CitySOS

WIRELESS NETWORKS GROUP

Lucent Wireless Internet Access System

System Description

Version 1.0

1. Overview

This document, is a detailed technical description of the LTWIAS system. This document includes: Network Architecture Overview, Description of Network Elements and Interconnectivity, RF Network Planning Process, Site Preparation and Civil Engineering, and Installation of WIAS and Network Equipment.

Usunięto: (why write this again, if it already shows up on the table of contents?)

1.1. General

The LTWIAS is a state-of-the-art complete last mile wireless solution for high speed Internet access, and Virtual Private Networking. The system is designed, to provide a cost-effective solution, both for business and residential users.

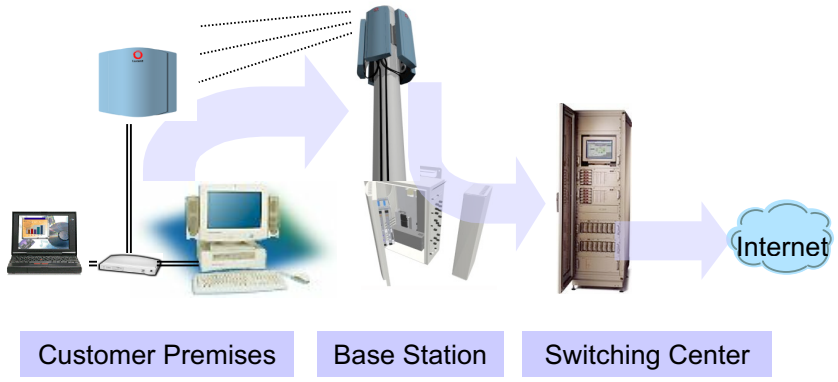
The LTWIAS solution operates in several frequency bands:

- Licensed Band- in the 3.4-3.6Ghz, using fixed frequency transmission.
- Unlicensed Band- in the 2.4 Ghz Industrial, Scientific and Medical (ISM) band, using Frequency Hopping Spread Spectrum (FHSS) technology.

Using packet-switching radio technology, LTWIAS system provides users with high-speed, high-performance fixed wireless access to the Internet and corporate Intranets.

The LTWIAS system includes three major building blocks:

- **Digital Switching Center (DSC)**, main switching and control station manages the interface to the Internet, and controls multiple Base Stations.
- **Data Base Stations (DBS),** provides wireless connectivity to customers' premises, in a Point to Multipoint configuration.
- **Wireless Modems (WM),** at customer premises unit, enabling end-user to access the WIAS network via air link to a Base Station.



1.2. Main Features

The LTWIAS wireless system features most valuable for Operators and Service Providers:

- High speed wireless Internet access
- Bit rate of 1.5Mbps per sector
- Cell size radius 3-6km
- Deployed in 3.5GHz licensed band, and 2.4Ghz unlicensed band
- Provide IP packet data services
- Full network management system
- Low cost, outdoor, compact system

1.3. Value Proposition

The value proposition to the Wireless Service Providers are:

- Enter the Internet access market
- Low initial investment
- Provide value-added VPN services
- Evolve to Voice over IP (VoIP)

The value proposition to the Customers are:

- Quick high-speed connection
- No new telephone connections
- Access to public and private networks
- Multiple computer connections per building
- VPN secured connection

2. Network Architecture Overview

This section is intended to introduce the reader to WIAS networking, system capabilities, and primary components.

2.1. Introduction to Network Architecture

The WIAS network provides Windows 95/98/NT based users with remote access to the Internet, and to private Intranets using VPN services over a high speed, packet switched, wireless data link. Users are able to access the public Internet, private Intranets and their Internet service providers over the wireless link. The network supports portability, that is, the ability to access the Internet and private Intranets using VPN services from anywhere that WIAS service is available. The network is targeted at users running horizontal Internet and Intranet applications. These applications include electronic mail, file transfer, browser based WWW access and other business applications built around the Internet.

2.2. Generic Internet Remote Access Architecture

The following figure gives a high level view of the remote access architecture that is deployed today for Internet and Intranet access. This architecture is based on dial-up POTS and ISDN technologies.

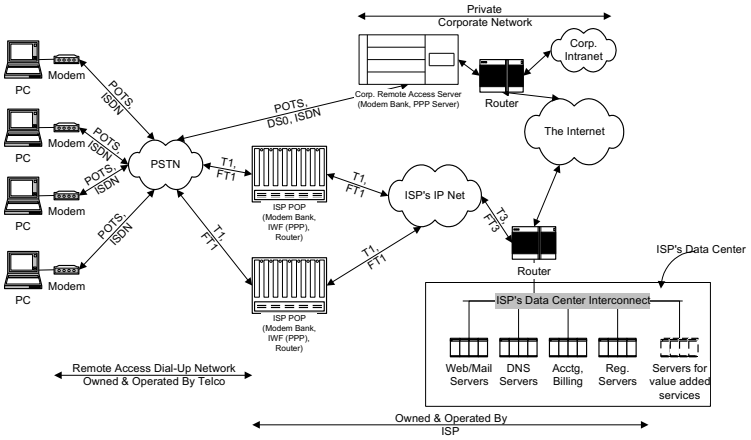


Figure 1 Generic Internet Access Architecture

As shown in Figure 1, there are at least three business entities, whose equipment, working together, provides remote Internet access to users. The first business entity is the telco that owns and operates the dial-up POTS/ISDN network. The telco provides the media in the form of the public switched telephone network over which bits (or packets) can flow between users and the other two business entities. The second business entity is the Internet service provider (ISP). The ISP deploys and manages the point of presence (POPs) in its service area to which end users connect for service. The ISP leases fractional T1 or E1, fractional T3 or E3 lines from the telco for connectivity to the PSTN. The ISP owns and operates its own Intranet backbone or leases bandwidth from an Intranet backbone provider. The POPs and the ISP's data center are connected together over the Intranet backbone. The data center houses the ISP's web servers, mail servers, accounting and registration servers, enabling the ISP to provide web content, e-mail and web hosting services to end users. Future value added services may be added by deploying additional types of servers in the data center. The ISP also maintains routers to connect to the public Internet backbone. In the current model for remote access, end users have

service relationships with their telco and their ISP and usually get separate bills from both. End users access the ISP, and through the ISP, the Internet, by dialing the nearest POP and running the Internet Engineering Task Force Point to Point Protocol (IETF PPP). The third business entity is the private corporation which owns and operates its own private Intranet for business reasons. Corporate employees may access the corporate network (e.g. from home or while on the road) by making POTS/ISDN calls to the corporate remote access server and running the IETF PPP protocol. For corporate access, end users only pay for the cost of connecting to the corporate remote access server. The ISP is not involved.

2.3. WIAS Network Architecture Overview

End systems are based on IBM compatible PCs running Windows 95/98/NT, connected to the WIAS wireless network using WMs. These WMs allow end systems to send and receive Media Access Control (MAC) frames over the WIAS air link. WMs are fixed and typically mounted on or near the rooftop. The initial offering of WIAS supports external WMs, and they will be attached to the user's PC/laptop via a 10 Base-T physical link. Thus, an Ethernet adapter card will be required in the user's PC or laptop.

Wide-area wireless coverage is provided by WIAS base stations. The range of coverage provided by base stations depends on factors such as link budget, capacity and coverage. Base stations multiplex end system traffic from their coverage area to the WIAS end system switching center over a wire line or a microwave back-haul network.

Figure 2 provides a high level view of the WIAS network architecture. It shows end systems with internal modems and also end systems attached to external modems via a 10Base-T link.

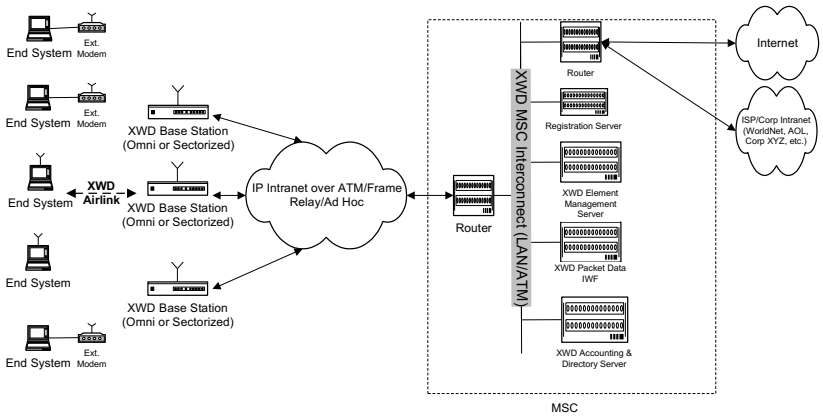


Figure 2 WIAS Architecture

The WIAS network architecture is independent of the MAC and physical layer of the air link. The architecture is also independent of the physical layer and topology of the back-haul network. The only requirements for the back-haul network are that it must be capable of routing IP packets between base stations and the DSC with adequate performance, using a T1/E1 interface. IP routers connect the DSC to the public Internet, private Intranets or to ISPs. Accounting and directory servers in the DSC are used to store accounting data and directory information. The element management server is used to manage the WIAS equipment that includes the WIAS base stations and accounting/directory servers.

The accounting server collects accounting data on behalf of users and sends the data to the service provider's billing system.

2.4. WIAS Equipment Overview

The WIAS system is comprised of WMs, APs, W-hubs, and DSCs. A DBS is comprised of a single W-hub and five APs. WMs and APs emit low power RF signals into integrated directional antennas. The small sized APs and integrated directional antenna can be viewed as sectors of a base station. APs and WMs can be mounted on roof-tops or side walls of buildings. The product line provides growth and migration paths which can be achieved by adding sectors to provide increased capacity.

Table 1 Wireless Modems

Parameter	Specifications for the Licensed Band	Specifications for the Unlicensed Band
Air Interface	1.5 Mbps Packet Radio	3.2 Mbps Packet Radio; 1.6Mbps fall back
Standard Frequency Plan	3.4 - 3.5 GHz uplink 3.5 - 3.6 GHz downlink Paired 5 MHz blocks, Frequency Division Duplexing (FDD) with 100 MHz frequency separation	2.402-2.480GHz 1 MHz Frequency Hopping Spread Spectrum transmission, Time Division Duplexing (TDD)
Capacity	One WM supports up to 10 simultaneous users based on present remote dial-up network traffic patterns	One WM supports up to 10 simultaneous users based on present remote dial-up network traffic patterns
Antenna	Planar Array integrated with radio unit	Planar Array integrated with radio unit
Antenna Gains	17 dBi typical (18 ° AZ × 18° EL HPBW)	15 dBi typical (20 ° AZ × 20° EL HPBW)
Physical	Dimensions: 12" W × 4" D × 14" H Weight: 8 lbs.	Dimensions: 12" W × 4" D × 14" H Weight: 8 lbs.
Environment	Outdoor -40°C to 46°C	Outdoor -40°C to 46°C
Power Supply WM	Utility Power: 120-240 VAC 50/60 Hz, Universal Power Converter: 24 VDC 36W AC to DC	Utility Power: 120-240 VAC 50/60 Hz, Universal Power Converter: 24 VDC 36W AC to DC

Table 2 Data Base Station (Access Point & W-hub)

Parameter	Specifications for the Licensed Band	Specifications for the Unlicensed Band
Air Interface	1.5 Mbps Packet Radio	3.2 Mbps Packet Radio; 1.6Mbps fall back
Antenna	2 Branch polarization diversity at base station using integrated planar arrays	2 Branch polarization diversity at base station using integrated planar arrays
Antenna Gains	15 dBi typical (72 ° AZ × 7° EL HPBW)	13 dBi typical (72 ° AZ × 7° EL HPBW)
Standard Frequency Plan	3.4 - 3.5 GHz uplink 3.5 - 3.6 GHz downlink Paired 5 MHz blocks, FDD with 100 MHz frequency separation	2.402-2.480GHz 1 MHz Frequency Hopping Spread Spectrum transmission, Time Division Duplexing (TDD)
Transmission Standard	Up to four T1/E1 frame relay connections to W-Hub	Up to four T1/E1 frame relay connections to W-Hub
Traffic Capacity	One W-Hub supports five Access Points One DBS initially supports up to 100 simultaneous PPP sessions based on present remote dial-up network traffic patterns	One W-Hub supports five Access Points One DBS initially supports up to 100 simultaneous PPP sessions based on present remote dial-up network traffic patterns

Cell Planning	5 sectors with 5 MHz spectrum allocation, 1 carrier/sector Overlapping coverage per sector possible if spectrum is available	5 sectors with 1 MHz Frequency Hopping (FH), 1 hopping sequence/sector
Physical	Dimensions: AP – 12" W × 5" D × 30" H W-Hub Outdoor – 28" W × 12" D × 30" H W-Hub Indoor – 22" W × 12" D × 30" H Weight: AP – 13 lbs. W-Hub Outdoor – 40 lbs. W-Hub Indoor – 30 lbs.	Dimensions: AP – 12" W × 5" D × 30" H W-Hub Outdoor – 28" W × 12" D × 30" H W-Hub Indoor – 22" W × 12" D × 30" H Weight: AP – 13 lbs. W-Hub Outdoor – 40 lbs. W-Hub Indoor – 30 lbs.
Environment	AP – -40°C to 46°C W-Hub Outdoor – -40°C to 52°C W-Hub Indoor – 5°C to 35°C	AP – -40°C to 46°C W-Hub Outdoor – -40°C to 52°C W-Hub Indoor – 5°C to 35°C
Power Supply W-Hub	Utility Power: 120-240 VAC 50/60 Hz, 750VA	Utility Power: 120-240 VAC 50/60 Hz, 750VA
Power Supply AP	48 VDC, 75 Watt supplied by W-Hub	48 VDC, 75 Watt supplied by W-Hub

2.4.1. Data Switch Center

The WIAS DSC is where common equipment is centralized to support a number of DBSs. The DSC equipment provides common services. In WIAS there are several wireless data services that are provided from within the DSC. The provided server functions are listed below. The actual implementation may group or partition these functions differently.

Database server: Storage for network configuration data, subscriber data, home directory, foreign directory, and accounting data.

Network management server: All network management functions are performed through this server.

Registration server: Performs all registration functions on behalf of users. It uses the RADIUS protocol to communicate with other WIAS network elements during the registration phase.

Accounting server: Collects and stores all accounting information generated by WIAS network elements on behalf of subscribers. WIAS network elements use the RADIUS accounting protocol to send user accounting information.

Routers: Information processed by the WIAS system flows through two distinct router groups. The inner router typically terminates the IP over frame relay connections from WIAS base stations. The outer router (not part of WIAS offer) connects to the public Internet.

RAS server: Terminates PPP locally in the DSC.

Terminal Server and Modem bank(s): Used for remote administration.

Table 3 Data Switch Center

Parameter	**Specifications**
Transmission Links	Back-haul to Internet T1/E1 or T3 or fractional T3
Physical	Dimensions:

	Server Cabinet – 24 " W x 34" D x 40" H Network Cabinet – 24 " W x 34" D x 74" H Network Growth Cabinet – 24 " W x 34" D x 74" H Weight: Server Cabinet – 530 lbs. (fully equipped) Network Cabinet – 585 lbs. (fully equipped) Network Growth Cabinet – 578 lbs. (fully equipped)
Environmental	Indoor 10°C to 35°C
Power Supply	Utility power 110-240 VAC 50/60 Hz, 4.7 kVA (with three racks)

2.5. Network Operation, Management and Supervision

A network management server provides a graphical interface to system elements to enable the customer to monitor the current state of the Access Points, W-hubs and trunks.

System management services enable technicians to monitor the status of the APs, W-hubs, and the management server. Should an equipment problem be detected, the following can be performed:

Access points can be reset (restarted) should their state become inoperative.
W-hubs can be reset. Configuration settings for the hubs can be installed and updated from the management system as necessary. Operational software can be updated from the management system.

2.6. Fault Management

WIAS provides fault management functions both on an element level and on an overall system integrated level. The high level Simple Network Monitoring Protocol (SNMP) manager (e.g. HP OpenView) is notified of alarm conditions. It is also able to periodically poll the WIAS element manager's Management Information Base (MIB) for the health and status of the WIAS network. System management personnel can view an iconic representation of the WIAS network and its current alarm state. By pointing and clicking on the WIAS icon, systems management personnel can execute the WIAS element management applications using a web browser and be able to perform more detailed management functions.

2.7. Configuration Management

Service providers deploying the WIAS network can control and configure the WIAS network and network elements from a network management system. The file transfer protocol (FTP) and SNMP protocols are used.

Service providers deploying the WIAS network can download software remotely to WIAS network elements from the DSC. The FTP protocol is used.

2.8. Security Management

Service providers can authenticate users before providing service. Authentication is performed for users accessing the service. The RADIUS protocol is used.

2.9. Performance Management

Service providers deploying the WIAS network can collect performance statistics from the WIAS network elements using the DSC. The SNMP protocol is used.

2.10. Subscriber Activation

A graphical user interface (GUI) based software tool to add new subscribers to the system and obtain subscriber authentication credentials is provided to the service provider.

2.11. Technician Service Port

Using the SNMP network management agent in WMs, service technicians equipped with PCs running SNMP network managers (e.g. HP OpenView, etc.) can perform complex OA&M operations at the user's site.

The W-hub is equipped with a serial port for setting up a User Datagram Protocol (UDP) link using the PPP protocol. A 56 kbps modem is normally connected to the serial port of the W-hub. The modem, in conjunction with the DSC, is used for remote base station management functions.

2.12. Quality of Performance

2.12.1. DSC recovery and reliability

DSC recovery and reliability is provided by active/standby server technology coupled with data storage redundancy. This combination provides an entry level solution that delivers reliable data storage, accessed by the DSC servers and provides greater system availability. Recoveries are reported to the network management system to enable maintenance personnel to make repairs to the faulty server, and restore it to the standby state.

2.12.2. Network recovery and reliability

The network management complex continuously collects health and status information from each network element. This information is provided via a graphical interface to technicians managing the network. When a network element experiences an error condition, the element is automatically taken out of service. Careful network design insures that whenever possible, performance degradation (reduced data capacity) is the result, rather than element loss. However, when a simplex network element fails, a critical alarm condition is registered at the network management system so that technicians may immediately initiate recovery and repair actions.

2.12.3. Access point recovery and reliability

Each AP is assigned a unique IP address. An SNMP agent continuously provide status and health information. The AP can be reset remotely when certain alarms are reported. When reset remotely, it enters a memory segment that can determine whether a new download of execution code is required. If required the AP code is automatically updated. Presently when an AP fails to boot or fails to communicate with the W-hub it stops transmitting over the media and attempts to establish communication with the W-hub. If the network management system can not remotely reset or monitor an AP, the AP must be power cycled or removed by a technician.

2.12.4. W-hub recovery and reliability

The W-hub is a simplex system element, and loss of the hub results in the loss of service for a cell site. Health and status information collected by the network management system reports a critical alarm when the hub experiences a severe problem, and alerts maintenance personnel to immediately recover the device. Should remote maintenance not rectify the alarming condition, technicians must be dispatched.

2.12.5. Wireless modem recovery and reliability

The WM is managed mostly by the end-user. The end-user is provided with a start-up disk that loads the WM memory with the latest version of executable code. Software updates can be subsequently loaded by the user. When a WM fails to communicate with the end-user terminal, the end-user can reset it by activating a special reset software that runs on the end-user terminal. If after multiple reset commands the WM continues to malfunction while the WIAS network is operational, the WM needs to be replaced. No redundancy is planned for a malfunctioning wireless modem.

2.12.6. Encryption Of Bearer Data

The WIAS network will support encryption of data sent between the end system and remote access servers (PPP encryption). End systems can negotiate encryption to be on or off by selecting the appropriate security context. A later release will add over-the-air encryption which can be turned on or off by the service provider.

2.12.7. Frequency Bands

The LTWIAS solution operates in several frequency bands:

Licensed Band- currently it operates in the 3.4-3.6Ghz, using fixed frequency transmission. LTWIAS radios are frequency band specific, and only operate in the designated band. The uplink band of operation is 3.450 - 3.500 GHz. The corresponding downlink frequency band is 3.550 – 3.600 GHz.

-

- Unlicensed Band- the 2.4 Ghz Industrial, Scientific and Medical (ISM) band, using Frequency Hopping Spread Spectrum (FHSS) technology. The ISM band is defined between 2,402-2,480 MHz.

Description of Network Elements and Interconnectivity
The following sections will describe each element of the SOS Internet WIAS network, and its interaction with related components.

2.13. Customer Premise Equipment

The following equipment is provided by SOS Internet to aid the service provider in WIAS installations:

1. Wireless Modem
2. Wireless Modem Installation Kit

Installing WIAS at a customer's site will follow the same general steps. Although, actual configurations may vary on a per installation basis.

2.13.1. Potential Customer Premise Configurations

Recognizing the need for a WM to work with different configurations of customer premise equipment, SOS Internet designed a WM that supports the needs of both residential and business subscribers. Section 2.1.2 and 2.1.3 outline two potential configurations.

2.13.2. Potential Residential Installation

For residential users, the WM connects to the end-user system via an Ethernet 10BaseT physical and link layer interface (RJ45 cable). The WM is mounted on the outside of a home, or apartment complex at an elevated point on or near the rooftop. The user terminal can be Windows95, or Windows98 based with a commonly available Ethernet 10BaseT card. Figure 2.13.2-1 shows typical residential subscriber unit configurations. Multiple subscribers can be served with a single WM.

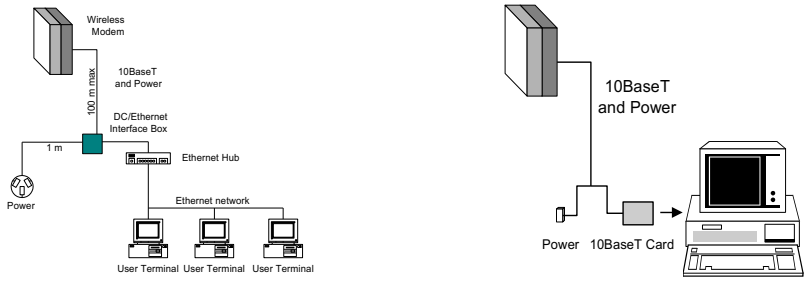


Figure 2.13.2-1. Single and multiple user subscriber equipment configurations.

In this configuration, the end-user terminal device stores the user's wireless security credentials. These credentials are used to authenticate connections made by the end-user terminal device. A dial-up networking icon is created for each PPP peer that is requested by an end-user device. This icon is used to specify details about the connection. If no remote PPP peer addressing information is provided, the network provides simple IP service to the end-user terminal device.

2.13.3. Potential Corporate Installation

In a corporate environment, users connect to the WIAS network using a wireless router. Users on a corporate LAN can use PCs equipped with Ethernet cards to route IP packets in and out of the wireless router. The wireless router terminates multiple simultaneous PPP links over which corporate LAN traffic is securely routed.

The corporate terminal equipment contains an optional Ethernet hub if multiple wireless routers have to be configured to share a single WM or vice versa.

The wireless router stores the corporation's wireless security credentials. These credentials are used to authenticate connections made by the router. For each PPP peer that a router wants to connect to, a dial-up networking icon is created. This icon is used to specify details about the PPP connection. If no remote PPP peer addressing information is available, the network provides simple IP service to the router.

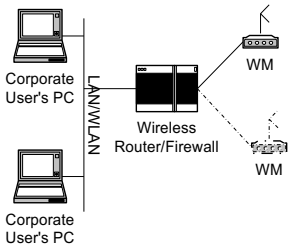


Figure 2.13.3-1. Corporate router architecture.

2.13.4. Wireless Modem

The Wireless Modem enables an end-user to access the WIAS network via the air link to an AP. The WIAS architecture uses RLP for in-sequence delivery of frames between the end-user device and the AP. RLP is a SOS Internet proprietary protocol.

WMs are designed for outdoor installations and can safely operate in all weather conditions. WM temperature rating is –40°C to 46°C. A WM weighs approximately 8 pounds and is approximately 12 inches in width, 14 inches in height, and 4 inches in depth. WM power is provided over a custom cable.

2.13.5. Wireless Modem Installation Kit

In addition to the WM, SOS Internet also provides some of the items necessary to complete a WIAS installation.

1. Interface Adapter Box (IAB)
2. Mounting Brackets (vertical or horizontal)
3. Power Supply
4. AC Cord
5. Plug-in Terminal Block
6. WIAS End-user Software

Further detail about WM installation, or the equipment provided by SOS Internet is given in WIAS installation manuals and site prep guides.

2.13.6. Customer Premise Equipment <u>not</u> Provided by SOS Internet

As was previously mentioned, WIAS can be installed in several different configurations. Before a WM installation can occur, an end-user's PC must have the following minimum equipment:

1. IBM or compatible PC
2. 16MB RAM

3. 20MB Hard disk space
4. Pentium 133 MHz processor
5. Ethernet card
6. Microsoft Windows 95/98

In the WIAS network, a PC is responsible for creating a PPP session to the LNS (described in section 2.4.1.3) for the purpose of obtaining network services. The PC also provides authentication information to the W-hub, and LNS. This is accomplished through two separate authentications. The first authentication occurs at the W-hub and checks to ensure that the subscriber has the appropriate credentials to use the airlink. The second authentication is between the PPP client and the LNS. The user information given to the LNS is entered in the Microsoft PPP connectoid. On Windows 95/98 systems, it is the user name and password dialogs just above the LNS IP address entry. Authentication methods for individual systems (W-hub and LNS) are described in later sections.

In the WIAS architecture, an Ethernet card is responsible for providing a physical interface from the client to the Wireless Modem. The Ethernet card can still provide other functions to its native network, while also providing SOS Internet WIAS network services.

A custom cable, provided by Madison Cable, a subsidiary of AMP Corporation, is also required in the course of a WM installation. This cable combines Ethernet and electrical power and connects the WM to the IAB.

2.14. WIAS Base Station

A WIAS base station is composed of up to 5 APs and a W-hub. The purpose of the base station is to provide wireless connectivity to the WMs.

2.14.1. Access Point

The AP terminates the air interface between the subscribers' WMs and the base station. The air interface is a critical aspect of the WIAS system. A minimum of one AP is required to provide coverage in a desired geographical area. AP antennas are sectorized antennas with beam widths of 72°. Multiple APs can be used to provide overlapping coverage if additional spectrum is available.

APs are designed for outdoor installations and can safely operate in all weather conditions. APs temperature rating is –40°C to 46°C. An AP weighs approximately 13 pounds and is approximately 12 inches in width, 30 inches in height, and 4 inches in depth. AP power is provided from the W-hub over a custom cable.

2.14.1.1. W-hub

After receiving data from the AP, the W-hub strips off the RLP overhead, and encapsulates the raw PPP data into L2TP. The interface between the APs and the W-hub is a shared 10Mbps 802.3 connection. The W-hub then takes the encapsulated data and transmits it over the back-haul to a LNS. The back-haul connection to the DSC is a T1/E1 interface.

The W-hub also provides an over-the-air authentication, enabling service providers to restrict airlink access to registered users. To accomplish this authentication task, a Radius Client is built into the W-hub. This radius client is responsible for querying a radius server, located at the DSC. The W-hub encapsulates and routes data to the DSC after obtaining the appropriate permissions from the RADIUS server. Additionally the Radius client can also make decisions concerning which LNS the user is allowed to access, or directing a user to the appropriate LNS altogether. The W-hub also gathers the raw subscriber usage information and forwards the information to the accounting server located at the DSC.

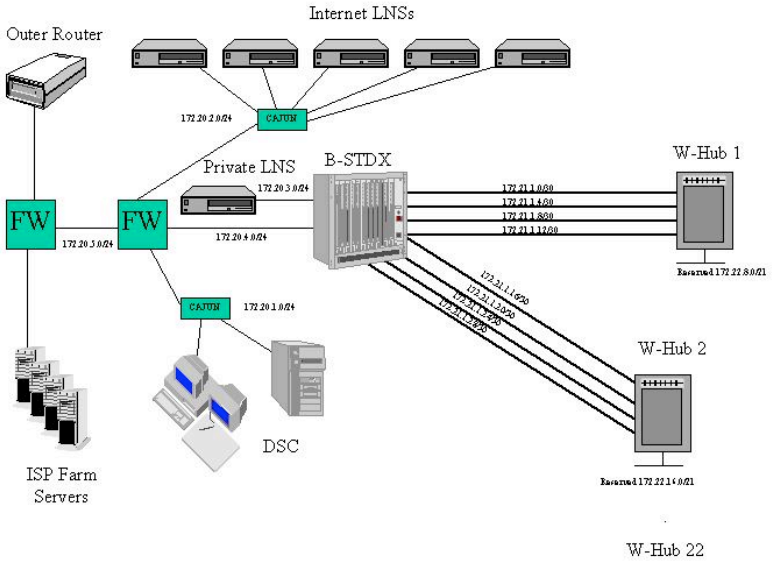
W-hubs support up to 5 APs and are designed for indoor or outdoor installations. Outdoor W-hubs can safely operate in all weather conditions. Outdoor W-hub temperature rating is –40°C to 52°C. A W-hub weighs approximately 40 pounds and is approximately 28 inches in width, 30 inches in height, and 12 inches in depth. The W-hub is powered by commercial 220 VAC power or by UPS batteries. The W-hub also provides 48 VDC power to each AP.

2.15. Back-haul Transmission Network

The back-haul transmission network is a function of the T1/E1 medium, the W-hub and the Ascend BSTDX-9000 switches. W-hub E-1 capability is presently provided via PMC cards that are plugged directly into the W-hub CPU board. There are 2 E-1 slots per card, and a maximum of 2 cards per W-hub. The E-1 cards are completely self-contained, with CSU/DSUs on board. Hence, T1/E1s may be plugged directly into the Telco provided E-1 circuit. The 4 E-1 ports do not have the ability to be bonded, but instead act as individual entities; thus traffic may not traverse more then 1 E-1 per call. However calls may be spread between E-1's based on LNS address. The BSDTX-9000 switch comes with built in CSU/DSUs and supports up to 96 T1/E1s.

2.16. Data Switching Center

The WIAS DSC is where common equipment is centralized to support up to 24 base stations. The DSC equipment provides common services, such as network management. Below is a picture outlining the components of a DSC.



2.16.1.1. Cajun Switches

The SOS Internet Cajun switches are used to concentrate traffic from the Ethernet interfaces on the Ascend BSTDX-9000 switches. Devices which are connected to the Cajun switch include:

- Ascend BSTDX-9000 Switches
- Compaq Network Management Cluster
- IBM 2216 L2TP/LNS Servers
- SOS Internet Managed Firewalls

The Cajun switch also provides layer-2 store and forwarding. As a result, everything but network broadcasts stays within two segments. Therefore computers which are running on the same switch cannot "see" each others traffic unless they are both connected to the same port.

2.16.1.2. Network Management/Database Cluster

The network management/database cluster is responsible for network operations. The cluster consists of 2 fault tolerant NT servers, running an Oracle database which stores parameters and settings as well as HTML/Java code that comprise the management interface. In this environment, a Java applet makes changes to the database via a web-browser. Whereas, Oracle back-end processes such as the Oracle Application server provides functions such as generating configuration files from the database for the various components of the SOS Internet WIAS network. The server cluster contains the following critical components:

WIAS Radius Server: Provides user authentication for the over-the-air segment of this procedure. An external Radius server not managed by SOS Internet provides the LNS authentication. The user information for the over-the-air authentication is also stored in the oracle database. The radius server is run completely with Java code, and uses a flat file (generated from the database) as the basis for authentications. The radius server is also responsible for processing accounting packets from the Radius client. The accounting packets are used by other systems such as a billing system

Oracle DataBase: Essential for storage of the configuration files and user information. The database is where all W-hub configuration files, Radius user tables, and other critical management information are stored.

NMS/SMS GUI: Network Management System/Subscriber Management System GUI is responsible for providing a UI or user interface to the SOS Internet WIAS network. Consisting of Java Applets and HTML, it is delivered to the user utilizing a standard web-browser.

HP OpenView: HP OpenView is used to query individual devices across the network. Queries may include status, traffic statistics, configuration parameters, etc. There are extensive MIB's available for most every component of the SOS Internet WIAS network.

NT Clustering Software: The NT clustering software is responsible for providing fail-over support to the NT servers. In the event that one system dies completely, within a short period of time, the second machine takes over failed applications, and processes.

It is recommended that the Network Management System/Database cluster be installed at a safe, secure, environmentally controlled location. An ideal place would the NOC for the SOS Internet WIAS network.

2.16.1.3. L2TP Tunnel Server (IBM 2216)

The IBM 2216 is used to terminate PPP sessions. Although the LNS server can be located anywhere in the network, it is typically located just before the outer router. In the case of VPN traffic, the LNS would

be located just behind a corporate firewall. This configuration allows only L2TP traffic from remote users into the VPN, while providing full access to the corporate network.

Two primary methods exist for authenticating the LNS. One possible method is to create, manage, and maintain local users file. This method has the benefit of being inexpensive and easy to implement. However, maintaining local user files has considerable drawbacks as a network grows. Another configuration, and a more robust option is to authenticate the 2216 via a RADIUS server. This option is recommended by SOS Internet. A key benefit of this implementation is that it enables the RADIUS server to seamlessly authenticate users.

Using the recommended configuration also enables the RADIUS server and the LNS to jointly support enhanced features inherent in the WIAS network, such as routing entire subnets to a single end user IP address. This joint interaction between the RADIUS server and LNS is critical, as managing enhanced services via a command line interface directly on the LNS requires human intervention which is time-consuming.

2.16.1.4. Outer Router or Border Router (Not Part of Core WIAS Offering)

The outer router function provides connectivity to another ISP's backbone network, or the public Internet. Typically an existing ISP would add the outer router to its group of core routers. Integrating the outer router into an existing network, will require placing LNS servers, to terminate L2TP sessions, behind the outer router. Depending on where you place this outer router it can also serve as a line of defense in additional to any firewalls. General filters applied at this router can help to insure that sensitive subscriber information is not made available via the network.

SOS Internet Technologies does not provide an outer router as part of the WIAS offering. However, SOS Internet does recommend that the outer router, chosen by a service provider, is capable of being upgraded to process 3 to 5 times initial bandwidth demands. This recommendation is driven by the rapid growth in Internet applications and consumers demand for bandwidth.

2.16.1.5. Out of Band Management System (Not Part of Core WIAS Offering)

In the unlikely event that your network goes down, you will want a way to access your core of operations without being dependent on external carriers. This can be extremely useful in reducing the downtime associated with configuration mistakes, and general mishaps which cause outages. An obvious hole in security, an Out of Band Management System must typically be able to traverse all areas of the network without incident. In the event of a network failure, you don't want to spend time reconfiguring your firewall, just so you can reach that router that happened to lose half of it's interfaces to who knows what. It is imperative that limited login access to the Out of Band Management System be given. It is ideal to authenticate this machine against local user table, and not via a Radius server. (how are you going to login in the event that the Radius server is down?) In short it needs to be completely independent from the rest of the infrastructure. It is for this very reason that management of login credentials for this unit to be paramount. The SOS Internet WIAS recommended out of band management system consists of a PM-2 terminal server. It has the capability to provide the user with access to W-hubs, whose back-haul transmission networks may be down. It can also provide access to WIAS components, which may not be reachable due to network connectivity problems. The PM-2 as recommended by SOS Internet has 3 modems attached. The first modem is used to dial-in to the DSC network in the event that the external connections to the DSC are severed. The second modem is used for Dial-Out to the W-hub via direct serial console. The third modem is used to Dial-Out to the W-hub via PPP in the event that you have switched the W-hub console to PPP mode. The PPP mode is necessary in the event that a software reload is necessary to restore the back-haul transmission network. The remaining serial ports on the PM-2 may be used to provide direct serial line connectivity to various routers, LNS servers, etc.

2.16.1.6. SOS Internet Managed Firewall

Network managers should address security concerns, since the WIAS network is connected to the Internet and is based on IP protocols. Although firewalls are not part of the core WIAS offering, the network has hooks to enable a service provider to easily configure a firewall. The following discussion is relevant for the SOS Internet Technologies Managed Firewall.

The SOS Internet Firewall application exists in a processor, called a brick, based on the Intel Pentium platform. The brick is equipped with four Ethernet interface cards and can be positioned between any type of Ethernet-based network elements (e.g., routers, hubs, switches, servers, PCs). Since, the brick is a bridge-level device, these network interfaces do not have IP addresses. Consequently, the brick is rendered invisible to other network elements.

The brick has no monitor, keyboard or hard disk. Other than a floppy disk drive for initial software boot, it has a minimum of moving parts (an on/off switch and a power supply fan). The brick initially boots from a floppy diskette that is created by the Security Management Server. Boot images subsequent to initial boot can be loaded from FLASH RAM in about 30 seconds. The firewall software that runs on the brick is based on the Inferno™ operating system, a small, highly efficient and highly secure Bell Labs-developed operating system. The firewall code — which is simple and small — is imbedded within the Inferno™ operating system kernel. The operating system itself has no user accounts or file system to be hacked. The entire firewall software resident on the brick fits on a single 3.5-inch floppy diskette. The brick communicates with its Security Management Server using IP. Accordingly, the brick must be assigned a logical IP address. To further preserve network invisibility, the brick can be configured to communicate only with the Security Management Server's network address, silently dropping all other communication attempts and thus remaining invisible to all other network addresses. All communications between each brick and the Security Management Server are encrypted and authenticated using native Inferno™ encryption and authentication mechanisms (Diffie Hellman for key exchange, ElGamal for digital signatures and signature verification, and Triple DES for session encryption).

The Security Management Server ("SMS") software resides on a remote server. The Security Management Server software provides the tools to manage the security policies of multiple security zones across multiple firewalls. The software runs at the application layer using hosted Inferno™ on Windows NT™ and Sun Solaris™. The primary components of the Security Management Server software are hosted Inferno daemons, Java™ server-side applications, and a graphical user interface.

3. WIAS RF Network Planning Process

3.1. Introduction

The design and optimization of a WIAS network is by definition geographically and demographically driven and thus RF propagation is a key parameter in network design. This section sets out to educate the reader as to the steps required to complete a RF network plan. This section is only applicable to WIAS 3.4 GHz, and does not address TRT MDL radio network design.

3.2. Inputs into the planning process

3.2.1. Network design requirements

The network design is driven by the customer's requirements that will, in most cases, be formally specified between the network design organization and the customer. These requirements define the scope of the design and detail the commitments made to the customer.

The interaction to develop the RF plan will encompass elements of the customer's business plan and must include the subscriber distribution, the subscriber service profile, the required network coverage (including the required probability of coverage), the physical geography and the RF spectrum allocation.

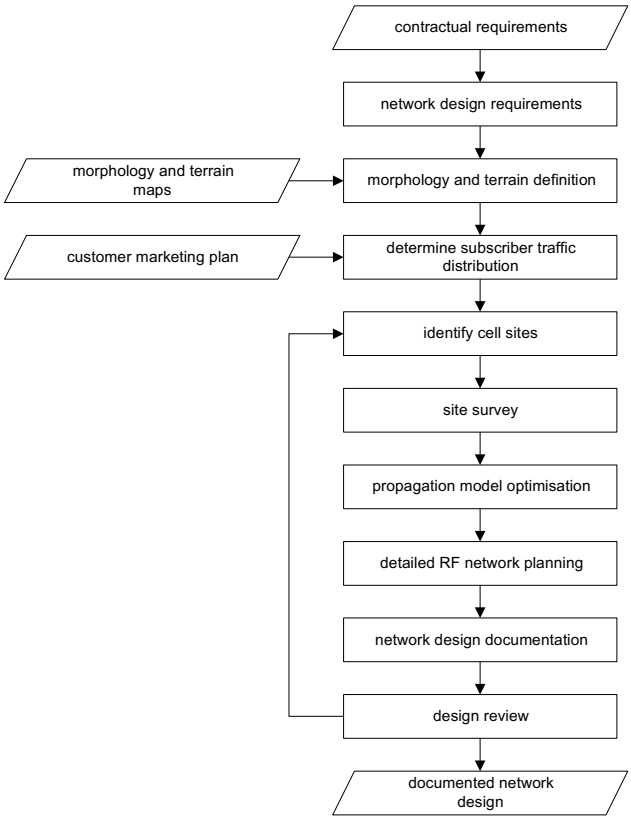


Figure 3.2.1-1. Network planning process

3.2.1.1. Subscriber distribution

The subscriber distribution is critical to the placement of cells and the configuration of base station equipment. There are two principal parameters for subscriber distribution:

- total number of subscribers to be served and anticipated growth of subscriber base
- distribution and density of potential subscribers

3.2.1.2. Physical geography

Data on the physical geography are required for propagation prediction and to aid the identification of suitable cell site locations if these are not provided. The principal requirements are:

- terrain (height of the ground)
- clutter (building heights, building density and land usage)
- for microcellular installation, building databases (height, location, etc.)

The resolution and detail of the terrain and clutter are largely dependent on what data is available. The finer the detail the more accurate will be the results of the propagation model and tool used.

3.2.2. Search Rings

Based on the physical geometry and customer requirements for coverage, initial search rings are issued to allow the customer and the site engineering teams to find candidate sites meeting the search ring criteria. Typically, the search ring criteria will include:

- height of base station
- height above clutter
- radius of search ring

3.2.3. Site Surveys

In many cases, the customer may provide a list of candidate cell sites meeting the search ring criteria requirements or initial inspection of the required coverage area may highlight suitable sites. These sites can then be subjected to a detailed site survey that is used to provide data for planning. The following lists the main survey requirements for the RF network planning of a WIAS network when a planning tool is used.

1. Frequency

    - The frequency band and the center of the operating frequencies.

2. Base site

    - Name
    - Address
    - Contact telephone number
    - Co-ordinates
    - Antenna height (above ground level)
    - Building or tower? - note any possible restrictions on construction e.g. power lines
    - AP location
    - Number of sectors
    - Other wireless systems located near the site: location, system (e.g. GSM), operator,
    - frequencies, power, bandwidth, antenna type, antenna azimuths and height.

3. Cell / Sectors

    - Radius
    - Number and bearings of sectors

4. Environment

    - Typical building heights
    - Typical building density
    - Typical types of buildings and roofs
    - Typical density of vegetation
    - Overall environment type (metropolitan, urban, suburban, rural, open, forest)

5. Maps

- Street map showing height contour lines and usage of land, i.e. buildings, vegetation, etc.; 1:10 000 scale preferred.
- Digital map of the terrain, clutter and vectors (railway lines, roads, etc.) of the area, preferably to the same scale as the street map. If the digital map is of a different scale to the street map then this must be allowed for in the data files.

7. Photographs

- Photograph of the base site
- Photographs from the base site pointing away from the site are useful to give the planner an idea of the terrain and clutter in the coverage area.
- Photographs should show the typical environment, i.e. buildings and vegetation types, heights and density.

3.3. Outputs of the planning process

3.3.1. Cell site configurations

3.3.1.1. Site location

The site address, latitude, longitude, and elevation are required.

3.3.1.2. Sectorization

The sector configuration for the site is required. The configuration possibilities are given in Section 3.6 and the principal parameters are:

- - number of APs (5)
- - assignment of APs to sectors and bearings

3.3.1.3. AP placement

For each AP at a base station site the following placement data is required:

- height above clutter level - base station APs are typically mounted at a height ≥ 15 m above the average clutter height
- bearing of main lobe (azimuth) - for five sector cells the bearing of the main lobe of each of the sectors should be at multiples of 72°. Typically, sectors in neighboring base stations will be aligned to a common pattern
- down tilt - some will have some degree of downtilt, typically, 2° - 10° which improves interference performance to neighboring cells.

3.3.2. RF and network performance predictions

3.3.2.1. Coverage

Coverage prediction and best server selection requires multiple sets of predictions for a given service area to provide insight into the direction of the best server for an arbitrary WM. Multiple coverage predictions are computed, and the best selection is chosen based on probability of coverage.

3.4. Provisioning resources for the network

3.4.1. Objectives

Given the subscriber distribution, a suitable network design can be produced. The first objective is to determine the required number of base station sites and their location. Having identified the number of base stations required, the back-haul network can be appropriately sized to provide the maximum capacity that the air interface can support.

3.4.2. Site identification

The identification of base station sites involves the mapping of cells over the area to be covered taking account of radio propagation and subscriber traffic patterns. Before detailed cell planning can be undertaken it is necessary to use an initial fix of base station sites. This is accomplished by consideration of the system limits and calculation of the absolute minimum number of cells required based on radio and traffic capacity limits. The greater of these two figures is then taken to be the minimum number of base station sites. Base station locations must then be chosen by examination of any mapping and survey data available. Suitable locations are identified by considering a number of factors, for example:

- clutter
- interference from/to other radio infrastructure
- back-haul
- site access
- planning restrictions
- power
- site availability
- rental costs

Frequently a list of candidate sites will be provided as the customer may have existing network infrastructure which they wish to re-use or may already have undertaken some site survey and acquisition work. The cell planning process is illustrated in Figure 3.4-1.

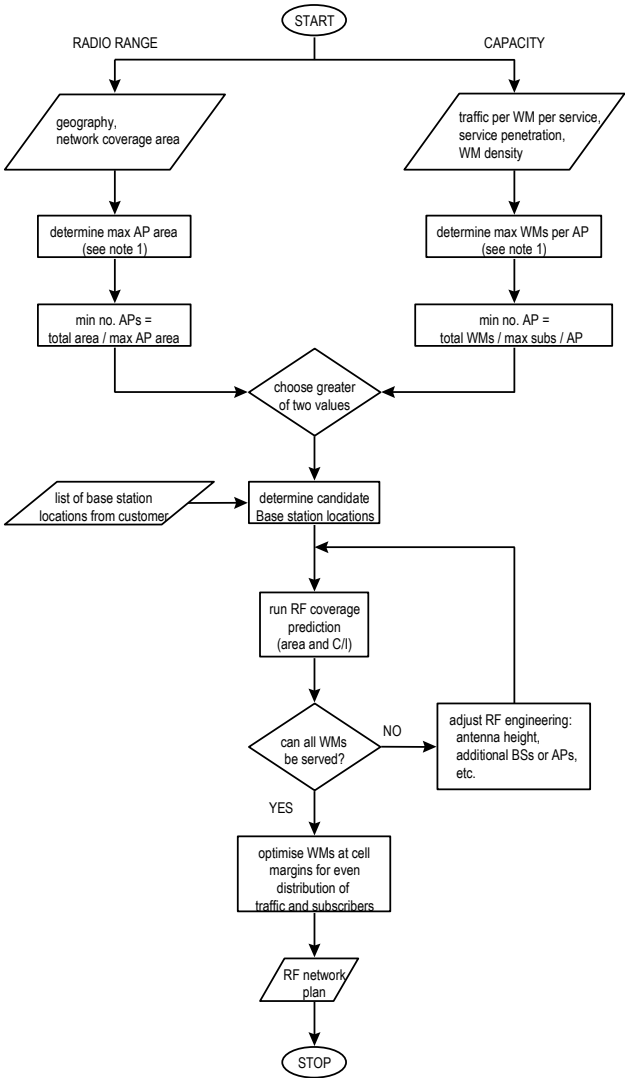


Figure 3.4-1. Flow chart for site identification and RF network planning

FIGURE 3.4-1 NOTES:

1. Calculation of these parameters is described in Section 3.4.3.1.

3.4.3. Network Limits

3.4.3.1. Limits on the size of a cell

The size of each cell is limited by both radio propagation and capacity exhaustion. These two mechanisms will each indicate a different value for the area of the largest cell. This approach minimizes initial infrastructure and installation costs. This approach has been used on other fixed wireless systems, with some unfortunate results when cell splitting is required to increase capacity. Splitting cells in a poorly designed network can require realignment of many WMs, which can be minimized if planned in advance. It is more appropriate to build out a network for a higher density sooner, rather than later, due to the potential need to realign subscriber unit already deployed in the field.

3.4.3.2. Traffic Capacity Limiting

Across a network each subscriber will generate a certain amount of traffic. Each base station within the network has a finite traffic carrying capacity. It follows that there will be a maximum size of cell dependent on the density of the offered traffic and the traffic capacity of the base station; the density of the offered traffic is, in turn, dependent on the amount of traffic offered by each subscriber and the subscriber density.

3.5. Base Station

3.5.1.1. AP

The BS can be equipped with up to 5 AP for each 5 MHz band of spectrum available. Each AP supports only 1 carrier, with carriers separated by 1 MHz. All APs provide a coverage beam of 72° degrees in azimuth. The actual number of subscribers that can be supported by an AP depends on the services offered and on the required quality of service.

3.6. Cell site configurations

3.6.1. Cell and AP configurations

The WIAS system can be configured for sectorized coverage. The sectorized scheme can employ 5 sectors. The current access point's azimuthal coverage angle is approximately 72° at the half power beamwidths (3 dB).

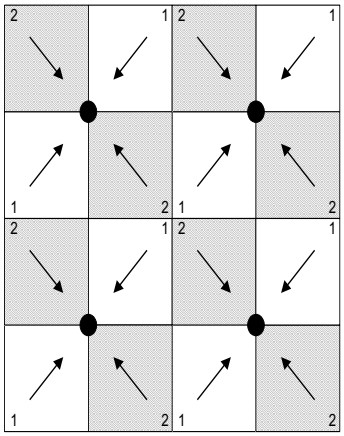


Figure 3.6-1. Basic sector and AP configuration
(5 sectors, 5 frequencies)

It is recommended that initially a site be equipped with five APs. The cell is divided into five sectors. This is shown in Figure 3.6-1.

3.6.2. Frequency reuse

3.6.3. Concepts

The WIAS system targets a frequency reuse of one, where all frequencies are reused in all cell sites. Initial roll outs can use higher frequency reuse values.

The directional nature of the WM also minimizes the interference to neighboring cells and sectors by minimizing the directions in which signals are radiated. WMs only radiate in the direction of their desired AP.

3.6.4. Frequency reuse for sectored cells

3.6.4.1. Frequency reuse rules

A rule that must be followed: non-adjacent frequency channels should be used on adjacent sectors of the cell site to minimize adjacent channel interference and front end overload at the AP and WM. Sometimes this may not be possible. The 5 sector pattern following that rule is shown in Figure 3.6.4.1-1.

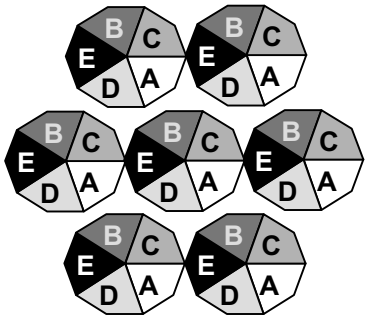


Figure 3.6.4.1-1. Replicated pattern for an WIAS network.

3.7. Coverage and air interface capacity planning methodology

3.8. Propagation for fixed wireless systems

3.8.1. Comparison with mobile cellular

Differences in the RF propagation conditions experienced by a WIAS system and conventional mobile systems arise for a number of reasons:

- directional WMs at the subscriber significantly reduces the effect of multipath
- installation of subscriber antennas at near rooftop height or above reduces the path loss relative to that experienced in a mobile system at the same frequency
- installation of the WM with knowledge of the received signal strength introduces a degree of "installation diversity". This reduces the variance of signal strength at a given distance from the AP site due to shadowing
- gross statistics of mobile subscribers change as a function of location, whereas the fixed subscriber is subject to the same gross signal and interference statistics
- fading encountered on fixed links can be more detrimental than on a mobile link due to the temporal response of the propagation channel. Fixed systems may encounter fade durations of 100 of ms covering 100s of kbits, whereas in mobile systems, the channel fade rate is much faster, and symbol times are 2 orders of magnitude greater. Interleaving can reduce the number of fading outages in mobile systems, whereas in fixed system, interleaving is not practical.

3.8.2. Propagation path loss

To determine the received signal strength at a particular WM or AP a number of factors must be known: the antenna gains at both AP and WM (variation with angle is described by the antenna pattern), the transmitted signal power and the path loss between the AP and WM antennas. The path loss is modeled as the sum of two components for a non-line of sight scenario: a deterministic component which predicts the mean path loss as a function of distance, and a random component due to obstacles in the path, i.e. *shadowing*.

3.8.3. Prediction of mean path loss

Prediction of the mean path loss depends on whether a line of sight (LOS) is available between the AP and WM. If LOS is available then path loss increases with the distance from the AP site as an inverse square law. Without LOS the path loss increases with a higher power of distance (three or more). At short distance between the WM and AP, the dominant mode is LOS and this becomes progressively non-

LOS as distance increases. This is often observed as a two slope path loss model where the rate of path loss increase changes from a LOS characteristic to a non-LOS characteristic.

Prediction of mean path loss is performed using empirically derived models. The model used depends on which frequency band is to be used:

- For 3.5 GHz, a SOS Internet Technologies developed proprietary model (similar to a Hata or COST231 type model) for 3.9 GHz systems is used together with a correction factor for use at 3.5 GHz.

These models require inputs of the environment type (urban, sub-urban or rural), antenna heights, and frequencies of operation and distance between AP and WM sites.

3.8.4. Effects of multipath

From measurements made in the fixed wireless access environment the channel can be characterized as having a single main received component and a small amount of multipath. An equalizer at the receiver minimizes the effects of short multipath. The current WIAS receiver has been shown to effectively combat delay spread to 1.5 ¦ s.

3.8.5. The effects of non-line of sight installation

WIAS systems do not require line of sight to all WMs to function correctly. The added loss of not having line of sight paths between APs and WMs is taken into account by the empirical propagation model and the statistical nature of the shadowing. Allowances for shadowing effects are taken into consideration when estimating the maximum reliable link budget to ensure that 90% coverage can be achieved.

3.9. RF, propagation and cell planning

3.9.1. Probability of coverage due to shadowing

3.9.1.1. Shadowing

Although the mean path loss at a particular distance from the AP site may be predicted using the model described above, there is still a random component of path loss that is not easily predicted. This is the shadowing caused by obstructions such as buildings. The randomly distributed position of these obstructers relative to the AP and WM means that the distribution of signal level is log-normal with a given standard deviation. This standard deviation may vary between 6dB and 12dB depending on environment and installation diversity.

3.9.1.2. Area coverage

There are two distinct aspects to the statistical variation of signals in a cellular system:

- *Location probability*
  The probability that a subscriber at a given location has service.
- *Area coverage probability*
  The percentage of subscribers in a specified coverage area that have service.

These terms are best explained by means of an example. If we consider the scenario shown in Figure 3.9.1.2-1 where predicted and measured received signal levels are shown on the same diagram, it can be seen that if a cell is planned using the absolute minimum pathloss that the receiver will operate with, then there will be a proportion of users that will not have coverage. It can also be seen that the further away from the base-site a user is, the more likely it is that he will not have coverage. The probability that a user at a particular distance has coverage is the location probability.

It can also be seen that if the minimum received signal level of the system is set artificially higher than required, a larger number of users will have service. As shadow fading is a log-normal random process,

the overall proportion of users with coverage can be predicted from the amount that the minimum received signal level is raised. It is therefore possible to predict an area of coverage, the signal level at the edge of which will be the absolute minimum receiver signal level plus the shadow margin. Within this area of coverage, there will be a probability of service.

In network planning, the probability of service will be one of the inputs and the area of coverage one of the outputs. If, for example, we are planning for 95% coverage, even when we have predicted an area of coverage using the correct shadow margin, there will be 1 in 20 potential subscribers that will not have coverage.

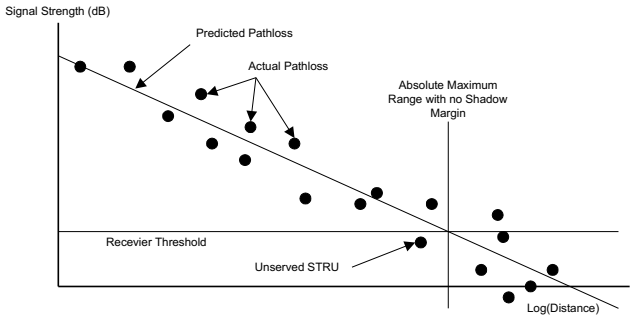


Figure 3.9.1.2-1. Predicted and Actual Pathloss Values.

3.10. Suggested Base Station Location Sites

Site acquisition requires having an understanding of the surrounding area and building or foliage clutter. It is recommended that the base station locations be such that a tower or a building is available for installation, and that the tower of building is a minimum of 15 meters higher than the surrounding clutter. This is a recommendation, not a requirement. If the APs are located higher than 15 meters above the clutter, the downtilt angles will need to be increased to reduce the cell coverage area. The detailed RF engineering of the site will indicate the suggested downtilt, and subsequent coverage area.

3.11. Network Growth

3.12. Types of network growth

Network Growth in an operational network will consist of two activities:

- increasing coverage
- increasing capacity

Planning for extended coverage is fundamentally the same as planning for a new network and the procedure outlined previously may be adopted. Planning for extended capacity in a given area due to increased number of subscribers is described in the next section.

3.13. Increasing capacity

Increasing capacity in the WIAS network will involve the addition of APs to the network. These can be co-located with existing APs if additional spectrum is made available, or they can be at new base stations sites if the same frequency band is to be reused. In certain hot-spots, frequencies can be reused within a base stations to provide very localized hot spot capacity improvements. This does, however, increase the interference to a neighboring cell, and further confuses the frequency planning.

Increasing capacity by forcing the access point coverage to be smaller will require realignment of some WMs already deployed in the field. This function must be kept to a minimum as the costs for realignment are high.

3.14. RF Planning with propagation tools

RF planning will be performed using SOS Internet CE4 WIAS module.

3.15. Summary of RF network design

The network design process can be summarized into several steps that may require a few iterations to converge on an optimized network. The steps are as follows:

Generate coverage plots for all the candidate cell sites.

- pick sites
- assign frequencies to sectors
- enter terrain, clutter databases for area
- enter shadowing statistics
- run coverage predictions, obtain coverage and C/I analysis plots

4. Site Preparation and Civil Engineering

4.1. Overview

This section sets out to explain, at a high level, the steps required to prepare and certify a site as ready for installation. These steps are a minimum, that is some sites may require additional preparation that is not specified in this document. Site preparation is explained in detail in the WIAS Site Preparation Guide.

4.2. Customer Premise

Relatively few activities are required to prepare a customer's site for WM installation. However, a critical aspect of WM site preparation is ensuring adequate spacing for the WM. A horizontal mounting bracket installation requires, 17 inches width and 12 inches of height and clearance to swing the WM from side-to-side. Whereas, a vertical mounting bracket installation requires 13 inches in the vertical and 33 inches in the horizontal plane.

Wireless modem site preparation should take approximately 1-2 hours. The time spent during site preparation will entail checking spacing, ensuring climbing safety, and minimum PC equipment.

4.3. Base Station

As indicated in a previous section, a base station comprises up to 5 APs and a W-hub. Site preparation for a base station involves numerous tasks which are outlined and detailed in the WIAS Site Preparation Guide. Some of these tasks include:

1. Local utility has provided electrical facilities.
2. T1/E1 back-haul is ready for connection to the W-hub.
3. Cable runs from APs to W-hub are completed.
4. Grounding and lightning protection systems are in place.
5. Rooftop and tower are certified ready to climb.

Although there are other tasks which are either included in the Site Preparation Manual, or may required for preparing an unusual site, the five steps listed above are a fair indicator of what is required when preparing a WIAS base station site. As installed dimensions of an AP and W-hub are provided in the following table

(amounts in inches)	Width	Depth	Height
AP	12	5	30
W-hub (outdoor)	28	12	30

Unlike other cellular systems, WIAS base stations do not usually require special floor loading considerations. WIAS' W-hub weighs approximately 40 lbs. and can safely be installed on most roofs.

Other considerations for site preparation include, the following physical limitations:

1. Maximum cable run from AP to W-hub is 100M
2. W-hub and AP clearances

In addition to these physical considerations listed above, one must take into consideration the ambient temperature requirements of an indoor W-hub.

Preparing a base station site should take into account any future network growth plans (i.e., cabling for extra sets of APs, ensuring the tower can support up to 3 sets of 5 APs, etc.).

Base station site preparation should take approximately 1-2 days. The time spent during site preparation will entail checking connections, running cable, ensuring physical requirements (AP spacing, Tower placement, etc.) are satisfied, and organizing the site for base station installation. A base station site is considered ready for installation when all items in the checklists have been satisfied. The checklists are available in Appendix A of the WIAS Site Prep guide

4.4. DSC

Preparing a site for a DSC installation requires careful selection and preparation of an environmental controlled room. The DSC consists of three primary cabinets: 1) Server Cabinet, 2) Network Cabinet, and 3) Network Growth Cabinet(s). Careful consideration will have to be given to the physical installation of a DSC, since the cabinets are approximately 7 ft. and weigh up to 600 lbs.

Given the weight and sheer size of the cabinets, floor spreaders may be required. This would be considered normal for preparing a DSC site and is the customer's responsibility. Fully equipped floor loading for each of the three cabinets should not exceed local regulations or 200 lbs./sq. ft..

Providing adequate air conditioning is also required in a normal DSC site prep. This need arises from the fact that a DSC is a collection of routers, hubs, servers, and computers. On average each cabinet is expected to generate 7,200 BTU. A service provider should also consider the effects of solar loading, in addition to the heat generated by the DSC. Air conditioning is required to maintain the room's ambient air temperature of 10°C to 35°C.

Generally considered completed when all the following conditions have been met.

1. All required grounding
2. 2 analog phone lines with modems
3. Cable protection and covers for back-haul system
4. Electrical AC power facilities
5. E1 facilities
6. AC surge protectors
7. E1 surge protectors

Site preparation for a DSC should take approximately 2-3 days. The time spent during site preparation will entail checking connections, ensuring physical requirements (floor loading, spacing, environmental, etc.) are satisfied, and organizing the site for DSC installation.

A DSC site is generally considered ready for installation when all items in the checklists have been satisfied. The checklists are available in Appendix A of the WIAS Site Prep guide.

5. Installation of WIAS and Network Equipment

5.1. Overview

This section of the document highlights the procedures, and timeframes for bringing up elements of the WIAS network. These descriptions are meant to only provide an overview and should be read in conjunction with the appropriate installation manual(s). Included in each section is a brief overview of the process and the approximate time frame to complete installation procedures. Each of the following sub sections are predicated on the site being certified ready for installation.

IMPORTANT - These estimates do NOT include:

- configuring routing protocols (e.g., RIP2).
- configuration of NAT (except for limited cases in firewall configuration).
- configuration of outer router or router filter rules to protect infrastructure.
- configuration of customer's actual user database beyond a few test cases.
- customer billing application or configuration thereof.

5.2. End-user Installation

The WM is modular in design, minimizing installation time and steps. Installation of a WM will follow the general steps outlined below:

1. Identify WM installation site
2. Determine mounting position, based on base station channel selection
3. Install mounting bracket and WM
4. Route cabling and connect WM
5. Test connections
6. Install WIAS software on end-users PC or Router.

These steps will be common to every WM installation. However, unique or unusual circumstances may arise at a subscriber’s premise which could require additional effort.

Physical installation of a WM may take up to several hours. The vast majority of this time will be spent running cable through a subscriber’s home or business. Using more experienced installers will significantly reduce the time spent a subscriber’s site.

Installing WIAS end-user software should take 5-10 minuets, providing no unforeseen circumstances.

5.3. WIAS Base Station

5.3.1. W-hub

The W-hub is modular in design, minimizing installation time and steps. Before installation can begin, the site must be certified ready for installation and a civil works completed. Obtaining this certification prior to installation will help minimize rework and the risk of improper installation.

Installation of a W-hub can be segmented into 2 categories: 1) physical, and 2) configuration. Physical installation of the W-hub includes the following steps:

1. Removing the W-hub from its box
2. Locating mounting bracket and ancillary items
3. Mount W-hub

4. Install wiring
5. Complete connections
6. Fasten I/O access panel and outer cover

A W-hub installation should take approximately 2 days, provided that all of the other elements are in place for the W-hub: E-1 back-haul, civil works, roof access permission, etc..

5.3.2. Access Point

The AP is modular in design, minimizing installation time and steps. Before installation can begin, the site must be certified ready for installation. Obtaining this certification prior to installation will help minimize rework and the risk of improper installation.

AP installation can be broken out into 2 categories: 1) physical, and 2) software. Physical installation of the AP includes the following steps:

1. Removing the AP from its box
2. Locating mounting bracket and bolts
3. Install and fasten AP bracket mounting support
4. Adjusting down tilt angle
5. Fasten AP to bracket
6. Create and test electrical connections
7. Fasten I/O cover
8. Recording MAC address

An AP can be programmed at the W-hub, after insuring a complete physical installation. Programming an AP requires approximately 5 minutes.

Estimated time to complete an AP installation is 2-3 hours, depending on the tower height and proximity to the W-hub. This estimate and the steps outlined above assume site is completed prior to installation and per SOS Internet guidelines, which are detailed in the site preparation guide.

5.4. DSC Components

The Data Switching Center includes several key components of the WIAS network: the server cluster, the inner router, and the LNSs, all connected to one or more Cajun Ethernet hubs. Though not essential to WIAS, other components will normally also be situated at the DSC site, including firewall(s), an outer router, management servers and ISP servers.

SOS Internet is providing installation and configuration services for most of these components, including many of those not part of WIAS.

Prerequisites:
Physical and environmental requirements for the DSC site have been defined in the Site Preparation Document. It is the customer's responsibility to have the DSC site ready and to document any exceptions with the SOS Internet team before installation begins so that installation can proceed successfully and efficiently. In particular, power and power conditioning equipment should be in place and operational. Cable trays, air conditioning, lighting, etc must be in place. The site should be clean and free from heavy construction (i.e., ready to accept electronic equipment). Network design data must complete, at least as far as the DSC components are concerned. This includes definition of the customer's LAN/WAN architecture, determination of frame relay parameters, IP network layout, L2TP tunnel profiles, PPP parameters, etc. All IP addresses, subnets, and netmasks, and frame relay parameters for all WHs and inner routers must be available prior to start of installation.

5.4.1. Server Cluster

The server cluster is one of the most critical pieces of the DSC network. It is essential for programming many components of the WIAS network. It is therefore recommended that the server cluster is installed and configured early in a DSC installation.

Hardware installation includes unpacking all components, assembling all components into the cabinet, making external LAN and power connections, and performing basic hardware tests. This should take about one day.

To fully configure and verify a complete DSC Server Cluster (software only) will take an experienced engineer approximately 3-4 days. Major steps in server configuration include:

1. Update or modify factory installed version of NT as needed.
2. Configure NT networking parameters on each server per network design data. Build and install hosts files per Network Design data. (Steps 1-2 require .5 to 1 days.)
3. Install Oracle Database software.
4. Install and configure Microsoft, Compaq and Oracle clustering SW.
5. Install Oracle Application Server, HP Network Node Manager, and all of the WIAS software databases and applications.
6. Configure cluster resource groups. Verify failover functionality. (Steps 3-6 require 1 day.)
7. Configure NNM with DSC elements and initial WH data. Verify functionality.
8. Create initial (1 or 2) WH configurations for NMS database (~6 hrs). Verify functionality.
9. Create initial user profiles (one "test" user per WH) for SMS database. Verify functionality. (Steps 7-9 require 1 day.)

Estimated time to complete a server cluster installation is 5-6 days, provided that all site preparation and civil works are already completed and the site is certified ready for installation.

5.4.2. Cajun Switches

The hardware installation includes assembling the individual switches from shipped components, installing in cabinets, and making the necessary power and LAN connections. This should take about one day if the cabinets and power are available.

These Ethernet switches can be operated in two modes. The simplest mode requires little beyond the initial hardware installation (setting DIP switches on the P116 and simple auto sense on the P550). This mode will be used initially and until the rest of the DSC is operational. It is therefore recommended to allocate one full day for installation of Cajun switches.

At a later time, additional configuration of the switches is required to support network management and software configurability. For the P116 this involves configuring the NMA module; for the P550 this involves installing CajunView software on an NT server. One additional day is to be allocated for this activity.

The approximate time to install a DSC's Cajun Switches is 3-5 days, provided that all site preparation and civil works are already completed and the site is certified ready for installation.

5.4.3. Back-haul Transmission Network (Ascend BSTDX)

Back-haul transmission network's typically include a number of components (fiber and microwave links, for example) in addition to the Ascend router. These are NOT included in the estimates given in this section. The Ascend router itself requires considerable time to setup since it includes installing and setting up the Sun management platforms (3) as well as the Ascend router.

The hardware installation should take 1 day if the rack and power are available.

Software configuration of the Naviscore System (SUNOS Ascend Management Station) will take 1-2 days each. Each individual Ascend switch will take an experienced engineer anywhere from ½ day to a full day to complete.

Sun configuration activities include:

1. Install/configure SUNOS.
2. Install/configure appropriate Naviscore components on each platform. This varies with platform, since they are used for different management functions.

Router configuration activities include:

1. Upgrade operational software to correct version, if necessary.
2. Configure IP interfaces. This means assigning IP addresses, netmasks, gateways, etc. to each Ethernet. This will include verification of network connectivity via pings from directly connected interfaces on the Ethernet(s).
3. Configure WAN ports. This includes assigning addresses, frame relay parameters.
4. Establishing connectivity with at least one WH over Frame relay to verify the correctness of the E1 and Frame Relay configuration of the Ascend.

Estimated time to install the back-haul transmission network is 4-6 days, provided that all site preparation and civil works are already completed and the site is certified ready for installation.

5.4.4. L2TP/LNS Server (IBM 2216)

The hardware installation of the LNSs should take 1 day if the racks and power are available.

Configuration and setup of an IBM 2216 can take anywhere from ½ day to 1 full day. This number reflects the time for software installation and assumes an already functional/tested hardware installation. Configuration/setup includes the following activities:

1. Upgrade IBM software to latest WIAS compatible load.
2. Configure basic parameters of the router (IP address, users login, routes, etc)
3. Configure global L2TP parameters.
4. Configure tunnel profiles.
5. Configure PPP address pools.
6. Verify connectivity between the LNS and each WH via ping.

Estimated time to complete a LNS installation is 2-3 days, provided that all site preparation and civil works are already completed and the site is certified ready for installation. Note that the 2-3 day estimate does not supporting the installation of the Nways management package.

5.4.5. SOS Internet Managed Firewall

All DSC installation procedures should be completed prior to installing a firewall application. Installing the SOS Internet Managed Firewall also requires a trained technician, in addition to an installed DSC. The following steps outline the recommended procedures when installing a SOS Internet firewall.

1. Brick installation
2. Obtain a valid Install Key from the SOS Internet Security web site
3. SMS installation
4. Configuration and activation of the Brick
5. Security policy installation

1. Position the Brick on the rack and fasten to it. Connect the Security Management Server to the brick using one of the Ethernet interfaces on the back of the brick. Connect the LANs to the Brick keeping a record of the connections. Expected time: 3 hours
2. Register the Bricks and obtain a valid installation key from the SOS Internet Security web site. Expected time: 30 minutes.
3. Installing the SMS Software (Windows NT). The PC must have installed Microsoft Windows NT Server or Workstation 4.0 with NTFS file system. It takes 1 hour to install it with a basic configuration.
    3.1. Install Service Pack 3
    3.2. Install Netscape Communicator
    3.3. Install Netscape Enterprise Server
    3.4. Modify the configuration of the installer Account
    3.5. Install the Security Management Server
    3.6. Install Adobe Acrobat Reader

Expected time to complete steps 1-3 is 3 hours.

4. Configuration and activation of the brick
    4.1. Configure a Brick
    4.2. Activate a Brick

Expected time to complete step 4 is 30 minutes

5. Security policy installation
    5.1. Define Security Zones
    5.2. Assign the Security Zones to the interfaces
    5.3. Install Security policies on each Zone
    5.4. Test

Total Expected time to install SOS Internet Managed Firewall: 2 – 4 days

These installation times do not account for ordinary delays or unforeseen circumstances. Expected installation times also assume a DSC installed and in good working order.

6. Acronym List

AP	**A**ccess **P**oint
CTSO	**C**ustomer **T**echnical **S**ervice **O**rganization
CSU	**C**ustomer **S**ubscriber **U**nit
DSU	**D**ata **S**ubscriber **U**nit
DBS	**D**ata **B**ase **S**tation
DSC	**D**ata **S**witching **C**enter
FTP	**F**ile **T**ransfer **P**rotocol
GHz	**G**iga **H**ertz (10^9 Hz)
GUI	**G**raphical **U**ser **I**nterface
HDD	**H**ome **D**omain **D**irectory
IP	**I**nternet **P**rotocol
IPsec	**Sec**urity extensions to **IP**
ISP	**I**nternet **S**ervice **P**rovider
IWF	**I**nter**W**orking **F**unction
L2TP	**L**ayer **2** **T**unneling **P**rotocol
LCS	**L**ocal **C**ountry **S**upport
LNS	**L2TP** **N**etwork **S**erver
WIAS	**SOS** **I**nternet **T**echnologies **W**ireless **I**nternet **A**ccess
MAC	**M**edia **A**ccess **C**ontrol
Mbps	**M**ega **b**its **p**er **s**econd (10^6 bits/sec)
MIB	**M**anagement **I**nformation **B**ase
MHz	**M**ega **H**ertz (10^6 Hz)
PC	**P**ersonal **C**omputer
PPP	**P**oint to **P**oint **P**rotocol
PVC	**P**rivate **V**irtual **C**ircuit
RADIUS	**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice
RAS	**R**emote **A**ccess **S**erver
RF	**R**adio **F**requency
RLP	**R**adio **L**ink **P**rotocol
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol
TCP	**T**ransport **C**ontrol **P**rotocol
TMN	**T**elecommunications **M**anaged **N**etwork
UDP	**U**ser **D**atagram **P**rotocol
UPS	**U**ninterruptible **P**ower **S**upply
UNI	**U**niversal **N**etwork **I**nterface
VPN	**V**irtual **P**rivate **N**etwork
W-hub	**W**ireless **H**ub
WM	**W**ireless **M**odem