnet mask, or default gateway on PC	1. IP address or subnet mask of router's Ethernet interface (on router) 2. Physical Ethernet link (hub and/or cable) to Remote router
ping the Remote router's radio interface	1. IP address or subnet mask of router's radio interface on router 1. Radio interface is *Enabled*
ping the central site WaveNet Access 3500 router's radio interface	1. IP address or subnet mask of Central router's radio interface 2. Physical radio link
ping the central site WaveNet Access 3500 router's Ethernet interface	3. IP address or subnet mask of Central router's Ethernet interface

8. If there is a failure, consider the possible problem sources listed for each step.

9. If communications cannot be established to the router, it may be necessary to reset the router's internetwork configuration to a known state.

10. To reset the router, remove router power and short pin 7 to pin 9 on the maintenance connector prior to re-applying power, then hold the short for 30 seconds after power is applied. After the short is removed, the router is reset and the router IP address is set to a known value (10.0.0.1). See Figure 4-2 for the maintenance connector pin locations.

11. If all of these steps are successful, verify the route tables of the WaveNet Access 3500 Central or Remote.

    If the route tables are correct, then the problem is likely outside of the WaveNet Access 3500 network.

5 Network Operation

This chapter explains how to modify the site configuration and monitor the network performance. It contains the following sections:

Control Operations

Click **control** on the router page to display the control management page. The **Control** page appears, as shown in Figure 5-1.

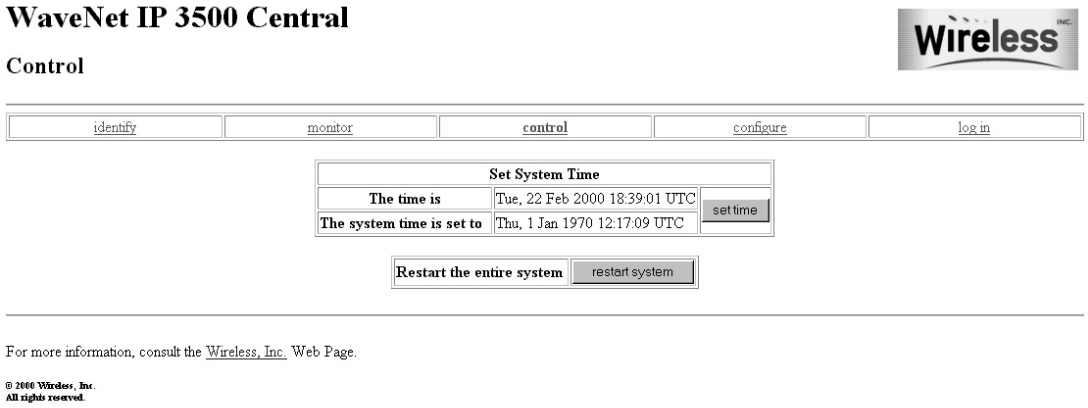


Figure 5-1. Control Page

Use the **set time** button to set the system time to the current time of the computer on which the Web browser is running. The system time is expressed relative to Greenwich Mean Time (GMT).

Use the **restart system** button to reset the WaveNet Access 3500 unit.

Note: Restarting the system takes the router and radio offline 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 *pinging* 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 database.

Removing a Remote Router from an Existing Network

Follow these steps to remove a router 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 logins are enabled, 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.

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 database.

Follow these steps to remove a router if the authentication feature is *not* being used at the Central unit:

1. Log in to the Remote router and open a Web browser.

2. Click **radio** on the **Configure** screen to display the **Configure Radio** subpage.

3. Click **Disable Radio** to prevent radio link transmissions and receptions.

CAUTION: If you disable a radio, a local Ethernet connection must be used to re-enable it, which requires a visit to the radio site.

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 (frequency channel).
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 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 (for example, 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, so configuration files should only be stored or 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.

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 on the router page, which brings up the **Monitor Radio Statistics** page, shown in Figure 5-2.

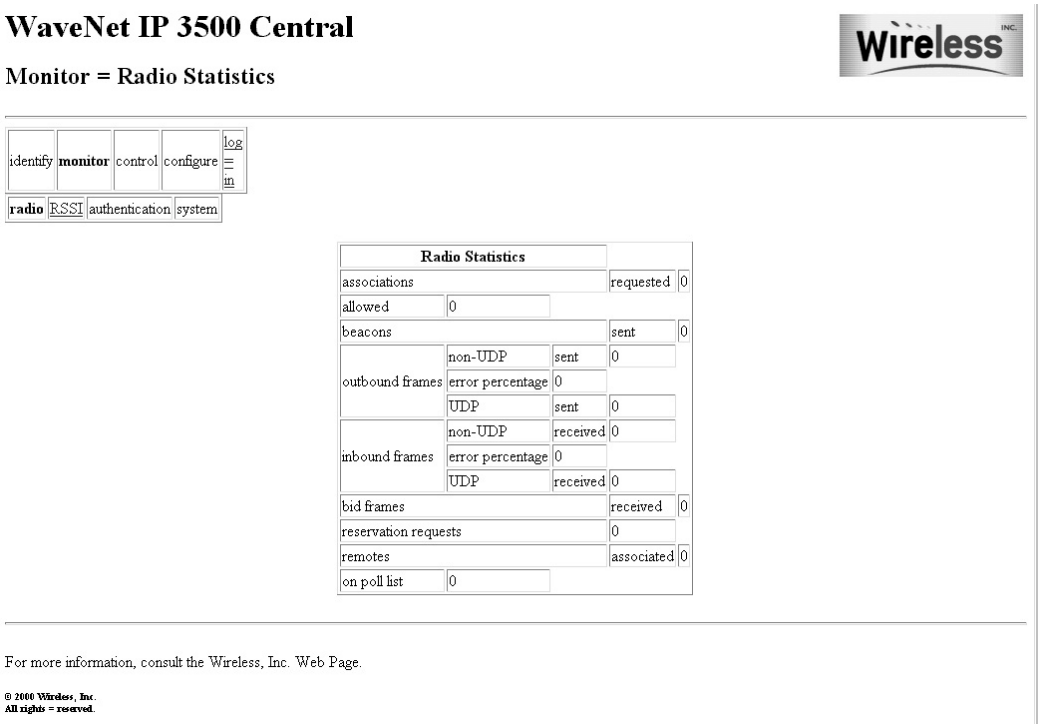


Figure 5-2. Monitor Radio Statistics Page

Statistics can be repeatedly sampled using the reload/refresh feature included with the Web browser. Monitor RSSI updates automatically approximately every 15 seconds. The following subpages can be selected:

- Monitor Radio Statistics
- Monitor RSSI: the router displays RSSI levels in dBm as a user-interface web page for each of the 8 channels available to the unit. The RSSI levels are presented as peak-hold values, where the highest level on each channel is be retained and displayed at each sample period. A button on the page can be selected to clear the peak-hold values and start with a fresh display.
- Authentication
- System statistics

Monitor Radio Statistics Subpage

Figure 5-2 shows the **Monitor Radio Statistics** page. Performance monitoring and troubleshooting of the radio link can be accomplished using radio statistics. Refer to Appendix D, "Radio Statistics" for definitions of each Radio Statistic.

Monitor RSSI Subpage

To display the **Monitor RSSI** subpage, click **RSSI** on the **Monitor Radio Statistics** main page. The page is shown in Figure 5-3.

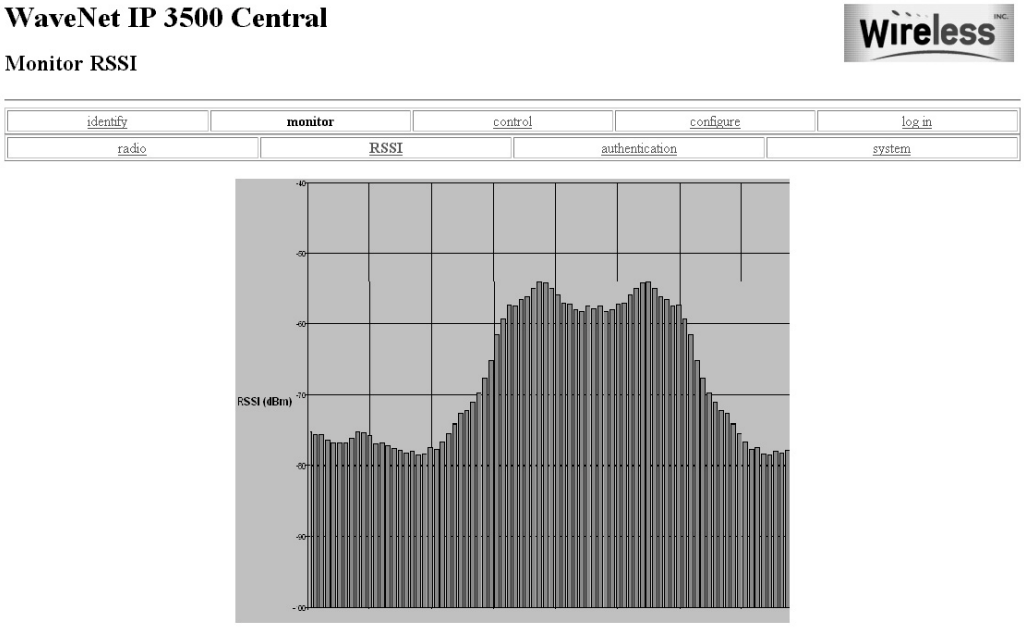


Figure 5-3. Monitor RSSI Subpage

The information displayed on the **Monitor RSSI** page can be used in the following ways:

- Verifying that actual receive levels agree with calculated numbers
- Determining if a particular site is suitable for installing a Central unit

- After installation, for periodic monitoring of RF links to verify that fade margins are maintained, and to determine if interference not originally in the vicinity has surfaced.

The **Monitor RSSI** page only measures signals on channels that are valid for the particular frequency band in which the WaveNet Access 3500 is configured to operate.

On a Remote unit, the Monitor RSSI page provides valid measurements only when the Remote is associated with a Central unit. At a central site, the Monitor RSSI page measures the ambient RF level on each channel, and provided no Remotes are actively transmitting data, only the level of potential interferers will be displayed.

A properly designed link with 20 dB or greater fade margin should indicate receive levels in the area of -73 dBm at remote sites. The accuracy of Monitor RSSI is approximately ±5 dB over the range of -90 dBm to -65 dBm.

Monitor Radio Authentication Subpage

To display the **Monitor Radio Authentication** subpage, click **authentication** on the **Monitor Radio Statistics** main page. The page is shown in Figure 5-4.

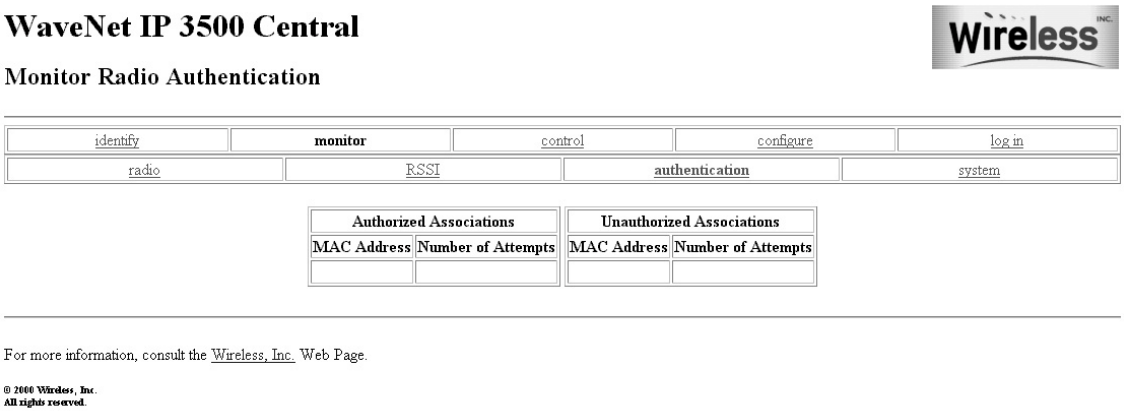


Figure 5-4. Monitor Radio Authentication Subpage

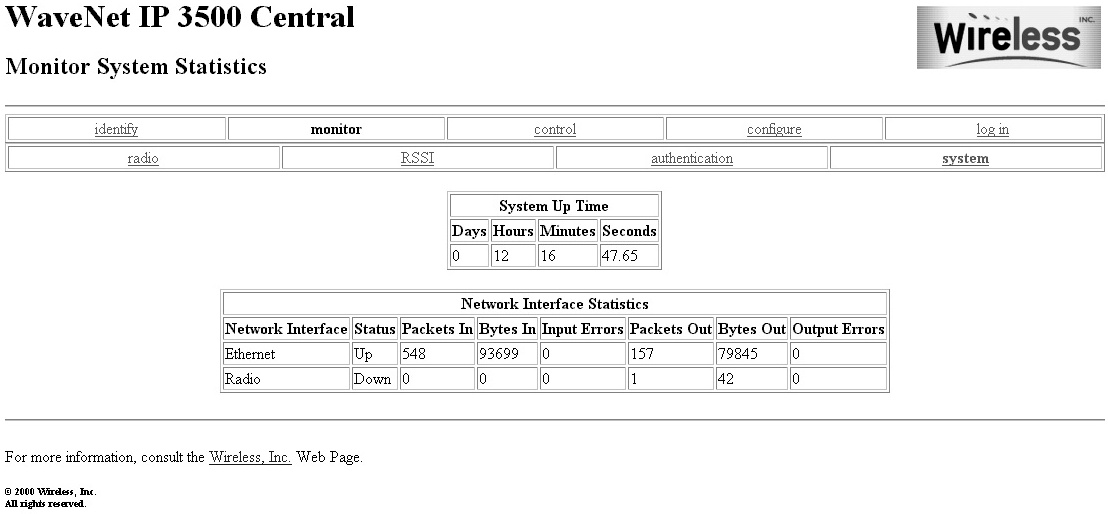
The **Monitor Radio Authentication** page allows you to see the number of association attempts made by a particular Remote unit, or in the case of a Central unit, how many association requests have been made by particular Remote units.

Authorized associations are recorded when the MAC address of the requesting unit is in the authentication table of the responding unit. Unauthorized associations are recorded when the MAC address of the requesting unit does not match any MAC address in the responding unit's authentication table.

The **Monitor Radio Authentication** screen applies only to the Central units. The Authorized Associations and Unauthorized Associations tables expand automatically as necessary.

Monitor System Statistics Subpage

To display the **Monitor Systems Statistics** subpage, click **system** on the **Monitor Radio Statistics** main page. The page is shown in Figure 5-4.



WaveNet IP 3500 Central

Monitor System Statistics

Wireless INC.

identify	monitor	control	configure	log in
radio	RSSI	authentication	system	

System Up Time			
Days	Hours	Minutes	Seconds
0	12	16	47.65

Network Interface Statistics							
Network Interface	Status	Packets In	Bytes In	Input Errors	Packets Out	Bytes Out	Output Errors
Ethernet	Up	548	93699	0	157	79845	0
Radio	Down	0	0	0	1	42	0

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

Figure 5-5. Monitor System Statistics Subpage

The **Monitor Radio Authentication** page contains two tables: **System Up Time**, and **Network Interface Statistics**.

The **System Up Time** table shows the amount of time in days, hours, minutes, and seconds that the system has been operational.

The **Network Interface Statistics** table shows various statistics for the radio and Ethernet 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 Access 3500 enterprise MIB (see Appendix B), which can be FTP'd from *F:/PUB/wn3500.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 SNMP traps are supported, and can be used to raise alarms on the network management station.

Monitoring Error Messages and Traps

The routers support the SNMP traps from MIB-II in addition to WaveNet Access 3500 enterprise MIB traps. When an error (or informational) message is generated by the router, an SNMP trap is issued (when enabled), and the message is also written to an error log maintained within the router. The router's error log table holds the last 256 error messages, and can be queried through SNMP reads. See Appendix C, "Grounding Practices and Lightning Protection Information" for a detailed list of router-specific messages/traps. See Appendix E, "WaveNet Access 3500 MIB" for the enterprise MIB traps (Group 8) definitions.

The error log is read ten entries at a time. To do an SNMP read of the first (oldest) ten entries, the following SNMP operations would be performed:

1. Set *elLogEntryNumber* to start at the oldest entry 0.
2. Set *elScrollControl* to forward to read log in FORWARD direction – oldest entries first.
3. Get *elTrapTable* retrieves the most recent ten entries – repeat for next ten entries.

Other SNMP operations:

- To read the log in the BACKWARDS direction, set *elScrollControl* to backward.
- To clear the log, set *elScrollControl* to clearLog.
- To set the threshold for the lowest severity of messages to be generated, set *elLevelDisable* to 1 (Normal) through 5 (Critical). This avoids filling the log with informational or non-serious errors.
- To set the current date and time (default after reboot is midnight, January 1, 1990), set the appropriate fields of *elTimeDate*, or use the Control Page on the UI. The timestamps included in error messages are generated relative to this date and time.

Performance Tuning and Load Balancing

By monitoring the radio usage statistics over time, it is possible to tell when the demands of the remote sites are exceeding the capacity of their radio network link. When it is desirable to improve performance levels, this can be accomplished by a combination of:

- Re-balancing the existing remote sites among the central site routers (when more than one Central router is installed at a site), and/or
- Adding additional central sites and re-balancing the Remotes among the sites.

By keeping statistics on each Remote router (to determine its load on the network), as well as each Central router (to determine the overall load on its network), optimal choices can be made. The first approach is often the simplest, since it only require re-aiming central site antennas and/or installing new routers at one (central) site. Re-balancing Remote routers among different sites typically requires re-aiming the Remote routers' directional antennas towards the new central site locations, which can be labor intensive if there are many remote sites.

Different classes of service can be achieved by installing more than one Central router with the same antenna coverage area. A smaller number of "premium" service Remote routers can be assigned to one Central router, while a larger number of "normal" service Remote routers can be assigned to the other Central router.

6 Maintenance

This chapter gives information on maintaining and repairing the WaveNet Access 3500 system. It contains the following sections:

Interpreting Palm PDA Device (with Palm OS 2.0 or above) Indicators

1. The power indicator is solid on when valid power is present; otherwise, it is off.

2. The Router Test indicator is on after both the hardware self-test and the software load have completed.

3. The Radio Test passed indicator is solid on after router self-test passes, radio interface is configured *Enabled*, radio board hardware self-test passes, and radio board software load complete.

4. The Radio Activity indicator blinks on upon reception of packets

5. The Signal Quality indicator is steadily on when a physical radio link is established

6. The Ethernet Transmit/Receive indicator blinks on when packets are physically transmitted or received

7. The Ethernet Link indicator is steadily on when a physical link is established

Maintenance Port

The maintenance port is accessible at the 9-pin circular MIL connector on the router enclosure. This port allows a device such as a Palm PDA device (with Palm OS 2.0 or above) to connect to the 9-pin connector through a special adapter cable. Application software written specifically for the maintenance port can then collect router board status.

This port should not be used except under the specific direction of Wireless, Inc. support staff. This physical interface is not protected against voltage surges, therefore no cables should be connected to it while the unit is installed outdoors. Misuse of the console interface could damage the integrity of the system software and/or configuration.

The maintenance port functions can also be accessed by opening a Telnet session to the unit. Telnet access is protected by the same passwords configured for FTP and HTTP access to the unit. Again, this interface should not be used except under the direction of Wireless, Inc. support staff.

Replacing Failed Hardware

If a router fails while installed, then the entire unit (including the enclosure) must be swapped. This can only be done at an authorized repair depot or at the factory.

Loading New Versions Of Software

New versions of software can be loaded onto the system by using FTP. Specific files and instructions will be included with software updates.

Before Seeking Further Assistance

Use the Palm PDA device (with Palm OS 2.0 or above) to verify the following:

1. Verify that power is being supplied to the power cable.
2. Verify the integrity of the power cable.
3. Did the unit pass self-test?
4. Verify the Ethernet interface.
   - Does the router respond to a *ping*?
5. If a network log in is possible, check the monitor pages for data and error statistics that may suggest a source of the problem.
6. Record all hardware and software version and identification numbers. If the router board is functional, these should be obtainable from the Identify Web browser page. Record the serial and model numbers from the label located inside the enclosure.

Where To Get Further Assistance

Your primary source of assistance is the support staff of the organization from which you purchased this product. Wireless, Inc.' support staff should only be contacted directly if you purchased the product directly from Wireless, Inc., or if you are unable to obtain sufficient assistance from your primary support contact.

Wireless, Inc. technical support staff can be reached at:

Wireless, Inc.
Customer Service

E-mail: *customerservice@wire-less-inc.com*

Product and company information can be obtained from our web site:
www.wire-less-inc.com

Requests for product or sales information should be addressed to:

Wireless, Inc.
Sales
5452 Betsy Ross Drive
Santa Clara, California 95054-1101
Phone: (408) 727-8383
FAX: (408) 727-0990
E-mail: *sales@wire-less-inc.com*

Return Procedure

Products may only be returned to Wireless, Inc. after receiving a Return Maintenance Authorization (RMA) number from your primary support contact or Wireless, Inc. support staff. Returned products should be packed in their original packing cartons to protect them from damage.

7 Specifications

This chapter contains the electrical, mechanical, and environmental specifications of the WaveNet Access 3500. It contains the following sections:

Electrical Specifications

External Interfaces

The following sections describe the connectors on the router.

Power Connector

The Power connector contains four pins and is shown in Figure 7-1.

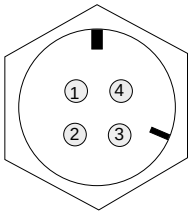


Figure 7-1. Power Connector Pinout

The pin assignments and descriptions are shown inTable 7-1.

Table 7-1. Power Connector Pin Descriptions

Pin	Description
1	AC Input
2	AC Input
3	Open
4	Ground

Data Connector

The Data connector contains eight pins and is shown in Figure 7-2.

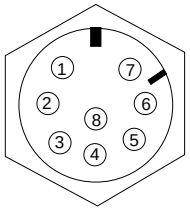


Figure 7-2. Data Connector Pinout

The pin assignments and descriptions are shown in Table 7-2.

Table 7-2. Data Connector Pin Descriptions

Pin	Signal Name	Description
1	TX+	Twisted-Pair Transmit Positive
2	TX-	Twisted-Pair Transmit Negative
3	RX+	Twisted-Pair Receive Positive
4	—	Not used (terminated)
5	—	Not used (terminated)
6	RX-	Twisted-Pair Receive Negative
7	—	Not used (terminated)
8	—	Not used (terminated)

Maintenance Connector

The Maintenance connector contains 9 pins and is shown in Figure 7-3.

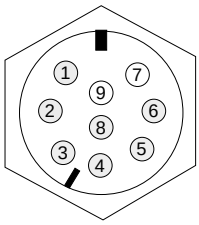


Figure 7-3. Maintenance Connector Pinout

The pin assignments and descriptions are shown in Table 7-3.

Table 7-3. Maintenance Connector Pin Descriptions

Pin	Description	Direction
1	RXD Terminal Receive Data	Output
2	TXD Terminal Transmit Data	Input
3	Router Self Test LED (active-LOW)	Output
4	Radio Self Test LED (active-LOW)	Output
5	Radio quality LED (active-LOW)	Output
6	Ethernet Link LED (active-LOW)	Output
7	Factory Default (active-LOW)	Input
8	Reset (active-LOW)	Input
9	Ground	—

Radio

The radio specifications are as show in Table 7-4 through Table 7-6.

Table 7-4. Radio General Specifications

Parameter	Value
Frequency Range	3.40 - 3.50 GHz
Number of channels	8 consecutive channels
RF Channel Bandwidth	1.75 MHz
Channel Increments	1.75 MHz
Radio Operation	Full duplex
Antenna Port Impedance	50 Ω nominal
Antenna Port Return Loss	≥ 15 dB minimum
RSSI Range	-50 dBm to -90 dBm
RSSI Tolerance	±5dB
Ethernet Port Data Rate	10 Mbps
Gross Data Capacity[1]	2300 kbps each direction
Effective Data Capacity[1]	1625 kbps each direction
FTP Throughput[1]	Get = TBD kbps Put = TBD kbps (assuming single FTP session on a single Remote
Packet per Second Throughput	600 pps each direction (1200 pps full duplex - 64 byte packets)

1. No data compression

Table 7-5. Radio Transmitter Specifications

Parameter	Value
Frequency Range	Central transmits in the 3.50 - 3.60 GHz band
	Remote transmits in the 3.40 - 3.50 GHz band
Number of Channels	8 consecutive channels
Channel Increments	1.75 MHz
Modulation	4QAM 0.5
Power Output on Central	+23 dBm maximum transmit power at antenna port, with at least 9 dB of manual transmit power control

Table 7-5. Radio Transmitter Specifications

Parameter	Value
Power Output on Remote	+23 dBm maximum transmit power at antenna port with at least 40 dB of Automatic Transmit Power Control (ATPC) dynamic range
Transmit Duty Cycle	100%
Emission Mask	Per ETSI EN 301 021 Type A
Frequency Stability	+/- 2.5 ppm
Spurious and Harmonic Output	≤ -50 dBm in 1MHz B.W. up to 5^{th} harmonic (per CEPT/ERC/Recommendation 74-01 E)

Table 7-6. Radio Receiver Specifications

Parameter	Value
Frequency Range	Central receives in the 3.40-3.50 GHz band Remote receives in the 3.50 - 3.60 GHz band
Number of Channels	8 consecutive channels
Channel Increments	1.75 MHz
Sensitivity	-90 dBm minimum receiver sensitivity at 10^{-6} BER
Maximum RF Input:	-30 dBm without receiver degradation -10 dBm damage level
Frequency Stability	± 2.5 ppm
Receiver Saturation	≥ -30 dBm
1^{st} Image Rejection	≥ 75 dB
Other Spurious Rejection	≥ 50 dB
C/I (1 dB degradation of BER @ 10^{-6})	C/I of -20 dBc co-channel C/I of +15 dBc +/- 1 channel away C/I of +45 dBc +/- 2 channels away

Protocols

The protocols are as follows:

- Network: IP Version 4.0 (with CIDR support), ICMP
- Transport: TCP, UDP
- Application: FTP, Telnet, HTTP, SNMP

Lightning Protection

The Ethernet interface must incorporate lightning protection on all four active lines. The amount of protection should be, at a minimum, consistent with that provided on WaveNet IP 3500. The specifications for the protection devices used on WaveNet IP 3500 are as follows (Semtech LC03-6):

- P_{pk} (Peak Pulse Power) 750 Watts with tp = 8/20µs
- I_{pp} (Peak Pulse Current) 50 Amps with tp = 8/20µs
- $V_{br} \geq 6.8$ Volts
- V_c (Max. Clamping Voltage 15 Volts @ I_{pp}
- C_j (capacitance) ≤ 25 pf on the Ethernet Interface
- Unused lines are connected to ground.

Mechanical Specifications

The router incorporates a water tight/RFI tight one piece gasket to seal the enclosure, and a Gortex patch to allow the enclosure to breathe. The enclosure is be sealed with tamper proof screws to discourage opening once it leaves the factory.

The router may be pole mounted on a 1.75" - 4.5" mast.

The router dimensions are 310mm x 351mm x 73mm (H x W x D) and it weighs 5 kg.

Thermal Specifications

The power dissipated within the enclosure should be minimized to the extent that the temperature inside the enclosure does not exceed the maximum ambient operating temperature of any component housed within the enclosure.

Environmental Specifications

The following sections give the router environmental specifications.

Shock and Vibration

The router complies with ETSI EN 300 019-2-4 V2.1.2 (1999-09) Equipment Engineering (EE); Environmental conditions and environmental test for telecommunications equipment; Part 2-4: Specification of environmental tests; Stationary use at non-weather protected locations.

Shock (Non-Operational)

- 100 m/s² (10.2g), half sine, 11ms.
- 100 bumps in each direction of each axis (600 bumps total).

This test is based on IEC 721-3-1, severity 1M3, as well as IEC 68-2-29 TEST Fc AND GUIDANCE: BUMP.

Shock and Vibration (Packaged)

Meets ISTA Test Procedure 2 & 2A

Sinusoidal Vibration (Non-Operational)

Table 7-7. Vibration Test Parameters

Amplitude	Frequency
3mm (.118 in)	5 Hz to 9 Hz
10m/s² (1.02g)	9 Hz to 200 Hz

The vibration test is based on 10 sweeps per axis (x, y and z) at a rate of 1 octave per minute. Each sweep is 5 Hz to 200 Hz to 5 Hz.

This test specification is based on IEC 721-3-1, severity 1M3, and IEC 68-2-6 TEST Fc AND GUIDANCE: VIBRATION (sinusoidal).

Sinusoidal Vibration (Operational)

Operational is defined as a unit under test being linked with a unit at 15 dB above threshold. The unit under test must not generate transmit errors nor receive errors during duration of test.

The vibration test is based on 10 sweeps per axis (x, y and z) at a rate of 1 octave per minute. Each sweep is 5 Hz to 200 Hz to 5 Hz.

Table 7-8. Vibration Test Parameters

Amplitude	Frequency
1.5mm (.059 in)	5 Hz to 9 Hz
5m/s² (.51g)	9 Hz to 200 Hz

This test specification is based on IEC 721-3-1, severity 1M3, and IEC 68-2-6 TEST Fc AND GUIDANCE: VIBRATION (sinusoidal).

Temperature and Humidity

The router must meet ETSI test specification T 4.1 E: Stationary use at non-weather protected location, extended – climatic tests.

Operational Limits

The router operates over the temperature range of -45 °C to +60 °C.

Non-Operational Limits

The router can be stored over the temperature range of -45°C to + 85°C, 95% humidity (non-condensing).

Altitude

Operational Limits

The router operates to an altitude of 4,500 meters

Non-Operational Limits

The router may be stored at altitudes of 0 - 50,000 ft. (0 - 15,000 m.)

A
Messages and Traps

This appendix contains an abbreviated listing of the common messages and traps that may be generated by the routers and monitored with SNMP. It contains the following sections:

There are other errors that can be emitted by the routers, but they typically occur in conjunction with the ones listed in this appendix, or else indicate internal problems with the router. Recurring critical or major severity errors should be reported to your primary support organization.

Table A-1. Alarm Severity Description

Alarm Severity	Definition
Critical	Critical alarms are used to indicate that a severe, service-affecting condition has occurred and that immediate corrective action is imperative, regardless of the time of day or day of the week.
Major	Major alarms are used for hardware or software conditions that indicate a serious disruption of service or the malfunctioning or failure of important circuits. These troubles require the immediate attention and response of a craftsperson to restore or maintain system capability. The urgency is less than in critical situations because of a lesser immediate or impending effect on service or system performance.
Minor	Minor alarms are used for troubles that do not have a serious effect on service to customers or for troubles in circuits that are not essential to operation.
Warning	A warning indicates an internal WaveNet Access 3500 problem.

Critical Severity Messages

Radio Init has Failed.

The attempt to initialize the radio has failed. The radio interface code makes three attempts to do so before being unable to continue. This message indicates that the unit is unable to function over the RF link. There are severe problems with the radio or its support files, depending on the previous error messages containing supplemental information.

The Radio Selftest has Failed.

The radio responded to a selftest request with a failure indication, or did not respond at all. The radio interface code makes three attempts to reinitialize before being unable to continue.

Major Severity Messages

Note that the radio will attempt to self-heal if there is a transient loss of radio connectivity. This should not be considered a serious condition as long the frequency of such occurrences is low.

The Radio Link is Down

A Remote has not associated with its Central, or a Central has not associated with at least one Remote (displays only once at the Central on first association).

Packet Dropped, Excessive Retransmits

A packet was discarded due to an excessive number of failed attempts to transmit it over the radio interface.

Packet Dropped, Excessive Re-Receives

A packet was discarded due to an excessive number of failed attempts to receive it over the radio interface.

TxAllowed Timeout, Link Down

The radio is reporting a lack of synchronization and proper association with a distant unit. The link is down. Indicates that the far end station is down, or that the local station cannot maintain a viable RF link. Automatic reboot of the radio is imminent

TxReady Timeout, Link Down.

The radio is reporting that its buffers are full for an excessive period of time. The link is down. Automatic reboot of the radio is imminent.

Remote Station not Responding.

A link that was up has been lost.

Remote Station has Been Restored.

A link that was lost has been restored.

Minor Severity Messages

Rcvd Invalid Authorization Address

An attempt was made to associate by a remote station not on the authorization list.

Warnings

Radio Configuration File has Been Lost

The radio configuration file was not found. A default version has been created. Most probably the file was never installed. This is a normal event for new units.

Authorization File has Been Lost

The authorization file was not found. A default version has been created. Most probably the file was never installed. This is a normal event for new units.

Packet Dropped, Buffers Exhausted

A packet was discarded due to high traffic levels and a lack of available buffers.

Normal (Informational) Messages

The radio has been initialized.

The radio sub-assembly has initialized correctly and indicated a successful selftest.

B
List of Antennas Compliant with ETSI Type Certification

Table B-1 lists the characteristics of antennas that can be used with the WaveNet Access 3500 system on Central radios (transmitting at 3.5 to 3.6 GHz and receiving at 3.4 to 3.5 GHz):

Table B-1. Central Site Antenna Characteristics

Gain	Beamwidth	Polarization	Mounting	Adjustability	RF Interface	Cable Length
12 dBi	90°	Vertical	Pole mount	15° downtilt	N-connector (female)	6’ maximum
12 dBi	90°	Horizontal				
16 dBi	60°	Vertical				
16 dBi	60°	Horizontal				

Table B-2 lists the characteristics of external antennas that can be used with the WaveNet Access 3500 system on Remote radios (transmitting at 3.4 to 3.5 GHz and receiving at 3.5 to 3.6 GHz):

Table B-2. Remote Site External Antenna Characteristics

Gain	Dish Dimensions	Mounting	Adjustability	RF Interface	Cable Length
20 dBi	18”	Pole mount	15° downtilt	N-connector (female)	6’ maximum
23 dBi	24”				

The characteristics of the Remote unit integrated antenna are as shown in Table B-3:

Table B-3. Remote Site Integrated Antenna Characteristics

Gain	Beamwidth	Dimensions	Polarization	Mounting
20 dBi	20°	9” x 9”	Vertical	Integrated in Router
20 dBi	20°	9” x 9”	Horizontal	Integrated in Router

The enclosure has two options: one for horizontal polarization, and one for vertical polarization. Antenna polarization can be changed at the Factory or at an authorized service depot.

Additional antennas may be added in the future. Any additional antennas will be tested prior to adding them to the lists in this chapter.

C
Grounding Practices and Lightning Protection Information

This appendix explains how to properly set up the system for grounding and lightning protection. It contains the following sections:

Overview

Good grounding ("earthing") practices, when used in telecommunications, have some direct benefits that can help you maximize the up time of your system as well as ensure the safety of those people working on the system. Among these benefits are:

1. Protection of personnel from electric shock and fire hazards
2. Reduction of radiated and conducted electromagnetic susceptibility

3. Improved system tolerance to discharge of electrostatic energy and lightning interference

4. Minimized service interruptions and service damage

There is no practice or formula that can completely eliminate the above risks, but Wireless, Inc. believes that good grounding and bonding practices can significantly reduce the risk of many of these hazards. We have included a bibliography at the end of this appendix that contains several publications that are readily available and contain detailed information on many aspects of grounding systems and their design, implementation, measurement, and maintenance.

Please note that every telecommunication site is unique, and must be evaluated accordingly. The following information is provided for generic reference and educational purposes only. The grounding plans and practices for a given site should only be established and accomplished by trained professionals, working in accordance with local practices and regulations.

Grounding

Grounding Plan

There should be a grounding plan designed at the outset of site design to provide the best grounding procedures and to minimize ground loop currents. This should be achieved by connecting the outer conductors of the cables through a large section copper strap to a central grounding point and the size of the conductor should be increased as each branch path is added. The final conductor should be connected directly to the grounding system. For a radio site a single copper grounding rod is insufficient because its impedance is likely to be too high.

Grounding of Feeders

All antenna feeders should be bonded to the tower at the upper and lower ends and grounded at the point of entry into the building. Weatherproof grounding kits are available from antenna manufacturers.

Note: Many of the cables used by Wireless, Inc. have braided rather than solid outer conductors; this type of grounding is not appropriate. In these cases we recommend the use of Wireless, Inc. approved lightning arrestors. For information on lightning arrestors, please contact our Customer Service department.

Grounding of Buildings

A ground ring ideally should surround the building and be connected to individual grounds associated with feeder entry, antenna support structure, building lightning conductor, equipment room, main AC supply and other facilities. Each connection should be made by the most direct route in order to minimize interaction between the different grounding functions.

The ground ring should consist of copper cable or tape with electrodes two meters or longer, buried to a depth of 0.6 meters and at a distance from the building not to exceed 1 meter.

Buildings may require lightning rods where they are not within the zone of another protected structure.

Lightning Protection

Radio sites can be particularly prone to lightning strikes by virtue of their normally exposed locations and the presence of relatively tall antenna support structures.

Note: It is not possible to provide and guarantee complete protection from the effects of lightning; however, they can be significantly reduced by careful attention to grounding, protection devices, and the layout of the site itself.

Reference should also be made to various publications, some of which are listed in the Bibliography. Where any site owner or user is in doubt about the protection requirements for any particular location, the appropriate authority should be consulted.

Protection Arrangements

The purpose of any protection arrangement should be to provide a suitable path to ground for the lightning current, to ensure adequate bonding between structures and all metalwork on the site and the common grounding system in order to reduce the side flashing, and to attempt to prevent the entry of flashes or surges into the building.

The resistance to ground should be kept to a minimum and a value of less than 10 ohms is recommended. The most important feature is that the system should ideally be at equal potential across the entire site.

Certain authorities and service providers have their own particular practices which have to be followed where applicable.

Arrangements vary considerably from very simple sites to complicated sites with multiple buildings, antenna support structures, and associated equipment, and may involve integration with existing systems. Such systems may require upgrading.

Lightning Conductors

Down conductors, bonding interconnections, ground rings, and radial tapes should be of uninsulated 000 AWG copper cable or solid copper tape with a minimum cross section of 25 x 3 mm with all connections protected by non reactive paste.

Protected test points should be included if appropriate, and sacrificial ground lugs should be clearly marked and easily accessible for periodic inspection.

Grounding of Antenna Support Structures

A structure generally acts as its own lightning conductor and therefore does not require an additional conductor from the top to the base. A lightning rod may be required to extend the zone of protection to protect equipment mounted on the top of the structure. The lightning rod should extend 2.5 meters above the highest equipment.

Ground mounted support structures should be connected at their base to a ground ring through sacrificial ground lugs. Towers should have a connection from each leg.

A ground ring should consist of copper cable or solid copper tape with ground rods equally spaced at two meter intervals around the base of the structure as close to it as possible, buried approximately 0.6 meters deep where soil conditions allow. An alternative method using radials rather than rings is detailed in “The 'Grounds' for Lightning and EMP Protection”, second edition, published by PolyPhaser Corporation.

The ground ring should be connected to the main building ground by the most direct route, buried as appropriate.

Roof mounted structures should be connected to the main building ground by the most direct route using sacrificial lugs and copper cable or tape as appropriate. Tower guy wires should be directly bonded at their lowest point to a suitable ground electrode or connected to the site ground by the most direct route.

Bibliography

ITU - T K.40
Protection against LEMP in telecommunications centres

ITU - T K.27
Bonding configurations and earthing inside a telecommunication building

ITU - T K.35
Bonding configurations and earthing at remote electronic sites

ITU - T K.39
Risk assessment of damages to telecommunications sites due to lightning discharges

ITU - T Lightning Handbook
The protection of telecommunication lines and equipment against lightning discharges

IEEE Emerald Book
Powering and Grounding

The “Grounds” for Lightning and EMP Protection, second edition
Published by PolyPhaser Corporation

D
Radio Statistics

Table D-1 provides a definition for each radio statistic on a **Central**:

Table D-1. Radio Statistics for Central

Statistic	Description
Associations	
Requested	The number of times one or more Remotes have requested to associate with the Central. A Remote must associate with the Central before the RF link will be allowed to establish.
Allowed	This is the number of times one or more Remotes have successfully associated with the Central
Beacons	Total number of beacons sent by the Central. Beacons contain control information that provide information to Remotes, such as what frequency to hop to next, etc.
Outbound Frames	Total number of outbound (Central to Remote) radio data frames sent by the Central.
Inbound Frames	
Received	Total number of inbound (Remote to Central) radio data frames received by the Central. This number is an aggregate of radio data frames received from all Remotes.
Received without errors	Total number of inbound (Remote to Central) radio data frames received by the Central without errors. This number is an aggregate of radio data frames received from all Remotes without errors.

Table D-1. Radio Statistics for Central

Statistic	Description
Contended Data Frames	
Received	Total number of contended inbound (Remote to Central) radio data frames received by the Central. This number is an aggregate of contended radio data frames received from all Remotes. Contended means that the Remote had to contend with other Remotes to send this amount of radio frames.
Received without errors	Total number of contended inbound (Remote to Central) radio data frames received by the Central without errors. This number is an aggregate of contended radio data frames received from all Remotes without errors.
Bid Frames	
Received	Total number of bid frames received by the Central. This number is an aggregate of bid frames received from all Remotes.
Received without errors	Total number of bid frames received by the Central without errors. This number is an aggregate of bid frames received from all Remotes without errors.
Reservation Requests	Total number of reservation requests received by the Central.
Remotes Associated	Number of Remotes presently associated with the Central.
Remotes on Poll List	Number of Remotes on the Central's poll list.

Table D-2 provides a definition for each radio statistic on a **Remote**:

Table D-2. Radio Statistics for a Remote

Statistic	Description
Associations	
Requested	The number of times the Remote has requested to associate with the Central. The Remote must associate with the Central before the RF link will be allowed to establish.
Allowed	This is the number of times the Remote has successfully associated with the Central.
Beacons	
Received	Number of beacons received by the Remote. Beacons contain control information that provide information to the Remote, such as what frequency to hop to next, etc.
Missed	Number of beacons missed by the Remote. The sum of beacons received plus beacons missed should equal the number sent by the Central in any given period of time.
Outbound Frames	Total number of outbound (Central to Remote) radio data frames received by the Remote.

Table D-2. Radio Statistics for a Remote (Continued)

Statistic	Description
Inbound Frames	
Sent	Total number of inbound frames (Remote to Central) radio data frames sent by the Remote.
Sent without errors	Total number of inbound (Remote to Central) radio data frames acknowledged by the Central as having been received from the Remote without errors.
Contended Data Frames	
Sent by this Remote	Total number of contended inbound (Remote to Central) radio data frames sent by the Remote.
Sent without errors	Total number of contended inbound (Remote to Central) radio data frames sent by the Remote without errors.
Total sent by all Remotes without errors	This number is an aggregate of contended radio data frames sent from all Remotes (to the Central) without errors.
Bid Frames	
Sent by this Remote	Total number of bid frames sent by the Remote.
Sent without errors	Total number of bid frames sent by the Remote without errors.
Total sent by all Remotes without errors	This number is an aggregate of bid frames sent from all Remotes (to the Central) without errors.
Reservation Requests	Total number of reservation requests sent by the Remote.

E
WaveNet Access 3500 MIB

```
WN_3500-MIB DEFINITIONS ::=3D BEGIN

IMPORTS
  enterprises, Counter
    FROM RFC1155-SMI
  OBJECT-TYPE
    FROM RFC-1212;

wireless            OBJECT IDENTIFIER ::=3D { enterprises 792 }
wavenet_3500        OBJECT IDENTIFIER ::=3D { wireless     4 }
wn3500_Identity     OBJECT IDENTIFIER ::=3D { wavenet_3500 1 }
rfConfiguration     OBJECT IDENTIFIER ::=3D { wavenet_3500 2 }
rfStatistics        OBJECT IDENTIFIER ::=3D { wavenet_3500 3 }
rfAuthentication    OBJECT IDENTIFIER ::=3D { wavenet_3500 4 }
rfSiteSurvey        OBJECT IDENTIFIER ::=3D { wavenet_3500 5 }
rfCongestion        OBJECT IDENTIFIER ::=3D { wavenet_3500 6 }
wn3500_ErrorLog     OBJECT IDENTIFIER ::=3D { wavenet_3500 7 }

wavenet_3500-central  OBJECT IDENTIFIER ::=3D { wavenet_3500 101 }
wavenet_3500-remote   OBJECT IDENTIFIER ::=3D { wavenet_3500 102 }


-- wn3500_Identity group

unitModelNumber OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The model number of the unit as a whole."
```

```
  ::=3D { wn3500_Identity 1 }

unitRevisionNumber  OBJECT-TYPE
     SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The revision number of the unit as a whole."
  ::=3D { wn3500_Identity 2 }

unitSerialNumber   OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The serial number of the unit as a whole."
  ::=3D { wn3500_Identity 3 }

rtrModelNumber  OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The model number of the router module."
  ::=3D { wn3500_Identity 4 }

rtrRevisionNumber   OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The revision number of the router module."
  ::=3D { wn3500_Identity 5 }

rtrSerialNumber OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The serial number of the router module."
  ::=3D { wn3500_Identity 6 }

sysVersionNumber OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
    "The software version number of the router module."
  ::=3D { wn3500_Identity 7 }

rfModelNumber   OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The model number of the radio module."
  ::=3D { wn3500_Identity 8 }
```

```
rfRevisionNumber    OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The revision number of the radio module hardware."
  ::=3D { wn3500_Identity 9 }

rfSerialNumber  OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..15))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The serial number of the radio module."
  ::=3D { wn3500_Identity 10 }

rfType      OBJECT-TYPE
  SYNTAX  INTEGER {
        central(1),
        remote(2)
      }
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The radio module type."
  ::=3D { wn3500_Identity 11 }

-- rfConfiguration group

rfTxPower   OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
      "Transmit power at the antenna connector, in dBm.  Read only at the remote."
  ::=3D { rfConfiguration 1 }

rfTxControl      OBJECT-TYPE
  SYNTAX  INTEGER {
       localLinkUp(1),
       localLinkDown(2),
       scanMode(3),
       remoteMaxTxpower(4)
       }
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
       "localLinkUp/localLinkDown enables/disables the radio transmitter at the local
       unit. ScanMode at a remote prevents link up with a central while scanning all
       channels for RSSI level.  RemoteMaxTxpower, when set at the central, acts to
       install a maximum transmit power level on the remote identified by the
       rfRemoteID object, in dBm.  Read only at the remote."
  ::=3D { rfConfiguration 2 }

rfChannelFrequencies OBJECT-TYPE
  SYNTAX RfChannelFrequencies
```

```
  ACCESS not-accessible
  STATUS mandatory
  DESCRIPTION
       "The transmit frequency of operation of the 8 selectable channels, in kHz.
       The receive frequency is 100 MHz lower at the central, 100 MHz higher at the
       remote."
  ::=3D { rfConfiguration 3 }

RfChannelFrequencies ::=3D
  SEQUENCE {
    rfChannel1
      INTEGER,
    rfChannel2
      INTEGER,
    rfChannel3
      INTEGER,
    rfChannel4
      INTEGER,
    rfChannel5
      INTEGER,
    rfChannel6
      INTEGER,
    rfChannel7
      INTEGER,
    rfChannel8
      INTEGER
  }

rfChannel1 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The transmit frequency of channel 1."
  ::=3D { rfChannelFrequencies 1 }

rfChannel2 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The transmit frequency of channel 2."
  ::=3D { rfChannelFrequencies 2 }

rfChannel3 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The transmit frequency of channel 3."
  ::=3D { rfChannelFrequencies 3 }

rfChannel4 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
```

```
      "The transmit frequency of channel 4."
  ::=3D { rfChannelFrequencies 4 }

rfChannel5 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The transmit frequency of channel 5."
  ::=3D { rfChannelFrequencies 5 }

rfChannel6 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The transmit frequency of channel 6."
  ::=3D { rfChannelFrequencies 6 }

rfChannel7 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The transmit frequency of channel 7."
  ::=3D { rfChannelFrequencies 7 }

rfChannel8 OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The transmit frequency of channel 8."
  ::=3D { rfChannelFrequencies 8 }

rfTxChannel     OBJECT-TYPE
  SYNTAX  INTEGER (1..8)
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
       "The current transmit channel of the unit.  The transmit frequency for each
       channel can be read in the rfChannelFrequencies table."
::=3D { rfConfiguration 4 }

voicePriorityEnable  OBJECT-TYPE
  SYNTAX  INTEGER {
       veryHigh(1),
       high(2),
       medium(3),
       low(4),
       disabled(5)
       }
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
      "Enables priority handling of voice packets at the expense of
       data packets in the RF transmit bandwidth. The settings have
```

```
       the following meanings:
        1=3D Data packets may be reduced to as little as 12.5% of the
           total transmit bandwidth in the presence of high voice loads.
        2=3D Data packets may be reduced to as little as 25% of the
           total transmit bandwidth in the presence of high voice loads.
        3=3D Data packets may be reduced to 37.5% of the total transmit
           bandwidth in the presence of high voice loads.
        4=3D Data packets will not be reduced below 50% of the total transmit
           bandwidth in the presence of voice loads.
        5=3D Voice packets are not given transmission priority.  Data
           and voice packets are handled in the same way.
       Read-only at the remote."
  ::=3D { rfConfiguration 5 }

rfMaximumRemoteTxpower   OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
       "Maximum transmit power that any remote in the network may implement.  Valid
       only at the central."
  ::=3D { rfConfiguration 6 }

rfRemoteTargetRSSI   OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
       "The desired received signal strength level (at the central) of remotes'
       transmissions,
        in dBm. Read only at the remote."
  ::=3D { rfConfiguration 7 }

rfRemoteMaximumTxpower   OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
       "Maximum transmit power that a specific remote in the network may implement.
       Valid only at the remote."
  ::=3D { rfConfiguration 8 }

rfRemoteID   OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
       "The remote ID (right-most two bytes of the mac address) of the remote
       targeted by a remoteMaxTxpower command setting in the rfTxControl object.
       Valid only at the central"
  ::=3D { rfConfiguration 9 }
```

```
-- rfStatistics group

rfStatisticsRecord OBJECT-TYPE
  SYNTAX RfStatisticsRecord
  ACCESS not-accessible
  STATUS mandatory
  DESCRIPTION
          "Radio MAC protocol statistics."
  ::=3D { rfStatistics 1 }

RfStatisticsRecord ::=3D
  SEQUENCE {
    -- statistics that apply to centrals and remotes:
    rfAssocReqs
      Counter,
    rfAssocResps
      Counter,
    rfBeacons
      Counter,
    rfOutboundUdps
      Counter,
    rfOutboundNonUdps
      Counter,
    rfOutboundUdpErrors
      Counter,
    rfOutboundNonUdpErrors
      Counter,
    rfInboundUdps
      Counter,
    rfInboundNonUdps
      Counter,
    rfInboundUdpErrors
      Counter,
    rfInboundNonUdpErrors
      Counter,
    rfBids
      Counter,
    rfBidErrors
      Counter,
    rfReservations
      Counter,
    rfAssociatedRemotes
      INTEGER,
    -- statistics that apply only to centrals:
    rfPolledRemotes
      INTEGER,
    -- statistics that apply only to remotes:
    rfMissedDwells
      Counter,
    rfTotalBidAcks
      Counter,
  }

rfAssocReqs OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
```

```
  DESCRIPTION
      "The number of Association Request frames,
       sent by a remote, or received by a central."
  ::=3D { rfStatisticsRecord 1 }

rfAssocResps OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Association Response frames,
       received by a remote, or sent by a central."
  ::=3D { rfStatisticsRecord 2 }

rfBeacons OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Beacon frames,
       received by a remote, or sent by a central."
  ::=3D { rfStatisticsRecord 3 }

rfOutboundUdps OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Outbound UDP Data frames,
       received by a remote, or sent by a central."
  ::=3D { rfStatisticsRecord 4 }

rfOutboundNonUdps OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Outbound non-UDP Data frames,
       received by a remote, or sent by a central."
  ::=3D { rfStatisticsRecord 5 }

rfOutboundUdpErrors OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Outbound UDP data frames received by a remote in error."
  ::=3D { rfStatisticsRecord 6 }

rfOutboundNonUdpErrors OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Outbound non-UDP data frames received by a remote in error."
  ::=3D { rfStatisticsRecord 7 }
```

```
rfInboundUdps OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Inbound UDP Data frames,
       sent by a remote, or received by a central."
  ::=3D { rfStatisticsRecord 8 }

rfInboundNonUdps OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Inbound non-UDP data frames,
       sent by a remote, or received by a central."
  ::=3D { rfStatisticsRecord 9 }

rfInboundUdpErrors OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Inbound UDP data frames received by the central in error."
  ::=3D { rfStatisticsRecord 10 }

rfInboundNonUdpErrors OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Inbound non-UDP data frames received by the central in error."
  ::=3D { rfStatisticsRecord 11 }

rfBids OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of bid frames, sent by a remote, or received by a central."
  ::=3D { rfStatisticsRecord 12 }

rfBidErrors OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of bid frames sent by a remote for which there was no response
       from the central.  Valid only at the remote."
  ::=3D { rfStatisticsRecord 13 }

rfReservations OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of Reservation Requests conveyed by
```

```
       setting the More request in Inbound Data frames,
       sent by a remote, or received by a central."
  ::=3D { rfStatisticsRecord 14 }

rfAssociatedRemotes OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "At the central, number of remotes that have successfully associated.
       At the remotes, indication of current association with the central."
  ::=3D { rfStatisticsRecord 15 }

rfPolledRemotes OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of remotes on the poll list.
       Meaningful only at a central."
  ::=3D { rfStatisticsRecord 16 }

rfMissedDwells OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of missed dwells.
       Meaningful only at a remote."
  ::=3D { rfStatisticsRecord 17 }

rfTotalBidAcks OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The total number of Acks of bid frames
       addressed to any remote.
       Meaningful only at a remote."
  ::=3D { rfStatisticsRecord 18 }

-- rfAuthentication group

rfAuthState OBJECT-TYPE
  SYNTAX  INTEGER {
       unrestricted(1),
       restricted(2)
       }
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
      "If this object is set to unrestricted, it allows
       this central to Associate with any remote.
       If this object is set to restricted, it allows this
       central to Associate only with remotes that
       are in rfAuthenticationTable.  Valid  only at the central."
  ::=3D { rfAuthentication 1 }
```

```
rfAuthNumber OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of entries in rfAuthTable."
  ::=3D { rfAuthentication 2 }

rfAuthTable OBJECT-TYPE
  SYNTAX  SEQUENCE OF RfAuthEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "The table of remotes with which this central is allowed
       to Associate."
  ::=3D { rfAuthentication 3 }

rfAuthEntry OBJECT-TYPE
  SYNTAX  RfAuthEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "A remote with which central is allowed to Associate."
  INDEX   { rfAuthId }
  ::=3D { rfAuthTable 1 }

RfAuthEntry ::=3D
  SEQUENCE {
    rfAuthId
      PhysAddress
  }

rfAuthId OBJECT-TYPE
  SYNTAX  PhysAddress
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
      "An authorized remote is identified by its MAC address."
  ::=3D { rfAuthEntry 1 }

rfAuthAttemptNumber OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of entries in rfAuthAttemptTable."
  ::=3D { rfAuthentication 4 }

rfAuthAttemptTable OBJECT-TYPE
  SYNTAX  SEQUENCE OF RfAuthAttemptEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "The list of remotes that have tried to associate with
       this central."
  ::=3D { rfAuthentication 5 }
```

```
rfAuthAttemptEntry OBJECT-TYPE
  SYNTAX  RfAuthAttemptEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "A remote that has attempted to Associate with this central."
  INDEX   { rfAuthAttemptId }
  ::=3D { rfAuthAttemptTable 1 }

RfAuthAttemptEntry ::=3D
  SEQUENCE {
    rfAuthAttemptId
      PhysAddress,
    rfAuthAttempts
      Counter,
    rfLinkUp
      INTEGER,
    rfRSSI
      INTEGER
  }

rfAuthAttemptId OBJECT-TYPE
  SYNTAX  PhysAddress
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "A remote is identified by its MAC address."
  ::=3D { rfAuthAttemptEntry 1 }

rfAuthAttempts OBJECT-TYPE
  SYNTAX  Counter
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of attempts to associate by a remote."
  ::=3D { rfAuthAttemptEntry 2 }

rfLinkUp OBJECT-TYPE
  SYNTAX  INTEGER {
            linkUp(1),
            linkDown(2)
            }
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The RF link to this remote is up, or down."
  ::=3D { rfAuthAttemptEntry 3 }

rfRSSI OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
       "The RF received signal level from this remote, in minus dBm. Valid only at
       the central."
  ::=3D { rfAuthAttemptEntry 4 }
```

```
-- rfSiteSurvey group

rfMultiChannelRssiMeasurement OBJECT-TYPE
  SYNTAX  SEQUENCE OF RfRssiMeasurement
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "Array of RSSI measurements, indexed by channel.
       Valid only for remotes."
  ::=3D { rfSiteSurvey 1 }

rfRssiMeasurement OBJECT-TYPE
  SYNTAX  RfRssiMeasurement
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "RSSI levels, per channel.
       Valid only for remotes."
  INDEX   { rfRssiChannel }
  ::=3D { rfMultiChannelRssiMeasurement 1 }

RfRssiMeasurement ::=3D=20
  SEQUENCE {
    rfRssiChannel
      INTEGER (1..8),
    rfRssiLevel
      INTEGER
  }

rfRssiChannel OBJECT-TYPE
  SYNTAX  INTEGER (1..8)
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The channel in which this measurement was performed."
  ::=3D { rfRssiMeasurement 1 }

rfRssiLevel OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The measured RSSI level in negative dBm, or 110
       if not available."
  ::=3D { rfRssiMeasurement 2 }

-- rfCongestion group

rfDataSuccessRate OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
       "The ratio of uncontended data acknowledgements sent from the central=20
```

```
      to a particular remote over the number of uncontended data frames sent to the
      central from that remote, integrated over the previous measurement period and
      expressed as a percentage.
      Valid only at the remote."
  ::=3D { rfCongestion 1 }

rfTotalBidUsage OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The ratio of contended bid acknowledgements sent from the central to all
      remotes over the number of contended bid slots available, integrated over the
      previous measurement period and expressed as a percentage.
      Valid only at the remote."
  ::=3D { rfCongestion 2 }

rfLocalBidUsage OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The ratio of contended bid acknowledgements sent from the central to all but
      a particular remote over the number of contended bid slots available,
      integrated over the previous measurement period and expressed as a percentage.
      Valid only at the remote."
  ::=3D { rfCongestion 3 }

rfBidSuccessRate OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The ratio of contended bid acknowledgements sent from the central to a
      particular remote over the number of contended bid frames sent to the central
      from that remote, integrated over the previous measurement period and
      expressed as a percentage. Valid only at the remote."
  ::=3D { rfCongestion 4 }

rfTargetBidSuccessRate OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The ideal contended bid success rate for the current local usage, expressed
      as a percentage. Valid only at the remote."
  ::=3D { rfCongestion 5 }
 =20
rfDwellsPerBidPeriod OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The number of dwells constituting a period during which a particular remote
      may transmit to the central exactly one contended bid frame.
      Valid only at the remote."
  ::=3D { rfCongestion 6 }
```

```
 =20
rfCurrentBidDwell OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The current dwell number in the current bid dwell period.
       Valid only at the remote."
  ::=3D { rfCongestion 7 }
 =20
rfBidSendDwell OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
       "The dwell number in the current bid dwell period during which the remote may
       transmit its contended bid frame to the central.
       Valid only at the remote."
  ::=3D { rfCongestion 8 }
 =20

--Error log

elScrollControl  OBJECT-TYPE
  SYNTAX  INTEGER  {
           forward(1),
           backward(2),
           clearLog(3)
           }
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
       "A variable used to control the direction in which the error log is scrolled
       on repetitive reads, or to clear the log of all entries."
  ::=3D { wn3500_ErrorLog 1 }

elLogEntryNumber   OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
       "The entry number of the trap at which the next reading of the error log
       should commence."
  ::=3D { wn3500_ErrorLog 2 }

elLevelDisable  OBJECT-TYPE
  SYNTAX  INTEGER =20
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
       "The highest severity level of traps to be ignored with respect to logging and
       trap reporting."
  ::=3D { wn3500_ErrorLog 3 }


elTrapTable OBJECT-TYPE
  SYNTAX  SEQUENCE OF ElTrapEntry
```

```
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "The chronological list of error traps that have occurred at this unit."
  ::=3D { wn3500_ErrorLog 4 }

--Traps

elTrapEntry OBJECT-TYPE
  SYNTAX  ElTrapEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "A single error log trap entry."
  INDEX   { elEntryNumber }
  ::=3D { elTrapTable 1 }

ElTrapEntry ::=3D
  SEQUENCE {
    elEntryNumber
      INTEGER,
    elSeverityLevel
      INTEGER,
    elMessage
      DisplayString,
    elParameter
      INTEGER,
    elTimeStamp
      DisplayString
  }

elEntryNumber   OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The entry number of the trap in the log (0 is the oldest)."
  ::=3D { elTrapEntry 1 }

elSeverityLevel  OBJECT-TYPE
  SYNTAX  INTEGER  {
              empty(0),
              normal(1),
              warning(2),
              minor(3),
              major(4),
              critical(5),
              linkup(16),
              linkdown(17)
              }
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The severity level of the trap entry."
  ::=3D { elTrapEntry 2 }

elMessage OBJECT-TYPE
```

```
  SYNTAX  DisplayString (SIZE (0..63))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The error message string of the trap entry."
  ::=3D { elTrapEntry 3 }

elParameter OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "A context defined error parameter value."
  ::=3D { elTrapEntry 4 }

elTimeStamp OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..23))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The time and date of the trap occurrence."
  ::=3D { elTrapEntry 5 }

trapMessage OBJECT-TYPE
  SYNTAX  DisplayString (SIZE (0..63))
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The error message string of the most recent trap."
  ::=3D { wn3500_ErrorLog 5 }

trapParameter OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
      "The parameter value of the most recent trap."
  ::=3D { wn3500_ErrorLog 6 }

elTimeDate OBJECT-TYPE
  SYNTAX  SEQUENCE OF ElTimeEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "The current time and date."
  ::=3D { wn3500_ErrorLog 7 }

elTimeEntry OBJECT-TYPE
  SYNTAX  ElTimeEntry
  ACCESS  not-accessible
  STATUS  mandatory
  DESCRIPTION
      "A single entry time and date table."
  ::=3D { elTimeDate 1 }

ElTimeEntry ::=3D
  SEQUENCE {
```

```
    elTimeHour
      INTEGER,
    elTimeMinute
      INTEGER,
    elTimeSecond
      INTEGER,
    elTimeMonth
      INTEGER,
    elTimeDay
      INTEGER,
    elTimeYear
      INTEGER
  }

elTimeHour  OBJECT-TYPE
  SYNTAX  INTEGER  (0..23)
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
      "The current hour."
  ::=3D { elTimeEntry 1 }

elTimeMinute  OBJECT-TYPE
  SYNTAX  INTEGER  (0..59)
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
      "The current minute."
  ::=3D { elTimeEntry 2 }

elTimeSecond  OBJECT-TYPE
  SYNTAX  INTEGER  (0..59)
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
      "The current second."
  ::=3D { elTimeEntry 3 }

elTimeMonth  OBJECT-TYPE
  SYNTAX  INTEGER  (1..12)
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
      "The current month."
  ::=3D { elTimeEntry 4 }

elTimeDay  OBJECT-TYPE
  SYNTAX  INTEGER  (1..31)
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
      "The current day."
  ::=3D { elTimeEntry 5 }

elTimeYear  OBJECT-TYPE
  SYNTAX  INTEGER  (0..99)
  ACCESS  read-write
```

```
  STATUS  mandatory
  DESCRIPTION
      "The current year."
  ::=3D { elTimeEntry 6 }

elIfIndex   OBJECT-TYPE
              SYNTAX  INTEGER
              ACCESS  read-only
              STATUS  mandatory
              DESCRIPTION
              "The ifIndex associated with this table."
              ::=3D { wn3500_ErrorLog 8 }

criticalTrapCnt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-central
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates a failure of one or more of the
    unit's critical subassemblies resulting in severe loss of functionality."
  ::=3D 1

majorTrapCnt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-central
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates a failure or impairment one of the
    unit's subassemblies resulting in major loss of functionality."
  ::=3D 2

minorTrapCnt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-central
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates a failure or impairment of one of the
    unit's non-critical subassemblies resulting in some loss or =
impairment
    of functionality."
  ::=3D 3

warningTrapCnt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-central
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates pending or imminent failure or impairment
    of one of the unit's subassemblies which may result in some loss
    or impairment of functionality in the near future."
  ::=3D 4

normalTrapCnt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-central
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates the occurrence or completion
    of an event or process in the manner expected."
  ::=3D 5
criticalTrapRmt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-remote
```

```
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates a failure of one or more of the
    unit's critical subassemblies resulting in severe loss of functionality."
  ::=3D 1

majorTrapRmt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-remote
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates a failure or impairment one of the
    unit's subassemblies resulting in major loss of functionality."
  ::=3D 2

minorTrapRmt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-remote
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates a failure or impairment of one of the
    unit's non-critical subassemblies resulting in some loss or impairment
    of functionality."
  ::=3D 3

warningTrapRmt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-remote
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates pending or imminent failure or impairment
    of one of the unit's subassemblies which may result in some loss
    or impairment of functionality in the near future."
  ::=3D 4

normalTrapRmt  TRAP-TYPE
  ENTERPRISE  wavenet_3500-remote
  VARIABLES  { trapMessage, trapParameter }
  DESCRIPTION
    "A trap that indicates the occurrence or completion
    of an event or process in the manner expected."
  ::=3D 5

linkupTrap  TRAP-TYPE
  ENTERPRISE  snmp
  VARIABLES {elIfIndex}
  DESCRIPTION
    "An SNMP trap that indicates that the RF link has been
    established."
  ::=3D 3

linkdownTrap  TRAP-TYPE
  ENTERPRISE  snmp
  VARIABLES {elIfIndex}
  DESCRIPTION
    "An SNMP trap that indicates that the RF link has been
    lost."
  ::=3D 2

END
```