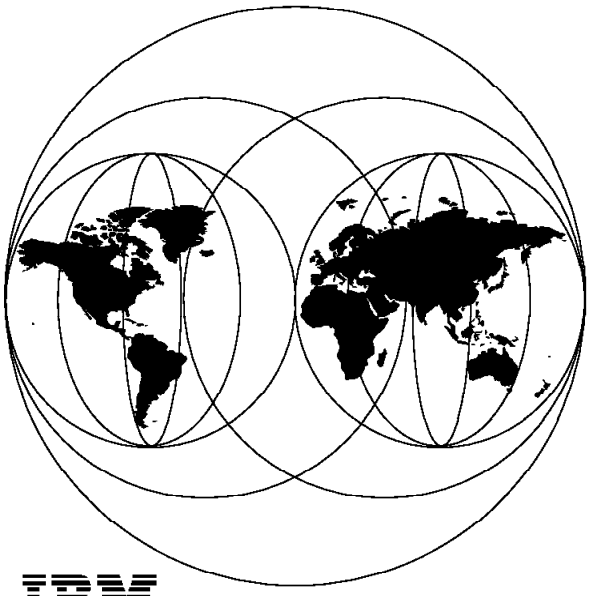
International Technical Support Organization

SG24-4466-00

Wireless LAN Communications

January 1996



IBM

International Technical Support Organization
Raleigh Center

International Technical Support Organization

SG24-4466-00

Wireless LAN Communications

January 1996

Take Note!

Before using this information and the product it supports, be sure to read the general information under “Special Notices” on page xiii.

First Edition (January 1996)

This edition applies to two IBM Wireless LAN communications products, with practical information for the installation and customization of these.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

An ITSO Technical Bulletin Evaluation Form for reader's feedback appears facing Chapter 1. If the form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

Abstract

This document presents an overview of two IBM wireless LAN products, IBM Wireless LAN Entry and IBM Wireless LAN, and the technology they use for wireless communications. The information provided includes product descriptions, features and functions. Some known product limitations as well as a cross-product comparison are included to assist the reader in understanding where and which product to use for given circumstances. Also documented are examples of product setup, configuration and the development of various scenarios conducted by the authors.

Our intended audience is customers, network planners, network administrators and system specialists who have a need to evaluate, implement and maintain wireless networks. A basic understanding of LAN communications terminology and familiarity with common IBM and industry network products and tools is assumed.

(147 pages)

Contents

Figures

Tables

Special Notices

This publication is intended to help IBM customers, systems specialists, network planners and programmers to understand the wireless technologies being used to implement new communications and applications. The information in this publication is not intended to be a specification for any programming interfaces that are provided by any IBM wireless products. See the publications section of the IBM Programming Announcement for IBM Wireless LAN, AS/400 Wireless LAN Access Points, and Portable Transaction Computers for AS/400 Wireless Networking for more information about which publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe on any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AS/400	IBM
NetView	OS/2
PCradio	Person to Person
Person to Person/2	PS/2
ThinkPad	

The following terms are trademarks of other companies:

Windows is a trademark of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

C-bus is a trademark of Corollary, Inc.

IPX	Novell, Incorporated
LANtastic	Artisoft, Incorporated
Mobitex	Televerket
Motorola	Motorola, Incorporated
NDIS	3Com Corporation and Microsoft Corporation
NetWare	Novell, Incorporated
Novell	Novell, Incorporated
PCMCIA	Personal Computer Memory Card International Association

Other trademarks are trademarks of their respective companies.

Preface

This document is not a product manual but it does have a product focus. The intent is to assist the reader in understanding the similarities and differences between specific IBM wireless products as they exist today.

The document provides very general information on wireless networking with applicable emphasis on areas which apply to the products surveyed.

For those new to wireless technology, the depth of the information presented should be sufficient to give a clear understanding of how it is being utilized by these products without the risk of being overwhelmed by a wave of new terminology, acronyms and design philosophies.

During the creation of this document, the authors found that some duplication of content was necessary. This was our attempt to keep each product chapter as a self-contained unit without requiring the reader to skip backwards and forwards for reference material that may be common to the individual products discussed.

How This Document Is Organized

The document is organized as follows:

- Chapter 1, “Overview of Wireless Communication”

  An overview of wireless communication technology is presented. Use this chapter to become familiar with the terminology of wireless technology that is frequently referred to in our book.

- Chapter 2, “ IBM Wireless Products”

  A short review and comparison of IBM Wireless products are offered. We introduce the products that will be discussed in our book and their features and functions.

- Chapter 3, “ IBM Wireless LAN Entry”

  A detailed look at IBM Wireless LAN Entry is revealed along with helpful comments and tips about our early experiences with the product prior to general availability.

- Chapter 4, “IBM Wireless LAN”

  We look at the IBM Wireless LAN from the vantage point of a new user and annotate the results of our work with it. Sample results and useful scenarios are shown.

Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this document.

- *IBM Wireless LAN Entry Network Planning Guide*, GA27-4983
- *IBM Wireless LAN Entry User's Guide* (shipped with product)
- *8227 IBM Wireless LAN Entry Access Point User's Guide* (shipped with product)

- *IBM Wireless LAN, Designing Your Network*, GA33-0189
- *IBM Wireless LAN, Installing and Operating Your Network* (shipped with product)
- *IEEE 802 Plenary 802.11 Documents, Draft*
- *Wireless LAN Design Alternatives*, by Bantz and Bauchot, IEEE Network, March/April 1994
- *IBM Wireless RF LAN Design and Architecture* by Lanne and Bauchot. *IBM Systems Journal, Vol. 34, No. 3, 1995* (order reprint G321-5574)

International Technical Support Organization Publications

- *An Introduction to Wireless Technology*, SG24-4465

A complete list of International Technical Support Organization publications, known as redbooks, with a brief description of each, may be found in:

Bibliography of International Technical Support Organization Technical Bulletins, GG24-3070.

To get a catalog of ITSO redbooks, VNET users may type:

```
TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
```

A listing of all redbooks, sorted by category, may also be found on MKTTOOLS as ITSOCAT TXT. This package is updated monthly.

How to Order ITSO Technical Publications

IBM employees in the USA may order ITSO books and CD-ROMs using PUBORDER. Customers in the USA may order by calling 1-800-879-2755 or by faxing 1-800-445-9269. Most major credit cards are accepted. Outside the USA, customers should contact their local IBM office. For guidance on ordering, send a PROFS note to BOOKSHOP at DKIBMVM1 or E-mail to bookshop@dk.ibm.com.

Customers may order hardcopy ITSO books individually or in customized sets, called BOFs, which relate to specific functions of interest. IBM employees and customers may also order ITSO books in online format on CD-ROM collections, which contain books on a variety of products.

ITSO Redbooks on the World Wide Web (WWW)

Internet users may find information about redbooks on the ITSO World Wide Web home page. To access the ITSO Web pages, point your Web browser to the following URL:

```
http://www.redbooks.ibm.com/redbooks
```

IBM employees may access LIST3820s of redbooks as well. The internal Redbooks home page may be found at the following URL:

```
http://w3.itsc.pok.ibm.com/redbooks/redbooks.html
```

Acknowledgements

This publication is the result of a project conducted at the International Technical Support Organization, Raleigh Center. The project leader and technical advisor for this work was:

Mark DeCain
International Technical Support Organization, Raleigh Center

The authors of this document are:

Toyoki Matsumura
IBM Japan

Steve Shaw
IBM Australia

Thanks to the following people for the invaluable advice and guidance provided in the production of this document:

Derek Jones
IBM UK

Special thanks to the following members of the IBM Wireless LAN Entry development team for their patience and assistance with the scenarios for IBM Wireless LAN Entry.

Sam Henderson
Bill Nunnery
Ralph Yeager

IBM Research Triangle Park, NC

We express our sincere gratitude to the following people for permission to use portions of their material and for their advice and support in the creation of this work.

Frederic Bauchot
Fabien Lanne
Francois Le Maut

IBM LaGaude, France

Our editing team provided us with many hours of help and we wish to acknowledge their contribution:

Martha DeCain
Gray Heffner
Linda Robinson
Gail Wojton

International Technical Support Organization, Raleigh Center

Chapter 1. Overview of Wireless Communication

This chapter presents an overview of the wireless technologies in use today which have been developed specifically for or modified to allow communication between mobile or at least portable data handling devices other than radio transceivers. A data handling device could be any size computer, but in the mobile environment it generally refers to a personal computer of the laptop or notebook size. It also includes the newer breed of hand-held devices known generically as Personal Digital Assistants (PDAs). The distinction between a PDA and a mobile phone is becoming blurred as the technology progresses and phones take on the functions of a PDA and vice versa. It is only a matter of time before this distinction disappears altogether. Indeed, this has all but happened in the case of GSM phones.

For greater detail on any of the topics presented here, please refer to *An Introduction to Wireless Technology*, SG24-4465.

1.1 The Electromagnetic Spectrum

The electromagnetic spectrum has often been divided up, somewhat arbitrarily, by wavelength; the divisions have been assigned familiar names like VHF (very high frequency), microwave and infrared. See Figure 1.

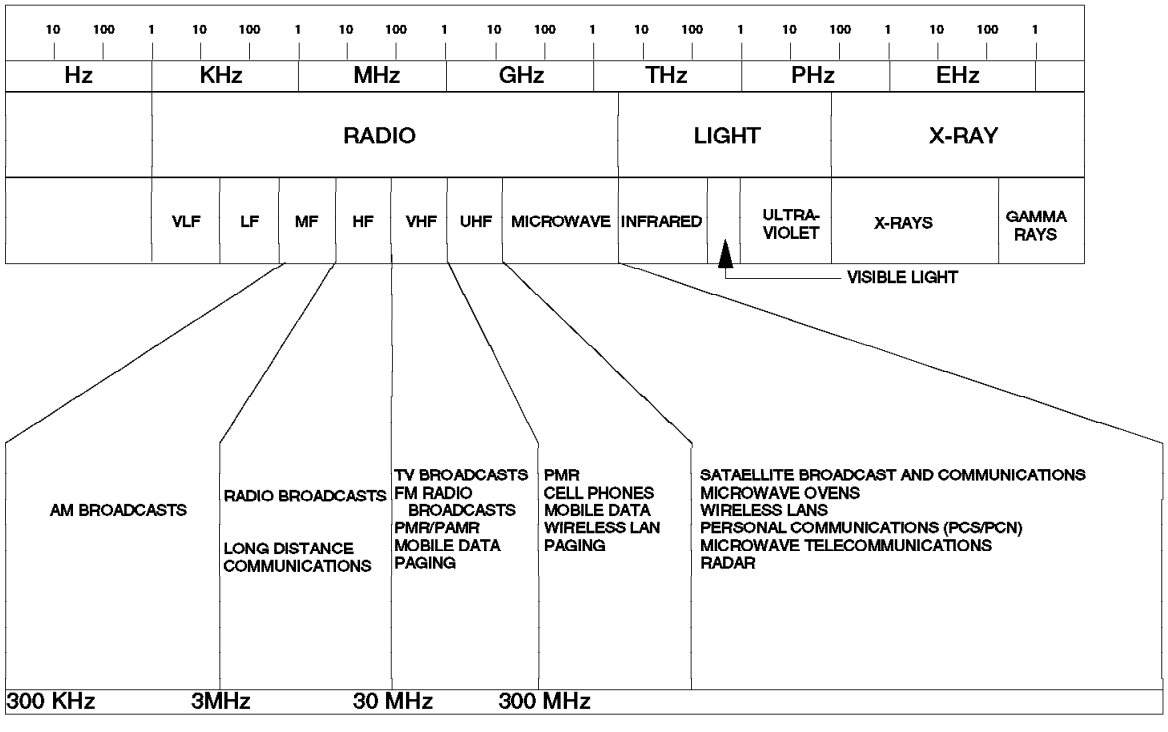


Figure 1. The Electromagnetic Spectrum. The divisions indicated here are not absolute. Other representations of the spectrum may show the divisions at slightly different wavelengths.

Superimposed upon some of these divisions are legacy names from the early days of radio (for example, short wave and long wave which refer to the particular region of the spectrum to which the radio transceiver is tuned).

Over the years uses have been found for every portion of the spectrum to the extent that every country has had to impose some form of licensing or regulation on users of transmitting devices. The uncontrolled use of spectrum leads to chaotic communications which in turn leads to potential life-threatening situations, where emergency messages cannot be received due to interference from other users on the same frequency. Less dramatic, but very damaging, would be the impact on business and human existence if radio communication could not be relied upon.

In some industrialized countries, the spectrum has been over-subscribed to such an extent that there is now an acute shortage of frequencies available for further exploitation. In the US, for example, there has recently been an auction of some under-utilized frequencies. A successful bidder for any of these frequencies has the exclusive right to build devices or services using them.

Internationally, there is a move to standardize the use of specific frequency ranges for particular applications. However, due to the adhoc nature of the way spectrum has been used in the past, this is no simple task. One successful allocation, however, has been in the ISM (Industrial, Scientific and Medical) bands. There are in fact three ISM bands, but only the middle band from 2.4 to 2.48 GHz is available worldwide for exploitation by wireless systems such as LANs.

These bands require no licensing, and the middle band in particular is widely used by different devices. Many consumer devices are found in these bands, including such things as baby monitors and garage door openers. The most familiar usage of this band is for microwave ovens. It is also proving very popular with wireless LAN developers. In the latter case, a special transmission technique must be used to minimize the interference with similar devices in the vicinity. The technique described later in this chapter is known as a *spread spectrum*.

1.1.1 Frequency and Wavelength

An energy wave of a particular frequency will have certain physical characteristics. For instance, a radio wave below about 900 MHz will be able to propagate well through walls and floors and be generally able to penetrate buildings. Broadcast radio between about 1600 kHz (AM) and 108 MHz (FM) are good examples of this. Frequency(f) and wavelength(lambda) are related to each other and to the speed of light by the following expression:

$$f \times \lambda = 3 \times 10^{\bullet}$$

where f is measured in cycles per second or Hertz (Hz)
lambda is measured in meters
the speed of light is measured in meters per second

It can be seen from this expression that since the speed of light is constant, if the frequency increases, the wavelength must decrease proportionally. Frequency and wavelength are said to be in inverse proportion to one another. These characteristics are important when considering radio or wireless technologies of any kind. For example, the shorter the wavelength, the more the

signal is attenuated by the air and the particles in it. This is why FM broadcasts tend to be localized, while AM broadcasts can be received over much greater distances at the same transmit power.

As the wavelength becomes shorter, the wave takes on more of the properties or characteristics of light. It is more easily absorbed by most materials, and so it attenuates quickly. The shorter the wavelength, the more pronounced the effect. However, light-like properties can be extremely useful to a wireless developer. Generally, the shorter the wavelength, the easier it is for the wave to be reflected, focused and generally controlled. A signal with a frequency greater than about 300 MHz can be focused using a parabolic reflector which is the familiar *dish* antenna seen at TV stations, on building roofs and even in domestic gardens. Focusing a signal in this manner and directing it towards a destination means the transmitting device needs far less power than if it were transmitting in all directions. Focusing an incoming signal with the same antenna means that a far weaker signal can be detected than with a conventional antenna.

1.2 Wide Area Cellular Networks

Cellular networks are now commonplace throughout the world alongside conventional wired networks. Some countries are electing to install cellular networks, in preference to wireline networks, in regions which have previously not had a telephone service.

Many people are familiar with the cellular phone; it is for voice transmission that these networks were developed.

1.2.1 Analog Voice Services

The basic design element of an analog service network is that of a cell, which consists of a base station and a number of mobile devices which it controls. To cover a larger geographic area without raising output power levels means distributing more base stations and hence creating more cells. This has the additional benefit of increasing channel reuse and therefore overall capacity. With the proper controls, users can roam between these cells without suffering a break in communication.

There is no worldwide standard for such cellular systems, but certain implementations do dominate. In the US, Canada and Japan, AMPS (Advanced Mobile Telephone System) is prevalent. In many European countries, TACS (Total Access Control System) and NMT (Nordic Mobile Telephone) are widely distributed although some countries, France, Germany and Italy for example, use a system specific to each country.

The AMPS, TACS, and NMT systems share some common features (apart from all being analog services). They all utilize either the 450, 800 or 900 MHz band depending on which country they are operating in and which band has been allocated. They all use FM (Frequency Modulation) and FDMA (Frequency Division Multiple Access) as their means of voice transmission.

It is possible to use these voice networks to send data. However, this is not generally desirable from an end user point of view. The main reasons for this are as follows:

- **Cost**

These are connection-oriented services which means that the user is paying for the entire connection period. Cellular phone charges are generally much higher than conventional PSTN (Public Switched Telephone Network) charges. The data rate can be up to 19.2 Kbps, but even at this speed a large file transfer would require a long connect time and high cost.

- **Reliability**

  These services were designed specifically for voice transmission, and absolute accuracy was not a consideration. The human ear is very tolerant when it comes to conversation. It can miss complete words and even sentences and yet still be able to infer what the missing pieces were with remarkable accuracy. Humans can maintain conversations over extremely bad communication lines.

  A data transmission is far less forgiving. Breaks in communication mean data has to be retransmitted which adds to the cost of the connect time. The receiving application may not be aware that it has missing data, so the end result may be incomplete. Noise on the channel may be interpreted as data and accepted, thereby corrupting the actual data.

  These are very real effects in an environment where a user may be moving into and out of areas of poor radio reception.

1.2.2 Digital Voice Services

A digital service network shares a similar design philosophy with an analog one in that there are a number of base stations controlling mobile users within the cells. As with analog services, there is no worldwide standard for a digital service. However, a widely accepted standard today is GSM (Global System for Mobile communication).

GSM operating in the 900 MHz range is now firmly entrenched throughout Europe and is the digital cellular standard there. A product which came out of the same development effort is DCS 1800 (Digital Cellular System 1800) which is also implemented in Europe but not to the same extent as GSM. It operates at 1800 MHz, hence the name, but otherwise it is essentially the same technology as GSM. Users on either system are able to share the infrastructure of both networks because of this similarity.

The US rival to GSM is DAMPS (Digital Advanced Mobile Phone Service) which, due to the extreme lack of frequency available there, must share the same band of 800 MHz as the AMPS analog service. In Japan, JDC (Japan Digital Cellular) is the available phone service. There is, at present, no shortage of spectrum in Japan, so JDC has the luxury of operating in three pairs of bands with distinctly separate uplink (mobile to base) and downlink (base to mobile) sub-bands as follows:

- 810 - 826 MHz downlink
- 940 - 956 MHz uplink
- 1429 - 1441 MHz downlink
- 1447 - 1489 MHz uplink
- 1453 - 1465 MHz downlink
- 1501 - 1513 MHz uplink

Digital systems are designed to eliminate some of the shortcomings of the analog networks as follows:

- **Efficiency**

  An analog conversation ties up the entire frequency channel for the duration of the conversation. Much of the time is *dead time* such as the spaces between words, pausing for breath and thinking time. A digital system can use this dead time for other conversations at the same frequency using the time-slicing technique of TDMA (Time Division Multiple Access).

  Digital technology allows speech to be compressed prior to transmission thereby permitting even more users per channel. GSM, for instance, can support eight conversations in the same bandwidth where analog technology will only support one.

- **Quality**

  A digital data stream can have error correction built in so that short breaks in communication and spurious noise on the channel can be largely overcome.

- **Security**

  Using TDMA as a transmission protocol makes the conversation very difficult to monitor and follow. Specialized equipment is required to do this.

On a reliability basis alone, digital cellular services hold more promise as a means of transmitting data than analog cellular services. It is still a connection-oriented service and there is still a connect time charge to be paid. However, the channel can be shared by up to eight users concurrently, and tariffing should be more reasonable.

Note: IBM's ARTour wireless product supports the GSM interface.

1.2.3 Packet Data Services

These networks were designed specifically for carrying data with no provision being made for voice traffic. As the name suggests they are packet data networks for the radio environment. Of the three services mentioned here, Mobitex and RD-LAP were designed to support mobile data services and in this capacity can be used by devices mounted in vehicles.

There is no worldwide standard for this technology and no common frequency on which to operate. However, Mobitex and RD-LAP are the two main services around which the world seems to be polarizing. A third and upcoming contender is CDPD.

- **Mobitex**

  This was developed by Ericsson Mobile Communications AB of Sweden and began operating commercially in 1986. Since then it has experienced a number of enhancements and is now implemented widely across Europe and the US. In the US it operates in the ranges of:

  – 935 - 940 MHz downlink

  – 896 - 901 MHz uplink

  In Europe the ranges vary by country, but all are within the range:

  – 425 - 459 MHz

  Mobitex has also been implemented in Australia and a number of South East Asian countries. The maximum data rate on a Mobitex network is 8.4 Kbps, but the actual throughput is closer to 8 Kbps.

- **RD-LAP**

  RD-LAP is the name given to the radio protocol which runs on a network developed by Motorola (with some input from IBM in the earlier stages). In the US, this network is known as ARDIS (Advanced Radio Data Information System) where it operates in the ranges of:

  – 851 - 869 MHz downlink

  – 806 - 824 MHz uplink

  Like Mobitex, it has been implemented in many parts of the world where it is known by various names. In Germany, for example, it is Modacom; in Australia it is Datatac.

  The data rate is 19.2 Kbps which gives an actual throughput of about 14.4 Kbps. An earlier protocol called MDC4800 (Mobile Data Communication 4800) is still used by some services on ARDIS, and as its name suggests it has a data rate of 4.8 Kbps. Both protocols, however, use exactly the same infrastructure.

The previous two radio networks have been developed independently of X.25, but they do resemble an X.25 network somewhat in their packet handling.

They have the same cell structure as the voice networks in that they have multiple base stations controlling mobile devices within their cells. The base stations then connect via landline (such as an X.25 network to a user's home network) where the user then has access to whatever applications that normally reside there.

Note: IBM's ARTour product supports both the Mobitex and RD-LAP interfaces.

- **Cellular Digital Packet Data (CDPD)**

  The CDPD service (originally Celluplan II) was initially developed in the US at IBM Boca Raton, with the following objectives:

  – To provide a digital packet (connectionless) network, able to transmit data reliably and cheaply

  – To use the same frequency allocation as the existing AMPS network without impacting the voice carrying capacity or conversations in any way

  – To utilize the dead time on channels in the AMPS network to transmit data packets

  – To use the existing AMPS network infrastructure

  The way CDPD works is to constantly monitor the existing AMPS channels for activity. When it has data to send, it selects the first available free channel and begins to transmit. It will continue to use this channel as long as it is not required to provide a voice call by the analog network.

  If the channel is required to provide a voice call, CDPD will cease to transmit on that channel immediately and will begin to scan the channels again until it finds another one free. At this point, it will switch to the free channel and continue its transmission. These breaks will not affect the integrity of the data being sent, and providing the break is not of a duration such that the receiving application times-out while waiting for some response, the data will arrive intact.

Considering that the amount of dead time, which has been shown to be as high as 50% on even the busiest of analog networks, such time-outs are likely to be rare.

So far, CDPD has only been implemented in the US, where it appears to be seeing some success. It is currently being offered by at least six carriers. Whether other countries choose to follow suit remains to be seen.

1.3 Wireless LANs

Wireless LANs and wired LANs operate in much the same way at the physical level. That is, they both use electrical energy to transmit data. One encodes its data upon an electrical impulse in a wire, and the other encodes it upon a radio or light wave.

With a waveform, the amount of data which can be transmitted is theoretically, directly proportional to the frequency of the wave. For example, if a particular piece of switching equipment in a transmitter is capable of encoding (modulating) one bit of data per cycle, then a wavelength with a frequency of 10 kHz (ten thousand cycles per second) is going to carry ten times as much data as a wavelength having a frequency of 1 kHz in the same period of time. This holds true for as long as the switching equipment can match the frequency.

Some modulating methods make it possible to encode up to 4 bits on a single cycle. Considering this and the high frequencies available, wireless LANs have the potential to transmit data at very high speeds.

As already mentioned, the characteristics of a wave change with respect to the rate of frequency change. The higher the frequency, the more the wave takes on the properties of light and the more it is absorbed or reflected. This has a number of implications; the main one being the fact that as the frequency increases the range of the LAN decreases due to the greater attenuation of the signal. Also, the equipment used to transmit and receive radio waves begins to strike some physical limitations as the frequency increases, so there is an upper limit to its practical application.

There is a wide frequency range which could potentially be used for wireless LAN communication. The range from about 200 kHz, through the microwave range, all the way up to the top of the infrared range at around 200 THz could be utilized. When selecting a range upon which to build equipment, consideration must be given to the required throughput versus transmission range. As one increases, the other decreases as mentioned previously. Greater range can be achieved at any frequency by increasing the transmission power. However, most governments impose strict controls on power output through their licensing and regulatory authorities. A more efficient antenna or a directional one can increase the range of any transmission, but this is nowhere near as significant a gain as simply increasing the power.

The choice of frequency range, however, has largely been limited by regulation. The same frequency shortages that occur, at these higher regions also occur lower down in the spectrum. Most frequencies need to be licensed, which adds to the cost of the technology. In fact, practically all wireless LAN development has gone into supporting a limited number of specific bands in the microwave and infrared regions. These bands have been identified (in some countries at least) for specific purposes and have no licensing requirement. However, there

are tight controls on permitted power output which effectively limits the range to a maximum of 400 meters.

Apart from the health consideration, this limitation attempts to reduce the amount of interference that would otherwise be experienced by different organizations employing the same technology in close proximity to each other.

1.3.1 Microwave LANs

In the US three bands have been reserved for ISM (Industrial, Medical and Scientific) use and require no licensing, but the restrictions, as mentioned above, do apply. A further restriction is that radio devices using these bands must employ a spread spectrum technique to further reduce the possibility of interference with other users. The first is in the UHF (ultra high frequency) band and the other two are in the microwave region. The frequencies of these bands are:

- 902 - 928 MHz
- 2.4 - 2.48 GHz
- 5.7 - 5.85 GHz

Other countries have recognized some or all of these designations, but only the 2.4 GHz band has been recognized internationally. In France and Japan (notable exceptions) only a subset of the 2.4 GHz ISM band is available.

Today, wireless LAN vendors must decide whether to build and support more than one range of equipment to cover multiple bands or to stick to the one band internationally available. An international traveler should be aware that a device which supports the 902 MHz or 5.8 GHz specification may not be legal in all countries. With the 2.4 GHz specification there is less cause for concern.

One of the drawbacks with using the ISM band is that other devices besides the radio have been built to the same specification. The most widely known of these would be the microwave oven. These can have an undesirable effect on nearby radio transmissions. However, commonplace machinery like generators, welding equipment and transformers can all produce frequencies in this range. Operating a wireless LAN in these areas pose unique design considerations to overcome strong radiators.

Note: The IBM Wireless LAN Entry and IBM Wireless LAN products both operate in the 2.4 GHz band.

1.3.2 Infrared LANs

The infrared portion of the spectrum is used successfully in a number of familiar domestic devices. Infrared heating lamps use the lower end or the infrared band. The rest of the band is utilized for things like television remote controls, motion detectors and door openers.

From a wireless point of view, light has the potential for very high transmission rates; the present technology already approaches that of wired LANs such as a token-ring at 16 Mbps. As with the ISM bands there are no licensing requirements for infrared use, but there are controls nonetheless. Transmitters are only allowed to operate at fractions of a watt, and the maximum range which can be achieved is about 20 meters. A great deal of infrared energy arrives at the surface of the earth from the sun. This precludes an infrared LAN from being used outdoors. This is in contrast to microwave LANs which are unaffected by

sunlight and are frequently employed in outdoor applications. Infrared signals tend to reflect off walls and ceilings, a characteristic which can be taken advantage of in a *diffused* design.

Infrared transmitters can be constructed with either a laser diode (LD) or a light emitting diode (LED). Both have their advantages and disadvantages and tend to find specific uses.

LDs are used in a line-of-sight placement, where a device needs to communicate with one other. The devices need to be precisely aligned for communication to take place. This is called *focused* infrared.

LEDs produce a spread of light rather than a beam and so lend themselves to transmission by diffusion. This is where the beam is transmitted over a wide angle. It may be reflected off multiple surfaces before being picked up by the receiver. When this happens, the same signal can arrive at the receiver from different directions and at slightly different times which is known as the multi-path effect. It is this same effect which produces the phenomenon of *ghosting* on a television set.

However, one advantage of being *surrounded by signal* is that workstations have the ability to move around the local area without losing contact with the base. In addition, where the LAN topology supports it, roaming can occur.

The multi-path effect can be overcome somewhat by a technique known as quasi-diffuse transmission. This is where the transmitters and receivers are all directed towards a particular spot on the ceiling known as a *satellite*. Instead of a diffuse spread, a focused beam is directed at the satellite from the transmitter. The reflected signal is then detected only once by all the receivers.

Note: The IBM Infrared Wireless LAN product is IBM′s offering in the infrared LAN arena.

1.4 LAN Access Methods

When a radio transmission is limited to one particular frequency, for example a radio broadcast, this is known as a narrow band transmission. When a band with a large frequency spread has been allocated, the transmission using it is known as a broad band transmission.

Broad band transmission can be either FDMA (Frequency Division Multiple Access) or spread spectrum. Spread spectrum techniques can be either CDMA (Code Division Multiple Access), Direct Sequence (DS) or frequency hopping (FH). Frequency hopping in its turn can use CSMA (Carrier Sense Multiple Access) or TDMA (Time Division Multiple Access) access methods. These last two techniques are equally applicable to narrow band transmissions if multiple stations wish to share the same frequency. The following list summarizes these techniques:

- Narrow band
  - TDMA
  - CSMA
- Broad band
  - FDMA

- Spread spectrum
  - CDMA
  - Frequency hopping
    - TDMA
    - CSMA
  - Direct sequence

1.4.1 TDMA

Time Division Multiple Access is a deterministic method of sharing a channel resource between multiple users on a *time-slice* basis. It follows the same philosophy as a token-ring in the wired LAN world. With TDMA, each station is allocated a time slot of a particular duration in which it can transmit data. If it has no data to send, the slot is allocated to another station. The actual allocation of time slots can be dynamic; that is, on a demand-priority basis.

Because a station only needs to listen at assigned times, there is a power saving potential for the device in question. TDMA tends to use bandwidth very efficiently and can handle isochronous data, such as video, in a very predictable manner. It also has the ability to prioritize data from particular stations.

TDMA is a technique equally applicable to wired and wireless LANs and also in wide area wireless where it is used in the GSM and CDPD technologies.

1.4.2 CSMA

Carrier Sense Multiple Access is a contention-based system and, as a design philosophy, shares a common ancestry with the Ethernet LAN. Indeed, the chip sets in common usage in wireless LANs are frequently the same as those used in wired LANs.

CSMA depends upon each station listening to an allocated channel when it has data to send, and if the channel happens to be free, it then transmits. This is also known as *Listen Before Talk* or *LBT*. If another station has done the same thing, then a collision occurs and both stations must retransmit but at different times. A *random backoff algorithm* is invoked on each station to ensure that they do not attempt a second transmission at the same time.

A wired LAN uses CD (collision detection) to determine whether a packet was sent successfully or not. In a wireless LAN, a station has no way of detecting a collision, so CA (collision avoidance) is implemented instead.

1.4.3 FDMA

FDM, also known as Frequency Division Multiplexing, is a broad band method of transmitting multiple signals concurrently over very closely spaced frequencies within a given band. It is the technique used by cable television to transmit multiple programs over the same piece of wire. It works equally well using microwaves as the carrier, and it could be utilized over a large range of the spectrum.

Its success depends upon the receiving station being able to detect and lock on to the desired frequency.

1.4.4 Spread Spectrum

Spread spectrum techniques spread a transmission over multiple available frequencies within a given band. Simply stated, the goal is to have a low watts-to-hertz ratio. Usage of the ISM bands for radio transmission of any kind demands that one of the two spread spectrum techniques be employed. The technology has been around for some 40 years and was originally developed in the US for military use.

In this environment, spread spectrum provides good protection against *channel jamming* and *intentional eavesdropping* by unfriendly elements. In the business environment it offers protection from radio interference and casual eavesdropping.

1.4.4.1 CDMA

This spread spectrum technique uses DS (Direct Sequencing) to artificially spread the signal over a greater range of frequencies than it would actually need if it were transmitting user data alone. Multiple user data streams can be transmitted concurrently over exactly the same spread of frequencies.

The factor which distinguishes one data stream from another is the additional *pseudo-random bit stream* with which it is combined. Every random bit stream is unique, which in turn makes every user data stream unique. Only the sending and receiving stations of a particular bit stream know what the random pattern is. The receiving station strips off the random bits and the user data remains.

This technique makes a transmission relatively insensitive to the effects of background noise even when that noise is at quite high levels.

1.4.4.2 Frequency Hopping

Frequency hopping is another spread spectrum technique which divides up the available bandwidth into a number of discrete channels. A transmission is synchronized between the sending and receiving stations such that they switch channels or *hop* in a *pseudo-random* pattern. Transmission will recommence on every channel that is hopped to.

Note: Either CSMA or TDMA can be used for channel access.

The technology distinguishes between FH (fast hopping) and SH (slow hopping) with SH being by far the most widely implemented. The stipulation with SH is that hopping must occur at least every 400 ms and must cover all available channels.

Chapter 2. IBM Wireless Products

IBM has developed wireless solutions for a variety of communication environments.[1] IBM Wireless LAN Entry, IBM Wireless LAN and IBM Infrared Wireless LAN, are designed for the local area network environment and support various IBM, OEM and industry standard communication protocols.

Three further products, RadioPAC/400, PagerPAC/400 and ARTour are designed for the wide area network environment. These provide communication between a wireless enabled device and a remote host. They depend upon a third party network provider to supply the wide area networking infrastructure.

Yet another product, AS/400 Wireless LAN, is also designed for the local area network environment and is host-based. IBM products with wireless capability are listed below.

Note: Only the IBM Wireless LAN and IBM Wireless LAN Entry products are dealt with in this document.

2.1 IBM Wireless Products

1. The following are local area network products:

   a. IBM Wireless LAN Entry:

      - It supports point-to-point communication between workstations in the same cell.
      - It supports communication with workstations in other cells when the cells are Ethernet LAN connected.
      - It supports seamless roaming between cells which are Ethernet connected.
      - It uses CSMA/CA as a transmission protocol.

        To connect a cell to a LAN, an IBM Wireless LAN Entry Access Point is required. The IBM Wireless LAN Entry Access Point acts as a MAC level bridge between the client devices in the cell and the Ethernet LAN.

        Note: IBM provides both the software and the wireless LAN adapters.

   b. IBM Wireless LAN:

      - It supports communication between devices in the same cell via a workstation configured as a base station.
      - It supports communication with devices in other cells or on a traditional LAN where the base stations for these cells communicate across a shared-media network.

        The base station can be both a MAC level bridge and a router, which allows communication between the client devices and other hosts or workstations on the LAN.

[1] Some products mentioned here may not have been announced or homologated in every country.

- It uses spread spectrum frequency hopping (SSFH) at the physical layer with a hybrid TDMA/CSMA transmission technique for the MAC layer. This results in a high level of throughput while providing a high level of security and access priority.

  Note: IBM provides both the software and the wireless LAN adapters.

c. IBM Infrared Wireless LAN:

- It is designed for indoor, short range operation only.
- It uses spread spectrum CSMA/CA as a transmission protocol.
- It supports point-to-point communication between workstations in the same cell.
- It supports roaming between LAN connected cells.
- It supports bridging to token-ring and Ethernet via an Access Point.

  An Access Point is a workstation with both wireless and wired LAN adapters. It is configured as a bridge between the two environments.

  Note: IBM provides both the software and the wireless LAN adapters.

d. AS/400 Wireless LAN:

- It connects PCs and dedicated data collection devices to an AS/400 system.
- It uses spread spectrum direct sequence as a transmission protocol.

  Mobile devices are Portable Transaction Computers (PTCs) which appear to the AS/400 host as 5250 terminals. This allows the PTCs access to applications and functions residing on the AS/400.

  Note: IBM provides both the software and the wireless LAN adapters.

2. The following are wide area network products:

a. RadioPAC/400

- It uses the AS/400 as a communications hub.
- It supports public and private radio frequency data networks.
- It provides two-way wireless communication between radio-enabled devices such as laptop and notebook computers.

b. PagerPAC/400

- It uses the AS/400 as a communications hub.
- It provides a one-way paging function via a public or private paging service.

c. ARTour

- It supports TCP/IP applications over a WAN using a carrier network.
- It supports GSM, RD-LAP (Motorola), Mobitex (Ericsson) and Inmarsat (satellite communication) radio interfaces.

  Note: A 3270/5250 Emulation application is available for access to host based applications.

Note: IBM provides the software. IBM also provides wireless LAN adapters to support the Mobitex and RD-LAP interfaces.

2.2 PC Wireless LAN Product Overview

IBM now supports a number of products which cater to the expanding Wireless LAN market. Although some of these products share common functions and features, there are differences in capability which makes each suitable to different areas of deployment.

These wireless LAN products are enabling technologies. Their fundamental purpose is to provide a radio interface and appropriate device drivers to common communication protocols such as TCP/IP, NetBIOS and IPX. The radio component of the LAN is totally transparent to applications using these protocols.

To the end user, an application works exactly the same way as it would on a conventional wired LAN such as Ethernet or token-ring. A brief summary of the host independent Wireless LAN products, IBM Wireless LAN Entry and IBM Wireless LAN is given in the following sections. These products are treated in greater detail later in the document.

2.3 IBM Wireless LAN Entry

IBM Wireless LAN Entry is a product which enables workstations to be grouped into logical cells using a radio interface built into a PCMCIA type adapter. These workstations can then communicate with other systems in the following ways:

- To other workstations in the cell on a peer-to-peer basis
- To other workstations in the cell via an IBM Wireless LAN Entry Access Point
- Via an IBM Wireless LAN Entry Access Point to servers or hosts attached to an Ethernet LAN
- To other workstations in other cells via an IBM Wireless LAN Entry Access Point and an Ethernet LAN

IBM Wireless LAN Entry operates in the 2.4 GHz frequency Industrial, Scientific and Medical (ISM) band. Operating in this band requires no license. IBM Wireless LAN Entry employs a technique known as spread spectrum frequency hopping as a means of transmission. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is the means by which multiple concurrent transmissions are handled on the same channel. This technique provides reliable security against eavesdropping. It also ensures that there is minimal interference from or to other devices in the vicinity which may be using the same band.

2.3.1 The Stand-Alone Cell

To operate in peer-to-peer mode, workstations are configured as part of a stand-alone cell. This configuration can support 32 workstations or more with a maximum distance between them of about 180 meters in an open environment. The actual number supported is determined by the amount of traffic and frequency of activity within a cell. In a closed or semi-closed environment, the effective distance is reduced by physical factors such as relative positioning of workstations, reflective surfaces and signal absorption by walls and ceilings. In

any cell, one workstation is configured as a cell leader whose responsibility it is to dictate what frequency channels are to be used within the cell and in what order. It also provides authorization functions for the workstations in the cell.

Multiple overlapping cells can exist without generally interfering with each other's operation, unless the workstation density becomes significantly high. Such overlapping is transparent to individual workstations, as they only communicate with members of their own cell.

2.3.2 The Ethernet-Connected Cell

Workstations in a cell communicate with servers, hosts or other devices on an Ethernet LAN by using an IBM Wireless LAN Entry Access Point as a transparent bridge between the radio and LAN interfaces. The cell then becomes known as an Ethernet-connected cell.

In this configuration there is the option of having the workstations continue to communicate directly with each other on a point-to-point basis or indirectly via the IBM Wireless LAN Entry Access Point. Communicating via the IBM Wireless LAN Entry Access Point has the effect of extending the range of communication as the signal is effectively boosted on retransmission. The trade-off is that the performance may be reduced, but overall delivery is more reliable. In an open environment the distance between workstations communicating via the IBM Wireless LAN Entry Access Point can be up to 360 meters.

In an Ethernet-connected cell, the IBM Wireless LAN Entry Access Point performs the tasks of allocating the channel frequencies for the cell and handles the authentication and authorization function. It also manages frame filtering of Ethernet traffic for the workstations in its cell. The recommended maximum number of workstations in an Ethernet-connected cell is 32.

2.3.3 The Network of Ethernet-Connected Cells

Workstations can communicate with workstations in other cells providing that all cells are Ethernet-connected to the same LAN. Each cell must be connected to the LAN by its own IBM Wireless LAN Entry Access Point.

Any number of cells can be connected on the LAN or on multiple Ethernet LANs bridged together. Individually, the cells and workstations in them operate in exactly the same manner as in an Ethernet-connected cell.

2.3.4 Network Management

The IBM Wireless LAN Entry Access Point can be configured to act as an SNMP agent and has a set of standard MIBs (Management Information Base descriptors) which define generic information about SNMP capable devices on a network. It also has a set of device-specific MIBs which describes the information specific to bridges. Finally, it has an IBM-specific MIB which describes information unique to a wireless bridge device.

As an SNMP agent, the IBM Wireless LAN Entry Access Point can collect and send this information to a management station running NetView for AIX or a similar monitoring application somewhere on the network.

2.3.5 Frame Filtering

The IBM Wireless LAN Entry Access Point can also be configured to act as a frame filter. This function can be used to prevent broadcast or multicast frames originating on the Ethernet LAN from reaching the workstations. NetBIOS frames addressed to cell members will be permitted while all others will be rejected.

2.4 IBM Wireless LAN

IBM Wireless LAN operates in the 2.4 GHz Industrial, Scientific and Medical (ISM) frequency band. It uses the spread spectrum frequency hopping technique of TDMA (Time Division Multiple Access) as its transmission protocol. TDMA divides the transmission time on a particular channel into a series of time slots. The slots are allocated dynamically to the stations which have data to transmit. The fact that a transmission *hops* from one channel to another provides good security against casual or intentional eavesdropping. (IBM Wireless LAN allows personal systems and workstations to access LANs, such as token-ring, Ethernet or the IBM PC Network, via short range wireless communication.)

An IBM Wireless LAN cell consists of a base station and one or more wireless workstations which are described as follows:

Wireless workstation: This is a workstation on the wireless network.

Base station: This is the focal point of the network providing frame relaying functions between the cell members (wireless workstations). The base station can also be the access point between the wireless workstations and a wired LAN where it can perform IPX/IP routing (Novell NetWare) and bridging (OS/2) functions between the wired LAN and wireless workstations. IBM Wireless LAN supports both the ODI and NDIS industry standard adapter interfaces.

A base station can coexist with various network operating systems and can support other functions besides bridging and routing. It can, for example, act as an *SNA gateway*.

2.4.1 The Stand-Alone Cell

This is the simplest configuration with the base station acting as the relay station for the cell members. A wireless workstation can communicate with the base station as well as with other wireless workstations via the base station. The wireless workstations are used in exactly the same way by the end users as if they were LAN attached. The only hardware requirement is the addition of wireless adapters for the stations. This configuration can support up to 50 wireless workstations but the number of simultaneous users in a cell depends on the volume and type of traffic.

It is possible to install several overlapping cells which do not interfere with each other′s transmissions. However, workstations can only communicate with workstations in their own cell.

Note: There is a physical limit of 12 overlapping cells. However, local (that is country) radio spectrum regulations may specify a maximum of less than this. In Japan, for example, the maximum number of overlapping cells permitted is six.

2.4.2 Multiple Wired LAN Cells

A wired LAN cell is a cell connected to a wired LAN backbone. In this configuration, wireless workstations can communicate via the base station with other workstations and servers connected to the wired LAN. If other wireless LAN cells exist on the same wired backbone, the wireless workstations in individual cells can communicate with those in other cells. Acting as a MAC level bridge, IP/IPX router or SNA gateway, the base station forwards frames from the wireless cell to the wired LAN and vice versa. In this configuration, the base station requires both a wireless adapter and an appropriate wired LAN adapter. See Chapter 4, “IBM Wireless LAN” on page 57.

2.4.3 The Network Administrator Program (NAP)

The NAP is provided as part of the IBM Wireless LAN product. It performs the administration functions for the cell. Such functions include workstation registration, authentication and security control. The NAP cannot be run from a wireless remote station. It can only be installed in a base station or other LAN-attached station designated as a network manager.

Every cell must be managed by a NAP from somewhere. In a stand-alone cell, the base station is that point. In a wired LAN cell the NAP can be run from that cell′s base station or it can be run from the base station of some other cell on the backbone. It may also be run from a dedicated management station somewhere on the backbone and which does not have to be part of any cell itself. In this way, the management of an entire group of up to 60 cells and the workstations in them can be concentrated in one management station.

The base stations communicate with each other and with the NAP station using TCP/IP.

2.4.4 Network Management

This is a completely different function to, and independent of, the NAP. The IBM Wireless LAN base station can act as an SNMP agent in much the same way as an IBM Wireless LAN Entry IBM Wireless LAN Entry Access Point. See 2.3.4, “Network Management” on page 16.

2.5 IBM Wireless LAN Entry and IBM Wireless LAN, Similar but Different

IBM Wireless LAN Entry and IBM Wireless LAN are very similar products in many ways. To the end user, workstations using either product can access a wired LAN and whatever resources the LAN supports. To the network administrator, network designer or systems integrator the radio technology employed in each product is very similar. However, the design concept is somewhat different for each product which gives rise to differences in functionality. Wireless implementers should be aware of these differences when considering a wireless solution. Table 1 gives a comparison of IBM Wireless LAN Entry and IBM Wireless LAN by feature and function.

Table 1 (Page 1 of 2). Comparison of Wireless LAN Products by Feature and Function

Feature/Function	IBM Wireless LAN Entry	IBM Wireless LAN
Stand-Alone Cell	Yes	Yes
Ethernet-Connected Cell	Yes	Yes
Token-Ring Connected Cell	No	Yes

Table 1 (Page 2 of 2). Comparison of Wireless LAN Products by Feature and Function		
Feature/Function	**IBM Wireless LAN Entry**	**IBM Wireless LAN**
Operating Frequency	2.4 GHz	2.4 GHz
Spread Spectrum	Yes	Yes
Frequency Hopping	Yes	Yes
Data Link Layer	CSMA/CA	TDMA/CSMA Hybrid (French Protocol)
Station-to-Station (Peer-to-Peer)	Yes	No
Station-to-Station (Indirect)	Via 8227 Access Point	Via Base Station
Bridge Device	8227 Access Point	Base Station
Bridge Type	Transparent	Source Routing and Transparent
NetBIOS Filtering (from Wired LAN)	Yes	Yes
Network Routing	Not applicable	Yes (IP and IPX)
Roaming Support	Yes	Yes [1]
SNMP Agent	Yes	Yes
Throughput	350 Kbps	Up to 1 Mbps
Registration	By 8227 Access Point	By adapter
Authorization	By 8227 Access Point	By NAP
Authentication	By 8227 Access Point or Cell Leader	By adapter
Data Compression	No	Yes
Data Encryption	No	Yes
Signal Strength Monitor	Yes (Indirectly)	Yes (RSSI)
Remote Program Load	Yes	Yes
Note: [1] Within own cell only.		

2.5.1 Reasons for Selecting IBM Wireless LAN Entry

- Low cost adapters
- Low cost dedicated Access Point unit
- Built-in Ethernet support
- Remote boot (RPL) from server
- Roaming capability
- High mobility
- Directional (8227 only) or omni-directional antenna

2.5.2 Reasons for Selecting IBM Wireless LAN

- Support for token-ring and Ethernet
- IP/IPX routing capability
- Centralized multiple cell management
- Non-dedicated base station
- SNA gateway support in base station

Chapter 3. IBM Wireless LAN Entry

This chapter deals specifically with the IBM Wireless LAN Entry product which from hereon will be referred to as the Wireless LAN Entry. The IBM Wireless LAN Entry Adapter will be referred to as the Wireless adapter and the IBM Wireless LAN Entry Access Point will be referred to by its hardware product number, 8227.

For specific information on the IBM Wireless LAN product see Chapter 4, "IBM Wireless LAN" on page 57. A summary and comparison of the two products can be found in Chapter 2, " IBM Wireless Products" on page 13.

This chapter has a logical progression from the simplest stand-alone cell to multiple stand-alone cells to a single Ethernet-connected cell and finally to a network of Ethernet-connected cells. The chapter ends with an example scenario that was performed in the same sequence.

Wireless LAN Entry operates in the 2.4 GHz ISM (Industrial, Scientific and Medical) Radio Frequency (RF) range of the Electromagnetic Spectrum.

3.1 Hardware and Software Requirements

The Wireless LAN Entry environments and the components for creating them are as follows:

- A stand-alone cell
  1. Minimum of two workstations with a PCMCIA Type II or Type III slot
  2. Wireless adapters for the workstations
  3. A workstation operating system
  4. A network operating system
- A network of one or more Ethernet-connected cells
  1. The items listed above
  2. One 8227 plus wireless adapter for each Ethernet-connected cell
  3. One Ethernet 10base2, 10base5 or 10BaseT cable for each Ethernet-connected cell
  4. One Ethernet transceiver for each Ethernet-connected cell using 10base2 or 10base5 type cabling
  5. A file (RPL) server accessible to an 8227

The operating system need not be the same on all workstations unless that is a requirement of the networking software. Workstations may use any of the following software:

- IBM OS/2 Version 2.1 or higher
- IBM PC-DOS Version 5.0 or higher
- Microsoft MS-DOS Version 5.0 or higher
- Microsoft Windows for Workgroups Version 3.11 or higher

The following are optional choices with respect to network software:

1. A network operating system
2. A combination of a network application program plus an interface and protocol program

These options are explained below:

- DOS environment

  If you are using Option 1, any of the following network software may be used:

  – Artisoft LANtastic Version 6.0 or higher (supplied with product)

  – IBM TCP/IP for DOS Version 2.1 or higher

  – Microsoft Windows for Workgroups Version 3.11

  – Novell NetWare Version 3.11 or higher (workstation for DOS and Windows feature)

  – Novell Personal NetWare Version 1.0

  If you are using Option 2, *both* of the following are required:

  – One of the following interface and protocol programs:

    - IBM LAN Support Program Version 1.38 or higher

    - IBM LAN Support Program/NDIS Version 1.0

  – A network application program that uses the IEEE802.2 or NetBIOS protocol such as:

    - IBM Personal Communications/3270 Version 3.1 or higher

    - DOS LAN Requester feature of IBM OS/2 LAN Server Version 3.0

    - DOS LAN Services feature of IBM OS/2 LAN Server Version 4.0

- OS/2 environment

  One or more of the following network application programs is supported:

  – IBM Communications Manager/2 Version 1.0 or higher

  – The requester feature for the IBM OS/2 LAN Server Version 3.0 or 4.0

An 8227 access point requires an RPL server to load from. The RPL file server (which stores the 8227 Remote Boot Image) must support LLC (logical link control). The following networking software programs include this support:

- IBM OS/2 LAN Server Version 3.0 or 4.0
- Novell NetWare Version 3.11 or higher

3.2 Wireless LAN Entry Design Considerations

The document *IBM Wireless LAN Entry Network Planning Guide*, GA27-4983 is an excellent reference document containing product details and information about the radio characteristics which affect or enhance the operation of the Wireless LAN Entry. It is strongly recommended that this document be reviewed as an essential aid to planning an installation for Wireless LAN Entry. The other two product specific documents are *IBM Wireless LAN Entry User's Guide* and *8227 Wireless LAN Entry Access Point User's Guide*, both of which are shipped with the products in question.

When designing a Wireless LAN Entry network, the following considerations apply:

- Type of environment
- Required operating range
- Factors affecting performance
- Number of mobile stations
- Type of end user traffic
- Roaming requirement
- Existing wired LAN arrangement
- Expansion plans

At this stage it is worthwhile to define some terms which will occur frequently throughout this chapter.

Terms and Expressions	Definitions
Cell	This is the basic organizational unit necessary for Wireless LAN Entry communication to exist. The simplest cell is a stand-alone cell (also known as a point-to-point or ad hoc cell). It consists of one workstation configured as a *cell-leader* and one or more workstations with a wireless capability. All workstations must be radio-enabled, which is to say they must have an appropriate transceiver device (the Wireless adapter which is a part of the Wireless LAN Entry hardware) and radio-enabling software (the Wireless LAN Entry software).
Cell-leader	This is where one workstation in a stand-alone cell manages particular functions of the cell on behalf of the other cell members. Its primary functions are: • Authorization of cell members • Notification of *frequency hopping pattern* and *channel* to the workstations Otherwise the cell-leader behaves just like other cell members. It is only required in a stand-alone cell.
LAN	In this case it is an Ethernet LAN. This is the only LAN type presently supported by Wireless LAN Entry. It can be 10base2, 10base5 or 10BaseT.
WnetID	This is Wireless Network Identifier. This is a parameter which is passed to a cell-leader or *access point* from a workstation. It is the means by which workstations identify themselves as being members of a particular cell.
Access Point	This is also known as the 8227. It acts as a MAC level bridge between the workstations and the LAN in an Ethernet-connected cell. Its primary functions are: • Authorization of workstations for cell admission and LAN access

- Notification of *frequency hopping pattern* and *channel* to the workstations
- Frame filtering from the LAN to the workstations (if required)
- Perform SNMP agent functions (if required)
- Enable *roaming* to occur between cells in a network of Ethernet-connected cells
- Register and control workstations which roam into its vicinity

Channel The 2.4 GHz band of the RF spectrum is divided up into a number of discrete frequency channels. Any of these channels can be used for transmission by the *spread spectrum* technique.

Country spectrum management regulations may determine how many channels the band is to be divided into and the minimum number of channels that a particular transmission must use. In the US, the FCC has stipulated that in the ISM bands from 2.4 GHz to 2.483 GHz, 75 of the 83 1 MHz bands must be used and FH systems are constrained to 1 MHz of bandwidth at a time.

Roaming This is the ability of a workstation to move seamlessly between cells in a network of Ethernet-connected cells; that is, without any apparent break in communication.

Hand-off This is the process by which a roaming workstation switches its registration and control between 8227s in a network of Ethernet-connected cells.

Spread spectrum These are techniques for sharing a large bandwidth of spectrum between multiple users without causing interference between those users.

Frequency hopping This is a spread spectrum technique whereby a particular radio transmission hops among available frequency channels and transmits briefly on each channel before hopping to the next. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is the access method used by Wireless LAN Entry with this technique.

Direct Sequence This is another spread spectrum in which each bit of data is encoded with a pseudo random pattern that can only be recognized by the destination receiver. Multiple users with individual patterns are thus able to share the same frequency channels.

3.2.1 Operating Environment

First, consideration must be given as to where the Wireless LAN Entry will be operating. There are three general classifications of operating environments indicated below:

Environment Characteristics for Wireless LAN Entry

Closed This is a house, a floor of individual offices or a building with rooms and corridors.

Semi-open This is a warehouse, exhibit hall, factory floor, a large space divided up by panels or a large office with cubicles or partitions.

Open This is an area where there are no obstacles to interfere with RF transmissions.

Obviously, many environments will be hybrids of those listed but these are a good starting point.

3.2.2 Factors Affecting Range

When considering the required operating range, it is important to also take into account factors which may affect radio performance. Factors may be obvious things like brick or concrete walls which have the effect of reducing the RF signal strength and thereby reduce the effective range of transmission. A less obvious but nevertheless influential factor is people. Human beings are composed of 72% water. Water is an extremely efficient absorber of RF in the 2.4 GHz range as is illustrated by the effectiveness of microwave ovens which use the same range. People moving about close to a Wireless LAN Entry transmitter can cause brief interruptions at the receiving stations.

Other objects can have the opposite effect and may act something like antennas and re-radiate the signal. This is undesirable because it generates multiple paths for the same signal and causes a reduction in the signal-to-noise ratio. It is the signal-to-noise ratio rather than pure signal strength which determines whether or not useful radio communication is possible. The metal studs in walls and building wiring generally are common causes of this phenomenon.

Multiple paths can also be produced as a result of signal reflections off walls and other surfaces. In some cases reflection can be quite advantageous as it may enable a signal to travel around a corner in a corridor for example. Where this is desirable, the effect can be enhanced by selecting and positioning the appropriate antenna. See Figure 7 on page 40.

Other radio sources in the vicinity can contribute to an overall reduction in the signal-to-noise ratio. Transformers, generators, electric welders and particularly microwave ovens can all introduce spurious RF signals which can affect the performance of the Wireless LAN Entry.

3.2.3 Mobile Stations and Cell Selection

The simplest cell is a stand-alone cell. It is often referred to as a point-to-point cell which indicates the direct path of communications between workstations. It is also referred to as an ad hoc cell because of the way in which new workstations can be added to the cell.

The maximum separation between any pair of workstations is the effective transmission range of the antenna in a particular environment. Stations within the same cell can almost double the separation distance by the addition of an 8227 Access Point which acts as a signal repeater between workstations. Since the 8227 has a built-in Ethernet capability, this arrangement is known as an Ethernet-connected cell. See Figure 2 on page 28 and Figure 5 on page 33.

Deciding how many mobile stations will be needed initially, and where they will be placed, determines what kind of cell structure is required. If future needs can

be estimated, so much the better. The Wireless LAN Entry is flexible enough to allow almost unlimited extension as and when required. A single stand-alone cell may be the initial requirement. But in the future, will there be a need to wire this cell into a LAN for cell-to-LAN communication or access to shared LAN resources? The important thing is to make sure there is provision for a LAN to be installed or that there will be access to an existing LAN if required.

If the initial setup requires no more than 10 to 15 users to be radio-enabled and all will be working within perhaps 25 meters (82 feet) of each other in a relatively radio-friendly environment, then a single stand-alone cell may be all that is required. See Table 2 for effective operating ranges. This will allow stations to move around the local area and continue to communicate with each other providing that the distance between the pair and the distance between either machine and the cell leader does not exceed the range capability of the transceivers.

Table 2. Maximum Separation Distances. Nominal and Maximum distances over which communication from workstation-to-workstation and workstation-to-8227 is possible. Distances are given in meters (feet).

Environment	Antenna Type					
	Patch•		Integral		Integral•	
	Nominal	Maximum	Nominal	Maximum	Nominal	Maximum
Closed	31.7 (104)	37.0 (122)	26.0 (85)	30.5 (100)	12.2 (40)	15.2 (50)
Semi-open	108 (354)	126.5 (415)	85 (280)	100 (328)	42.6 (140)	50 (164)
Open				366 (1200)		183 (600)

Note:

•Patch antenna only available for 8227.
•Stand-alone or Ethernet-connected (non-centralized) cell.
In this mode, workstation-to-workstation distance equals workstation to 8227 distance.

In a multiple workgroup environment, communication between members of a group would be required but not necessarily between groups. In this case, multiple stand-alone cells could be the solution. Each cell would have one workstation configured as a cell-leader. In this situation the cells could overlap each other without affecting each others performance and the maximum distance between members of a particular cell would be unchanged.

Another potential usage for multiple stand-alone cells would be when a particular set of users need to exchange graphical images or other large files. Transmitting a particular image may require the total throughput capability of the cell. If this happens, there could be an unacceptable delay between sending and receiving the file or the other workstations may not be able to communicate at all until the image has been received. In this case, splitting the cell, that is, creating two individual stand-alone cells each with its own cell-leader would make sense. The graphics users could have their own cell with full bandwidth available for their use only. Similarly the non-graphics users would have their own cell and neither group would have any impact upon the performance of the other.

If at some later date the workstations have a requirement to access a server or host based on an Ethernet LAN, then that would be the time to consider switching to an Ethernet-connected cell.

If the requirement happens to be for communication between workstations in different cells, then a network of Ethernet-connected cells is the answer. This type of network is just a collection of Ethernet-connected cells which happen to be on the same LAN (or network of bridged LANs). So, whatever LAN-based services are available to one should be available to all.

Finally, roaming has to be considered. This requirement usually comes about when end users must move around a location, often beyond the coverage of the cell to which they are registered, but still maintain contact with some LAN-based function. This is where the value of a network of Ethernet-connected cells becomes apparent.

When properly organized, the 8227s belonging to individual cells will recognize that a new workstation has *roamed* into their coverage area. An 8227 seeing the newcomer will verify whether or not it is authorized to access the LAN through this particular 8227. If so, it will permit access and assume control of the workstation until such time as the workstation roams off out of range or otherwise disconnects. The hand-off between 8227s should be totally transparent to the end user.

3.2.4 Security

In a stand-alone cell security is handled by the WnetID alone. Every member of the cell including the cell-leader has the same WnetID configured during installation. When a cell-leader detects a request from a workstation to join the cell, it requests the WnetID first and if this is the same as the cell-leader′s, it is allowed to join the cell. It may now establish communication with the other workstations.

Even when operating in point-to-point mode, workstations must constantly advertise their presence and their WnetID to the cell-leader so that it is aware at all times of how many active members there are. This prevents the WnetID from being changed *on the fly*, since the workstation will be immediately dropped from the cell′s control if this happens.

No extra security is required for multiple overlapping cells as each is completely independent of the other. Each cell however, requires an individual WnetID.

In an Ethernet-connected cell or network of Ethernet-connected cells, the security of the LAN is to be considered. This is accomplished by means of the Address Range Authorization Table (ARAT) and the Address Specific Authorization Table (ASAT) which are stored in the 8227. The ARAT specifies the highest and lowest number of a range of MAC addresses pertaining to the Wireless adapters which will be used in the cell. Up to 12 discrete ranges can be specified. The ASAT is a list of specific adapter addresses which will be permitted access.

The default state of these tables is *disabled*. However, once enabled (either one or both tables), the admission of workstations can be very tightly controlled. These tables relate only to a specific 8227. In an Ethernet-connected cell, any workstation not recognized by the 8227 will not be allowed access to either the cell or the LAN, even if the WnetID is correct.

In a network of Ethernet-connected cells, there are multiple 8227s controlling their own cells. Each 8227 can have a different set of addresses to manage. This determines which workstation will be allowed access through which unit.

Each cell can still have a different WnetID and this is checked along with the address table entry by any 8227 before it will allow access.

Where roaming is required, the only change that needs to be made is to the WnetID. All 8227s and workstations must have a common WnetID for roaming to occur. Again, restriction by the MAC address can be applied to specific 8227s. This means that particular roaming workstations may be permitted access to the LAN but only via particular 8227s.

As far as eavesdropping is concerned, the spread spectrum transmission technique offers excellent protection. The individual cells are assigned a hopping pattern which defines what order the channels are switched to for transmission. This order or pattern is dictated by the cell-leader or 8227. It is difficult to monitor a transmission which swaps frequencies every 200 ms, and although equipment is available for doing this, it would be prohibitively expensive for all but the determined few. Generally speaking, spread spectrum is considered to be very secure.

If greater security than this is required, for example DES encryption, then IBM Wireless LAN may be a more suitable product. For specific information on the IBM Wireless LAN product see Chapter 4, “IBM Wireless LAN” on page 57.

3.3 The Stand-Alone Cell

The stand-alone cell is the simplest functional Wireless LAN Entry unit. It consists of two or more workstations which communicate via radio transmission in the 2.4 GHz band. They operate in a point-to-point mode which is to say that any pair of stations will talk directly to each other without having to go through an intermediate device. See Figure 2.

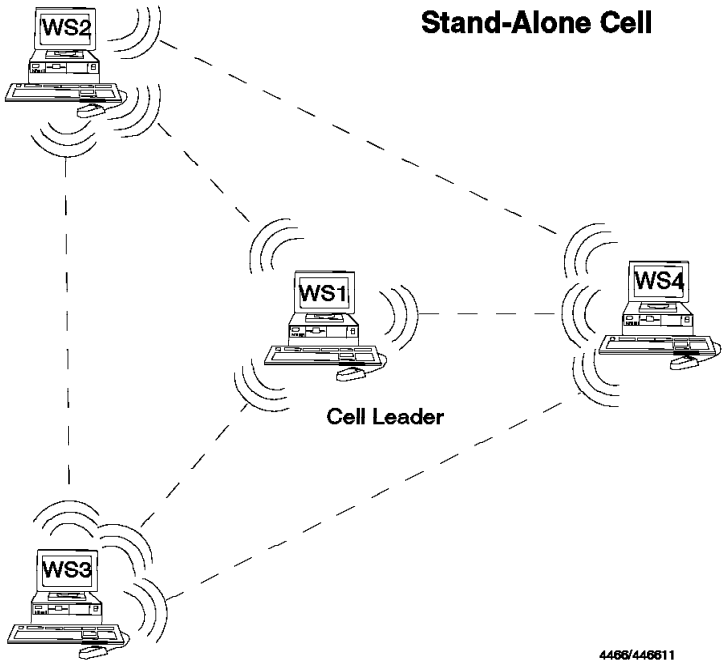


Figure 2. The Stand-Alone Cell. Workstations 2, 3 and 4 communicate in point-to-point mode and not through the cell-leader. They communicate with the cell-leader for information about the cell.

3.3.1 The Cell-Leader

One and only one station in the stand-alone cell must be configured to be a cell-leader. The specific functions of this station are:

- Notification of the frequency hopping pattern and channel to the workstations
- Authorization of workstations for cell admission

Using the spread spectrum technique of frequency hopping, the 2.4 GHz RF band is divided up into a number of sub-bands or frequency channels. In the US this number is 83 channels of 1 MHz each (from 2.4 to 2.483 GHz, however 2.4 GHz is reserved as a guard band and is not used). Other countries may specify a different number or may leave it up to the equipment manufacturer. Every transmission may use some or all of these channels providing that the transmission is of sufficient duration to do so. Once again, different countries may specify a different minimum number of channels to be used or may leave it up to the manufacturer′s discretion. In the US the minimum number of channels employed must be 75 of the 82 available (2.4 GHz is not used). A transmission may commence on any channel, but after a timespan of 200 ms the transmission will switch or hop to the next in sequence. Here, the transmitting station listens for traffic and, if the channel is free, transmission will continue for a further 200 ms before hopping again.

All the workstations in the cell, including the cell-leader, must hop to the same channel at the *same instant* so that only one channel is being used by a particular cell at any one time.

The order in which the channels are selected is called the *Frequency Sequence Pattern* or *Frequency Hopping Pattern* and is directed by the cell-leader. The cell-leader configuration contains a frequency sequence pattern number which can be 01, 02, or 03. It is this parameter which determines the order of channel selection.

The advantage of this method is that multiple transmissions between overlapping cells can happen simultaneously with very little chance of collision. A further advantage is security from eavesdropping. It is practically impossible to monitor a transmission when the hopping pattern is not known.

Authorization

All stations belonging to the same cell, including the cell-leader, must have the same WnetID. This is an alphameric name, of up to six characters, which is given to each of the stations during configuration. This has nothing to do with individual workstation names which are required by higher-level networking software products such as Artisoft LANtastic or TCP/IP.

When a station first comes within the range of a particular cell, the cell-leader detects its request for admission to the cell. Assuming that the WnetID matches the one being used by the cell, the newcomer is permitted to participate. The cell-leader tells the newcomer which hopping pattern is being used by the cell members and what channel to begin to transmit on. From this point on the newcomer is part of the cell.

3.3.2 Multiple Overlapping Stand-Alone Cells

As mentioned earlier, an organization may require multiple independent LANs for workgroups, departments or some other organizational division. This can be accommodated quite easily in the Wireless environment with multiple stand-alone cells in much the same way as individual departments may have their own dedicated token-ring or Ethernet LANs. These cells can overlap each other's ranges without causing any interference. See Figure 3.

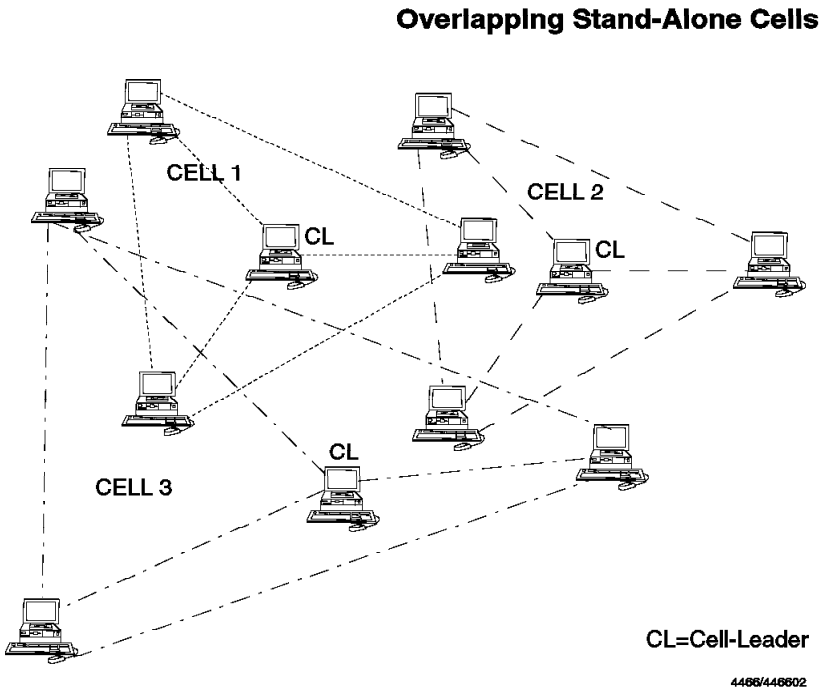


Figure 3. Overlapping Stand-Alone Cells. Frequency hopping ensures that these cells do not interfere with each other's transmissions.

There are only two considerations:

1. The WnetID

   This must be different for each cell. A workstation can only be a member of one cell at a time and it is the WnetID that determines which cell it is.

2. Hopping Pattern

   In the cell-leader setup there is a choice of three hopping patterns. Selecting different patterns for adjacent cells will ensure that there are minimal collisions with traffic in other cells trying to allocate the same frequency channel at any instant in time. In practice, it is unlikely that any two transmissions would start at *exactly* the same instant, so even if two cells had the same pattern and commenced transmission on the same channel, one would tend to always follow the other. It is possible that due to slight variations in the hopping speed of the individual cells, transmissions may eventually coincide. After one coincidence however, they would follow their own unique patterns once again.

3.4 The Ethernet-Connected Cell

At some stage, workstations in a stand-alone cell may require access to services on a LAN. There would be a very easy transition from one environment to the other with minimal disruption to the end users. There would be no hardware changes necessary on the workstations to allow them to gain access to the LAN. The only change to the cell structure would be to replace the cell-leader with an 8227 IBM Wireless LAN Entry Access Point which performs the functions of a MAC level bridge between the Wireless LAN Entry and wired LAN. The 8227 would be attached to a suitable Ethernet LAN (10base2, 10base5 or 10BaseT), and the new cell configuration would be complete. See Figure 4.

Caution

Never configure a cell-leader and an 8227 with the same WnetID. This may cause unpredictable behavior on a workstation having the same WnetID and within range of both.

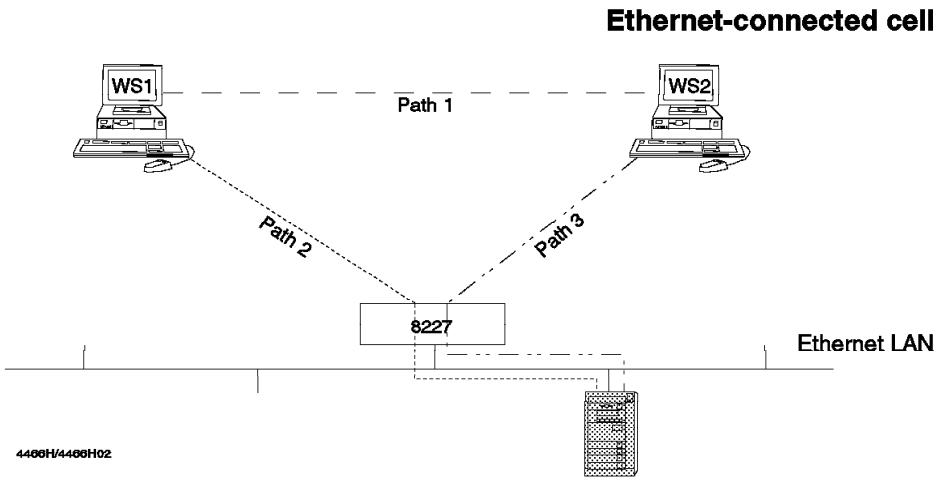


Figure 4. The Ethernet-Connected Cell. The workstations are shown here operating in point-to-point (non-centralized) mode along Path 1. They have the option of communicating with each other via the 8227 in an indirect (centralized) mode. Paths 2 and 3 are used for LAN access. See also Figure 5 on page 33.

3.4.1 The 8227 Access Point

In a stand-alone cell the frequency allocation function is handled by the cell-leader. In an Ethernet-connected cell, it is performed by the 8227. The functions of the 8227 in this environment are as follows:

- Cell type setting
- Authorization of workstations for cell admission and LAN access
- Notification of the frequency hopping pattern and channel to the workstations
- Frame filtering from the LAN to the workstations (if required)
- Perform SNMP agent functions (if required)

Control Mode: This can be either *non-centralized* or *centralized*. In non-centralized operation the workstations in the cell continue to communicate in a point-to-point manner just as they do in the stand-alone cell with no change in range or function. An advantage of this approach is that data transmissions can proceed at their maximum rate.

In a centralized operation all the workstation traffic is routed through the 8227. This has the effect of slowing the transaction somewhat, but in practice, this may not be noticeable except for very large data transfers. The benefit is that the signal is effectively retransmitted at full strength, which allows for a doubling of the distance between workstations. See Figure 5 on page 33.

In the non-centralized mode, therefore, the effective range of communication between a pair of workstations would be the radius of a circle having the 8227 at its center. In the centralized mode the range would be the diameter of the same circle.

Authentication and authorization: Where a wired LAN is involved, extra security precautions need to be in place to prevent unauthorized access. The WnetID is still used to verify cell members, but beyond that the 8227 has the ability to accept or reject cell members′ requests for LAN access. It does this by way of the Address Range Authorization Table (ARAT) or the Address Specific Authorization Table (ASAT).

The ARAT contains the highest and lowest numbers of the range of MAC addresses of the Wireless adapters which are to be used by the cell workstations and which will be permitted access to the LAN. Unless the MAC addresses are numbered sequentially, it is possibly a better idea to use a Locally Administered Address (LAA) than the Universally Administered Address (UAA). The UAA is burned-in to the adapter by the manufacturer and is displayed on a label on the underside of the Wireless adapter as *Net Address*. The ARAT can accept 12 discrete address ranges.

The ASAT is a list of MAC addresses specifically configured to permit access to the LAN. Again, either LAAs or UAAs can be used. Both ARAT and ASAT can be enabled concurrently to give greater flexibility over access and denial. If both are disabled, the 8227 assumes that if the requester is a member of the cell as indicated by its WnetID, then access can be granted to the LAN. The ASAT can accept a maximum of 256 individual entries.

Locally Administered Address

If an LAA is to be used, it is entered as a parameter in either the PROTOCOL.INI file or the NET.CFG file on the workstation. It must be in canonical format and the statement would appear similar to the following:

NETADDRESS = ″02008040**C020**″

The entry can be done manually, but it is easier to use a configuration tool such as LAPS on OS/2 or LSP on DOS.

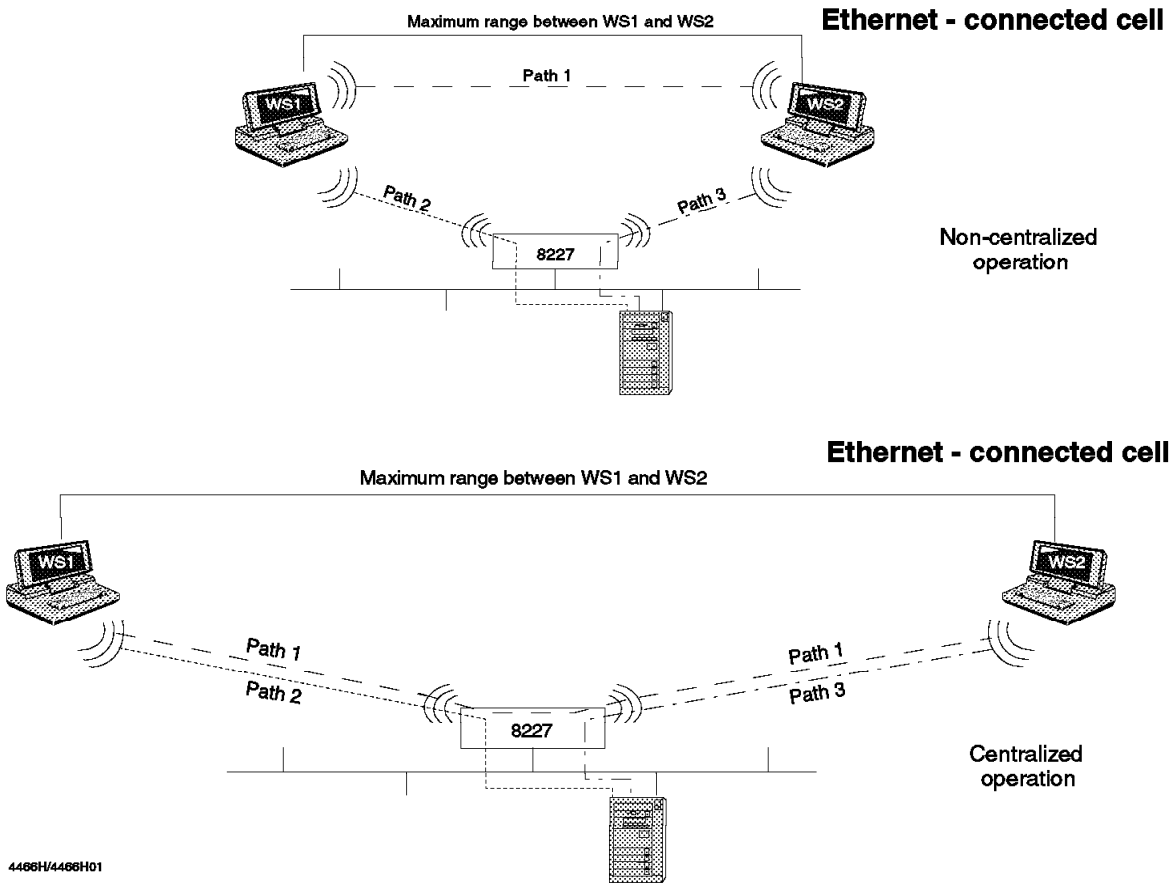


Figure 5. Centralized versus Non-Centralized Operation. The separation distance (Path 1) between workstations in centralized mode can be double that for non-centralized mode since the 8227 is retransmitting the signal. Paths 2 and 3 are used by the workstations to access the LAN-based services.

3.4.2 Loading and Configuring the 8227

The *IBM Wireless LAN Entry Access Point User's Guide*, GX27-4002 shipped with the 8227 contains all the instructions needed for configuring and loading. A detailed explanation of the configuration parameters is also included, so it is not repeated here. The *IBM Wireless LAN Entry Access Point Network Planning Guide*, GX27-4003 also includes details on configuration. The details are not reviewed here, but an outline of the procedure is given below:

Copy the configuration utility from the utility diskette to a suitable workstation.

Run the configuration program which creates a configuration file and copies the configuration file to the operational software diskette.

Using the operational software diskette, create a remote boot diskette image on a suitable server on the LAN to which the 8227 will be connected.

This procedure creates an image of the 8227's operating environment including ARAT/ASAT table entries and any SNMP and filtering functions which it may have to perform. The RPL procedure downloads this image over the LAN into the 8227. When the 8227 has loaded this image into memory, it is ready to

perform the appropriate control functions. It will continue to do this until it is powered-off, in which case it will need to go through the whole procedure again when it powers up. Once the image is loaded, the 8227 needs no further communication with the RPL server.

In order for the Remote Program Load (RPL) procedure to function, a Logical Link Control (LLC) path must exist between the 8227 and the boot image server. The following network operating systems (one of which must be installed on the server) all support LLC:

- IBM LAN Server Version 3.0 and 4.0
- Novell NetWare Version 3.11 and 4.0 or higher

The same boot image can be used for multiple 8227s. This is one way of keeping their MAC address (authentication and authorization) tables synchronized in a network of Ethernet-connected cells. See 3.5.1, “Updating the 8227s” on page 35.

The RPL process starts soon after the 8227 powers-on. The 8227 repeatedly broadcasts a *find* frame on to the LAN until a server responds with a *found* frame. The 8227 then transmits a *send.file.request* frame to the server. The server responds by sending a bootstrap image to the requesting unit. The image is loaded into the 8227 after which it is ready for operation.

3.5 The Network of Ethernet-Connected Cells

Going one step further than the Ethernet-connected cell, it may be desirable for an organization to build a network of Ethernet-connected cells. It may in fact already have workgroups of Ethernet-connected cells accessing the same LAN, but until now they have not been able to access each other. There may now be the requirement for the mobile users to wander beyond the boundaries of their own cell but still maintain access to the LAN. The network of Ethernet-connected cells will satisfy this requirement. This environment is created by simply connecting multiple Ethernet-connected cells to the same LAN and giving the 8227s and workstations in all the cells a common WnetID. See Figure 6 on page 35.

The 8227 in a network of Ethernet-connected cells takes on the following functions:

- It enables roaming to occur between cells.
- It registers and controls workstations which roam into its vicinity.

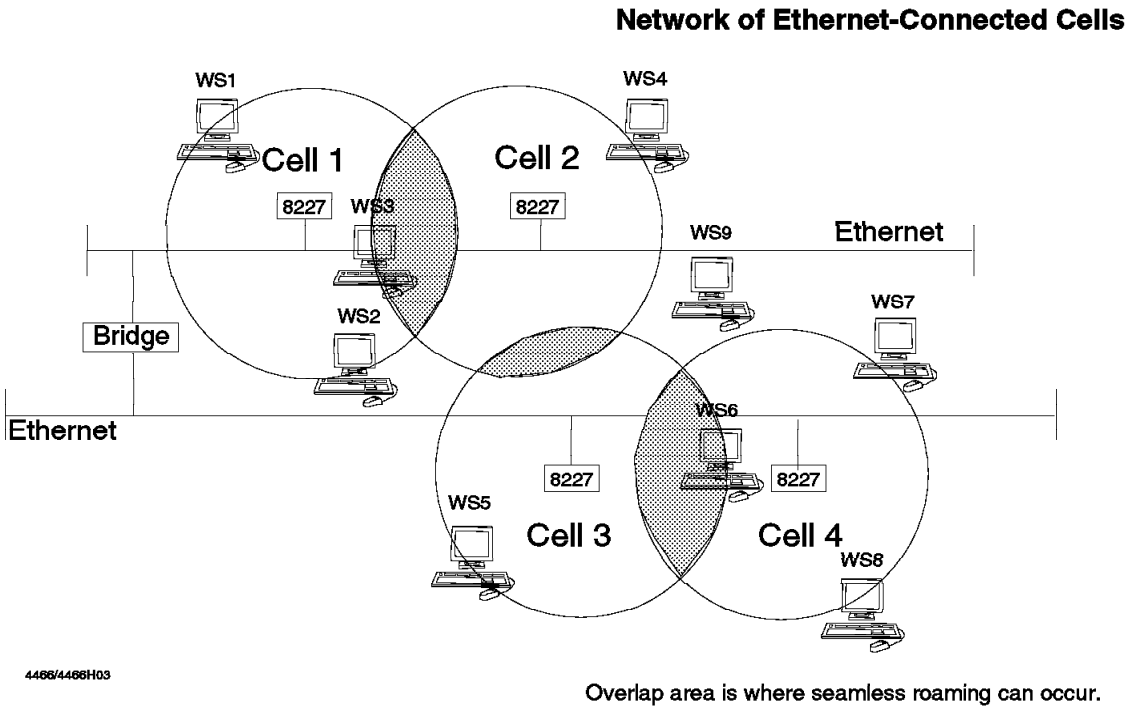


Figure 6. The Network of Ethernet-Connected Cells. Workstations 3 and 6 are in the overlap area of two cells each and could be registered with either. Workstation 9 is presently unregistered but could easily roam into the control area of any one of three cells. All other workstations would have only one registration option in their present locations. Circles represent the effective limit to the cells' transmission ranges.

3.5.1 Updating the 8227s

Besides changing the WnetID, some other changes need to be made to the configurations of each 8227:

Frequency Sequence Pattern Number: In an 8227, this can be a value between 01 and 15, and it is good practice to select a different pattern for each cell or at least for the ones whose ranges may overlap. See 3.4.1, "The 8227 Access Point" on page 31 for previous comments on this issue.

Authorization Table: This requires some planning before making any changes. Just as with the single Ethernet-connected cell, both ARAT and ASAT are supported in the network of Ethernet-connected cells. If the total workstation population is small and everyone is to be allowed access via any 8227, then it makes sense to have authentication disabled on all 8227s. However, for security reasons it may be desirable to take the opposite approach and have every workstation known to every 8227 by enabling ARAT/ASAT on all 8227s.

Between these two extremes there are any number of possibilities of permitting access to specific users via specific 8227s. Coming back to the workgroup concept, a particular 8227 may be reserved for a particular group of individuals but can also be enabled for access by specific users who have a genuine roaming need within the organization.

In Summary

If an 8227 has authentication and authorization enabled and your workstation's MAC address is not known to it, you will be denied access to both the cell *and* the LAN through this particular access point. The WnetID, correct or otherwise, will be ignored.

3.5.2 Roaming

In the wide area environment, roaming refers specifically to a mobile device moving between networks provided by different carriers without any apparent break in communication. In the Wireless LAN Entry environment the concept is the same, but the user is simply moving between different cells in relatively close proximity to one another and, more often than not, controlled by the same organization.

Suppose a workstation is powered-on and its radio interface is enabled within the range of an 8227 (to which it is authorized). Then the workstation begins rapidly scanning the frequency channels listening for a transmission from an 8227. When it hears one, it immediately attempts to contact the 8227 on the same channel with a *hello* data frame which contains the MAC address of the workstation. If the 8227 hears the request, it will check to see that it has the MAC address in the authorization tables. If this is valid, then the workstation is told what hopping pattern sequence to use and whether the centralized or non-centralized operation applies to the cell. It may then use the services of the 8227 which includes access to the LAN.

At some point, the user of this workstation may decide to go on a journey and begin to move away from the 8227 and towards the cell boundary. Sooner or later the distance will prevent effective communication and the signal will begin to break up, which, in reality, means that the frames are being lost. For a while, this will be overcome by retransmitting the lost frames, but once the workstation loses four consecutive *trailer* frames, this particular transmission is terminated.

A trailer frame is the last frame sent to a workstation by the 8227 before the workstation has to switch channels (which occurs every 200 ms). It specifies what the next four transmission channels will be. The workstation can miss one trailer because it still remembers the next three channels from the last trailer it received. If it misses a second trailer, it only knows about the next two hops. After missing four consecutive trailer frames, it no longer knows what channel to hop to next, so it must re-register with an 8227 for a new hopping sequence. The same process applies between a workstation and a cell-leader in a stand-alone cell.

When the workstation realizes it has lost communication with the 8227, it attempts to reestablish contact by going into *rapid acquisition mode* which is essentially what happens when its interface is enabled in the first place. If successful, it then has to go through the registration process once more and will have to repeat the whole sequence every time it loses and regains contact.

In a network of Ethernet-connected cells however, as the workstation was distancing itself from the local 8227, it may have been passing through an overlap area between two adjacent cells and before it lost communication was in fact far closer to a neighboring 8227 than to its own. Now, when it goes into rapid acquisition mode, the chances are that the nearer 8227 is the one with

which the workstation makes contact. The new 8227 checks its authorization tables for the MAC entry and if none is found, the workstation will be denied access through this particular unit. If, however, it finds an entry, it will restore access along with all services via the new 8227.

Back at the original 8227, besides the static authorization table, a dynamic registration table contains the MAC addresses of all stations currently being serviced by this unit (which would include stations that have just roamed in). The entries in this dynamic table have a *time-to-live* value. If no transmission has been received from the workstation within a specified period, the 8227 deletes the entry from the table and assumes no further responsibility for it.

However, the workstation may have acquired the new 8227 before the time to live period has expired on the first 8227. So, to avoid potential problems on the LAN, the workstation immediately contacts the first unit via the LAN and informs it that a new 8227 has been found. The first 8227 then removes the table entry if it still exists. The process of switching control units in this manner is known as a hand-off, and it is this process which provides the seamless part of seamless roaming in the Wireless LAN Entry.

Note

When a workstation is enabled within range of two or more 8227s belonging to the same network of Ethernet-connected cells, it is the first unit to respond which takes and maintains control of the workstation. This does not have to be the unit with the strongest signal (although it often is). There is no decision made to hand-off to a different unit with a stronger signal. Hand-off only occurs after transmission has been broken due to frames being lost as mentioned previously.

3.6 Other Functions of the 8227 Access Point

Many of the capabilities of this device have already been discussed. It can also perform other functions not specifically related to wireless operation.

3.6.1 SNMP Agent

Simple Network Management Protocol (SNMP) is part of the TCP/IP suite of applications. It was developed as a means of acquiring status information about any node in a TCP/IP network. Many network monitoring products have since been developed which utilize SNMP and provide various levels of sophistication. Our IBM offering is NetView for AIX. A workstation running a monitoring program is usually referred to as an *SNMP manager*.

A manager is able to request and receive information about any device in the network which supports the SNMP protocol. Such devices are known as *SNMP agents*. The 8227 can be configured as an SNMP agent if required. In this capacity it is able to collect and report information relating to the workstation activity in its cell.

The information considered to be most useful in this environment is based on the concept of the MIB (Management Information Base descriptor). MIBs can be divided into the following three categories:

Standard: All SNMP capable devices support a standard set of either 174 MIBs (in the MIB-II specification) or 119 MIBs (from the earlier MIB-I specification) covering things such as the MAC address of the network adapter, operating system software and the system contact name.

Device specific: These MIBs relate to functions restricted to a particular class of device, a bridge or router for example.

Vendor specific: These MIBs have been created by a vendor specifically for that vendor's device which usually belongs to some existing device class.

The 8227 supports three MIBs specific to bridges and one IBM-specific MIB relating to wireless LAN bridge equipment. This IBM-specific MIB is responsible for collecting and forwarding the information about cell activity as previously mentioned.

3.6.2 Frame Filtering

The 8227 has a filtering capability which can be enabled during the configuration process.

Broadcast filter: If enabled, the 8227 will discard all broadcast frames moving across the LAN. A broadcast frame is a frame sent from one station to all other stations on the LAN.

Multicast filter: If enabled, the 8227 will discard all multicast frames moving across the LAN. A multicast frame is a frame sent from one station on the LAN to a specific group of stations on the LAN.

NetBIOS filter: If enabled, the 8227 will discard all the NetBIOS frames moving across the LAN except for those whose source or destination NetBIOS name begins with the characters specified in the NetBIOS name parameter of the cell members. If multicast filtering is enabled, the NetBIOS filter will have no effect on what frames the 8227 discards.

The NetBIOS name is a four character parameter. All the workstations in the cell must have a NetBIOS name beginning with the same four characters. When configured in this way, all the frames on the LAN with a destination name containing this NetBIOS name will be passed to all the cell members.

Note

If filtering is disabled (default state) on the 8227, then all the frames will be broadcast to all the workstations in the cell.

3.7 Antennas

The Wireless LAN Entry hardware includes two different types of antennas:

- Integral
- Patch

They are physically different in both appearance and transmitter characteristics. See Table 2 on page 26 for details of transmitter ranges and operating environments.

3.7.1 Integral Antenna

The integral antenna is built in to the transceiver which in turn is part of the PCMCIA Wireless adapter and is the only one which can be used in a workstation. It transmits over a 360° area with equal signal strength in all directions. In many environments this antenna will be used in both the workstations and the 8227s. An 8227, so equipped, should be mounted high up. Install it against a ceiling, for example, as close to the center of the required operating area as possible. The workstations in the cell can be arranged anywhere within the area of coverage.

This antenna should only be used in the horizontal plane.

3.7.2 Patch Antenna

The patch antenna is an alternative to the integral antenna for the 8227. It connects to the PCMCIA Wireless adapter by cable, so it may be installed some distance from the 8227 itself. The range of transmission is asymmetrical, forming two lobes of 180° each. One lobe takes the shape of a pointed dome and has a range somewhat greater than the integral antenna. The other lobe is a flattened dome and covers a much smaller area. This antenna is typically mounted high up against a wall and oriented such that the largest lobe points in the direction of the largest workstation concentration.

It is also possible to arrange workstations in the much smaller area covered by the second lobe, providing that the signal can radiate in this direction. If the antenna is mounted against a wall, then the wall construction may prevent this from happening effectively. See Figure 7 on page 40.

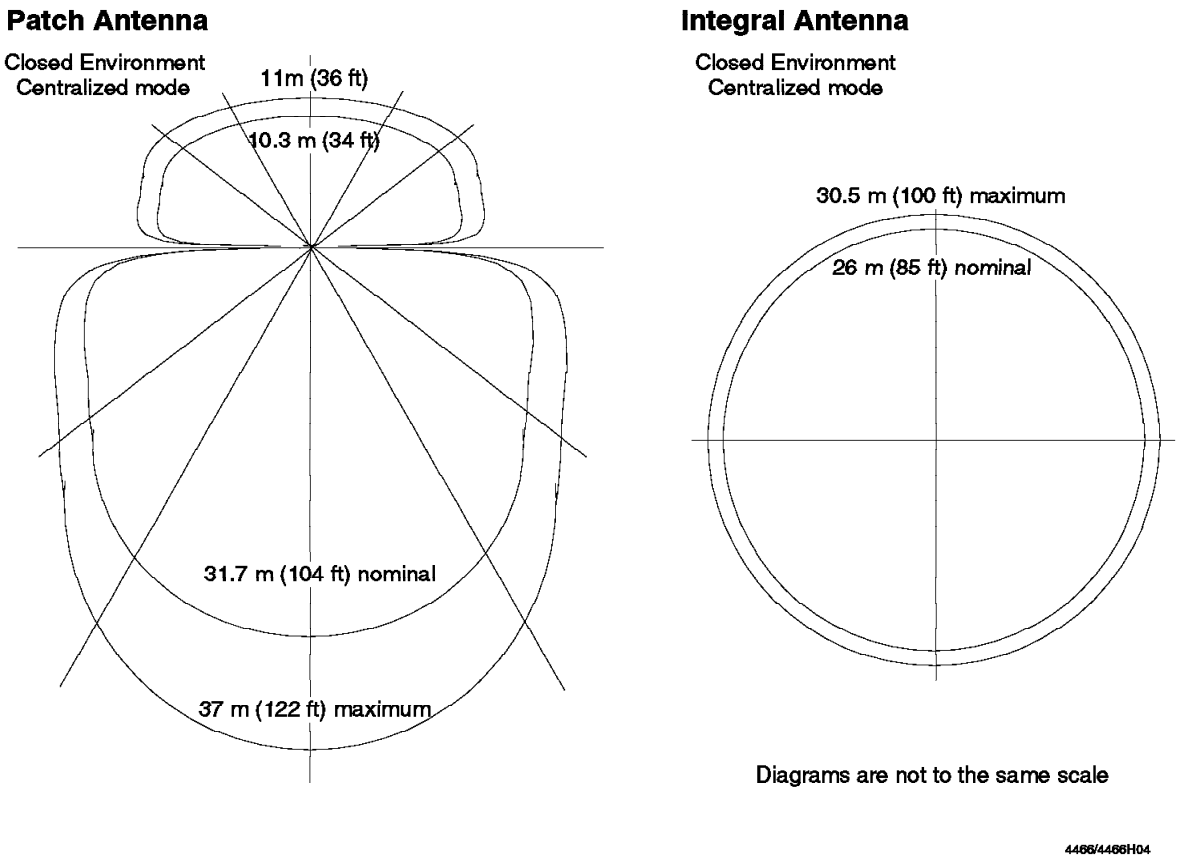


Figure 7. Transmission Patterns. Selecting the appropriate antenna is important as it can affect the overall performance of the cell significantly. The focal point is the 8227. Workstation to workstation communication is possible anywhere within the patterns.

3.8 Setup Experiences

At the time of writing, the Wireless LAN Entry product was not generally available. Our work was done in the development laboratory on both the hardware and software components as well as the various operating system and network operating systems interfaces. Our preliminary product work was carried out with a subset of the final product. The intent was to use the product and bundled software straight out of the box. The sample equipment consisted of the following:

- PS/2 9595-3NC for a RPL server
- 8227 Access Point unit with integral antenna
- ThinkPad 720c workstation with integral antenna
- ThinkPad 720 workstation with integral antenna

The server and 8227 were connected by a 10BaseT Ethernet loopback cable.

The software consisted of the following:

- OS/2 WARP and LAN Server 4.0 on the RPL server
- DOS 6.1, Windows for Workgroups and Artisoft LANtastic V6.00 on the ThinkPad 720c. This was the file server for the cell. It was also the

cell-leader in the stand-alone cell environment. Its workstation name was FEN1.

- DOS 6.1 and Artisoft LANtastic V6.00 on the ThinkPad 720. This was the client to FEN1. Its workstation name was FEN2.

The Wireless Entry software can be used with either PCMCIA Card and Socket Services or a point enabler. Card and Socket Services is a program that usually ships with a PCMCIA equipped computer. The wireless point enabler is software that ships with the Wireless LAN Entry and is found on the installation diskette. The following are two supported options for a PCMCIA port and adapter:

- Card and Socket Services (comes with later versions of DOS)
- Point Enabler Services (comes with some PCMCIA adapters)

The difference between the two options is fully explained in the *Wireless LAN Entry User's Guide*. The installation of LANtastic proceeds a little differently in either case, but at the application level there is no apparent difference. LANtastic creates a PROTOCOL.INI file during the installation; the contents of the file depend on which service was used. See Figure 8 and Figure 9. Notice that FEN1 is defined as the cell-leader and controls the hopping pattern sequence for the cell.

```
 PROTMAN_MOD
        DriverName = PROTMAN$
        DYNAMIC=YES


 IBMWINDS_NIF
;IBM Wireless Credit Card
        DRIVERNAME = IBMWIND$
        PCMCIA
        WNETID = "STEVE"
        ADHOC
        CELLEADER
        FREQUENCYSEQ = 1
```

Figure 8. \lantasti\protocol.ini File from FEN1. This is the FEN1 configuration in a stand-alone cell environment. Card and Socket Services were used for PCMCIA support.

```
 PROTMAN_MOD
        DriverName = PROTMAN$
        DYNAMIC=YES

 IBMWINDS_NIF
;IBM Wireless Credit Card
        DRIVERNAME = IBMWIND$
        IOBASE = 0x300
        INTERRUPT = 5
        RAMADDRESS = 0xC8000
        WNETID = "STEVE"
        ADHOC
```

Figure 9. \lantasti\protocol.ini File from FEN2. This is the FEN2 configuration in a stand-alone cell environment. Point enabler services were used for PCMCIA support. The extra fields were default values suggested by the installation process.

3.8.1 Building a Stand-Alone Cell

Wireless LAN Entry comes bundled with LANtastic. This combination provides all the networking software required to create a cell. Artisoft LANtastic is a fully functional network operating system with many useful features. During our scenarios however, it was only used as a connectivity tool as described below.

3.8.2 Installing Artisoft LANtastic

The LANtastic documentation suggests how to install for a Windows environment. The IBM documentation suggests installing from the DOS prompt which is simpler and yields the same result. LANtastic comes on two diskettes, the first of which is used to start the installation. The LANtastic manual suggests installing from within Windows or from the DOS prompt using a:\install\dos\win; either of which will enable both the DOS and Windows interfaces. In fact, a:\install will do everything required and create the appropriate icons in a Windows program group. However, the Windows interface was never used in our scenarios; we ran everything from the DOS prompt.

The installation is generally very straight-forward and the configuration parameters are easy to follow. The following are things to be aware of:

- The IBM documentation mentions the fact that the x:\lantasti directory must be created before installation. If this is not done, the installation may fail displaying the message `Unable to open x:\lantasti\protocol.org`.
- If reinstalling after a failed installation, look for a file called \lantast in the root directory. If it is present, delete it because otherwise the message `\lantasti directory is not valid` may appear during installation. The installation can still proceed but something other than the default directory must be selected.

At the device driver selection, select the **NDIS** option and use the Wireless LAN Entry *Diskette 1* when requested. As per the IBM documentation, when the LANtastic installation completes, don't reboot the system; quit the installation process and carry on with installation of Wireless LAN Entry, then reboot.

Hint

At the initial installation it is a good practice to define *only* one workstation as a file server; give some or all of the other clients access to a shared disk. This is because when a LANtastic client starts up it seeks all servers to which it believes it has access. It beeps every ten seconds (approximately) until either a server becomes available or the seek function is cancelled. LANtastic clients do not complete their startup sequence until one of these actions has taken place.

Since the cell-leader has to be available before anything will work in a stand-alone cell, it makes sense (for the purpose of trying connectivity as well) to have this workstation defined as the file server. In a production environment the cell-leader and server functions are probably best kept on *different* systems.

3.8.3 Installation of Wireless LAN Entry

Wireless LAN Entry also comes on two diskettes. Again, using the install program found on the first diskette is all that is required. In our environment the *Express* installation (which is easy to follow) was used. The previous part of this chapter covers all the required parameter information. One and *only one* system must be nominated as cell-leader during installation. Upon completion, the workstation is rebooted and Wireless LAN Entry should start up followed by LANtastic (which will establish connections with the server or servers).

To create a new cell from the existing workstations, Wireless LAN Entry can be reinstalled without reinstalling LANtastic. If the requirement is only to assign a different cell-leader or WnetID, then this can be done by editing the *x:\lantasti\protocol.ini* files on the workstations.

3.8.4 Connectivity

The stand-alone cell was given a WnetID of *steve* and was set up as shown in Figure 10.

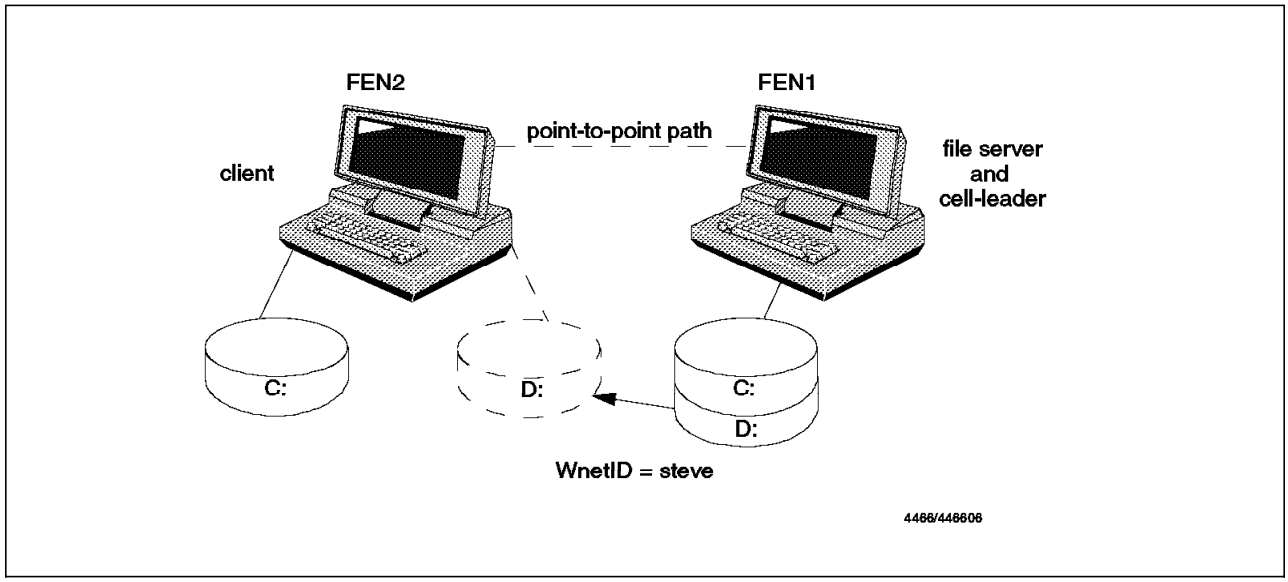


Figure 10. Stand-Alone Cell Sample Environment. The minimum requirement is a cell-leader and another workstation.

The virtual D-drive on FEN2 was the real D-drive on FEN1, this made FEN1 both the cell-leader and the file server, so it was preferable for this machine to complete its boot sequence first. If FEN2 was booted first, it would not complete the LANtastic startup until it had a response from the server. The fact that it does complete the startup indicates that communication has been established. If FEN2 had not been defined as a client, it would have completed the sequence without a pause, but it would not have been able to do any work until the cell-leader became available.

Since FEN2 was a client, it was able to switch to the virtual D-drive where all the usual DOS commands could be run. The response was pretty well instantaneous while the workstations were within about 20 meters of each other. Beyond that there was a noticeable delay which increased with separation until communication was finally lost. This was at about 40 meters in our particular closed environment.

Another simple function was to use the LANtastic *chat* function. From the DOS prompt on FEN2, the command net chat brought up a panel from which FEN1 could be called. This displayed a message at FEN1 which read: From: FEN2 I am calling you - type "NET CHAT" from DOS or select CHAT from WINDOWS.

Doing as instructed produced the same panel on FEN1 which allowed text typed at one station to be displayed at the other.

Note: Once communication is lost, DOS will eventually display the Abort, Retry or Fail? message. Moving back within the range and retrying does not seem to have any effect. It is much quicker to abort and run the command again.

3.8.5 Building an Ethernet-Connected Cell

For this environment, FEN1 and FEN2 were again used and the cell was completed with the addition of an 8227 (connected by a 10BaseT Ethernet loopback cable to the PS/2 RPL server running WARP OS/2). The workstations had Wireless LAN Entry reinstalled to define both of them as being members of an Ethernet-connected cell, but this was not strictly necessary as the changes can be made in the PROTOCOL.INI files. The same WnetID of steve was retained.

Compare Figure 11 and Figure 12 with Figure 8 on page 41 and Figure 9 on page 41.

```
 PROTMAN_MOD
        DriverName = PROTMAN$
        DYNAMIC=YES


 IBMWINDS_NIF
;IBM Wireless Credit Card
        DRIVERNAME = IBMWIND$
        PCMCIA
        WNETID = "STEVE"
```

Figure 11. \lantasti\protocol.ini File from FEN1. This is the FEN1 configuration in an Ethernet-connected cell environment.

```
 PROTMAN_MOD
        DriverName = PROTMAN$
        DYNAMIC=YES


 IBMWINDS_NIF
;IBM Wireless Credit Card
        DRIVERNAME = IBMWIND$
        IOBASE = 0x300
        INTERRUPT = 5
        RAMADDRESS = 0xC8000
        WNETID = "STEVE"
```

Figure 12. \lantasti\protocol.ini File from FEN2. This is the FEN2 configuration in an Ethernet-connected cell environment.

Notice that in FEN1, all reference to the cell-leader and its frequency hopping control have been removed. The AD HOC flag has been removed from both machines. Ad hoc refers to the way in which new workstations are added to a stand-alone cell; that is, in an ad hoc manner with the only requirement being that the workstations have the correct WnetID. This flag is what a particular workstation (other than a cell-leader) uses to determine whether it is joining a stand-alone cell or an Ethernet-connected cell.

The Ethernet-connected cell was set up as shown in Figure 13.

Caution

It is good practice to change the default WnetID from *public* to something else whenever Wireless LAN Entry is installed because, by the very nature of wireless communication it is quite possible that someone else will be setting up a similar environment close by. This happened when setting up our sample cell where the default name was retained. The development laboratory, separated from the sample cell by a number of offices and corridors, had done exactly the same thing on one of the laboratory Wireless LAN Entry LANs. The laboratory 8227 was connected to a LAN supporting various servers, domains and protocols.

At one point, someone′s workstation made contact with the sample 8227 instead of the expected laboratory unit. Since neither unit had authentication and authorization enabled, there was nothing to prevent this from happening. In fact Wireless LAN Entry was working as designed. The result was that this workstation suddenly began complaining about ″domain unknown,″ ″no response from server″ and other disturbing phenomena as a result of these things not being available on our prototype LAN.

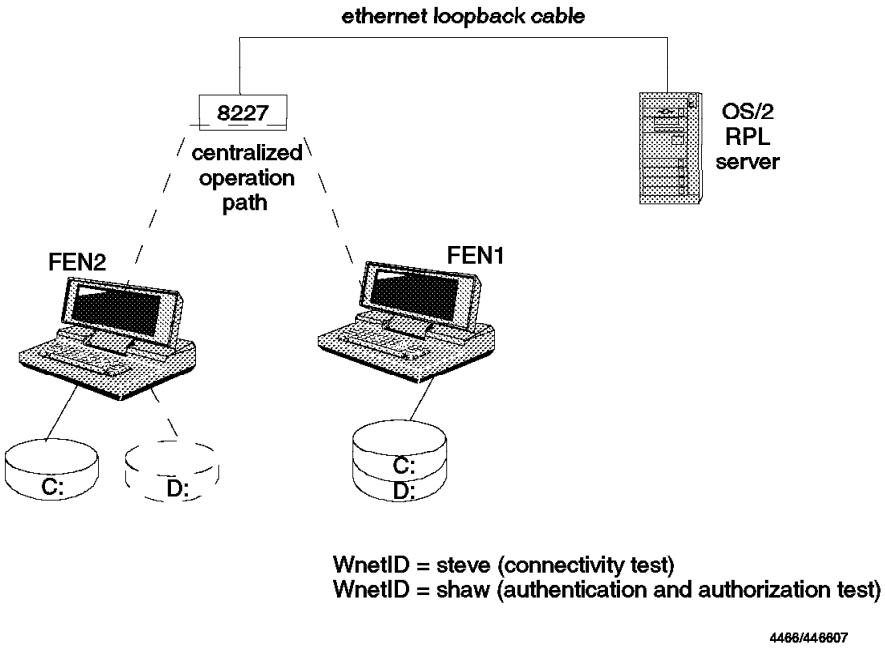


Figure 13. Ethernet-Connected Cell Test Environment. Changing from a stand-alone cell to an Ethernet-connected cell requires an 8227, LAN connection and RPL Server.

3.8.6 Creating the 8227 Configuration File

This procedure, once again, is well documented in the *IBM Wireless LAN Entry Access Point User's Guide*. It begins by making a copy of the operational software diskette. The utility diskette contains the configuration program which is copied to a DOS or OS/2 system. The program requests the configuration parameters which will be used for a particular 8227 (this is well-explained in the *8227 IBM Wireless LAN Access Point User's Guide*, GX27-4003). Once complete, the program writes the configuration out to the operational software diskette copy. This diskette is used to create the remote boot image file.

It is worth mentioning that any number of configuration files can be created on separate diskettes for an 8227 (although only one can be used at any given time). For example there may be a need to switch from centralized to non-centralized mode from time to time, or occasionally there may be a requirement to enable authentication and authorization to restrict access to the 8227 while LAN diagnostics or testing is being performed. An individual operational diskette can be created for each of these environments from which individual remote boot image files can be built on a suitable server or servers.

The same flexibility can be achieved by editing the appropriate files on the diskette and on the RPL server, but this requires a good understanding of the environment and is a less structured approach to LAN management.

Caution

An RPL server identifies an 8227 by its MAC address which is configured in the Remote Boot Image file on the server. An 8227 can have a boot image file on multiple servers, but the images must be identical. The unit will then receive the same configuration parameters regardless of which server sends the image.

An 8227 may also store multiple different images on a single server, but only one can be active at any one time. In LAN Server, this is controlled by the file *ibmlan**rpl**rpl.map*. (Don't be tempted to play with this file until you are sure of the impact your changes will have.)

3.8.7 Creating the Remote Boot Image File

The instructions for this procedure were contained in Appendix C in the documentation available to us at this particular time. The test RPL server had LAN Server V4.0 installed for which there are specific instructions for creating the remote boot image file.

Important

There are instructions under the headings *Setting Up RPL Files* and *Updating Files for DOS RPL* in the same Appendix which *must* be followed. Failure to do so will produce errors which may or may not be immediately obvious.

If you are familiar with the LAN Server interface, creating the remote boot image from the operational diskette will be straightforward. If LAN Server is new to you, take a little time making your way through the icons and configuration panels as you create your first remote boot image file. Some of this information ends up in the *ibmlan**rpl**rpl.map.* file. Using the same name for the **Image**

Name and **Machine ID** caused errors when this file was being called. Using different names avoids the problem.

When all the parameters have been entered, the *create* function reads from the operational diskette and builds the remote boot image file which should then appear in the icon window. At this point, it is worth looking at the resulting RPL.MAP file. The last line should show the MAC address of the target 8227 and details about the active image file. See the test example in Figure 14.

```
;  server record fields:
;  1    = yyyyyyyyyyy
;  2    = boot block configuration file (.cnf)
;  3    = number of retries before default boot
;  4    = time window for retries (in seconds)
;  5    = acknowledge (A,N)
;  6    = loader parameters ( for os2, image share name for dos)
;  7    = descriptive comment
;  8,9, =
;  A    = ,,,
;  B    =
;  C    = workstation type; first letter is always R
;  D,E  =

; server records
;yyyyyyyyyyy dosbbtr.cnf  3 10 N IBMLAN$ DOSTOKENRING          ,,, Z R_DTK
;yyyyyyyyyyy dosbbpc.cnf  3 10 N IBMLAN$ DOSPCNET              ,,, Z R_DPC
;yyyyyyyyyyy dosbbet.cnf  3 10 N IBMLAN$ DOSIBMISAETHERNET       ,,, Z R_DET
yyyyyyyyyyy dosbbet.cnf  3 10 N IBMLAN$ DOSIBMETHERNET        ,,, Z R_DET
yyyyyyyyyyy dosbbet.cnf  3 10 N IBMLAN$ DOSIBMIBMENIENETNDIS       ,,, Z R_DEN1_NDIS
;yyyyyyyyyyy dosndtr.cnf  3 10 N IBMLAN$ DOSTOKENRINGNDIS     ,,, Z R_DTK_NDIS
;yyyyyyyyyyy dosndet.cnf  3 10 N IBMLAN$ DOSIBMETHERNETNDIS   ,,, Z R_DET_NDIS
;yyyyyyyyyyy dosnd3ei.cnf  3 10 N IBMLAN$ DOS3COMETHERLINKII   ,,, Z R_D3CELNK_II
;yyyyyyyyyyy dosnd3em.cnf  3 10 N IBMLAN$ DOS3COMETHERLINKMC   ,,, Z R_D3CELNK_MC
;yyyyyyyyyyy dosnlae.cnf  3 10 N IBMLAN$ DOSIBMLANADAPTERFORETHERNET   ,,, Z R_DETLAE
;yyyyyyyyyyy dosnps2.cnf  3 10 N IBMLAN$ DOSIBMPS/2ADAPTERFORBNC/UTPETHERNET   ,,, Z R_DETPS2
;yyyyyyyyyyy dosn316.cnf  3 10 N IBMLAN$ DOS3COMETHERLINK16(3C507)   ,,, Z R_DET316
;yyyyyyyyyyy dosn3e3.cnf  3 10 N IBMLAN$ DOS3COMETHERLINKIII(3C509)   ,,, Z R_DET3E3
;yyyyyyyyyyy dosnwdp.cnf  3 10 N IBMLAN$ DOSSMCETHERCARDPLUSELITE16   ,,, Z R_DETWDP
;yyyyyyyyyyy dosn164.cnf  3 10 N IBMLAN$ DOSIBMTOKENRINGNETWORK16/4ADAPTERII   ,,, Z R_DTK164
;yyyyyyyyyyy dosnaae.cnf  3 10 N IBMLAN$ DOSIBMLANADAPTER/AFORETHERNET   ,,, Z R_DETAAE
;yyyyyyyyyyy dosnls.cnf  3 10 N IBMLAN$ DOSIBMLANSTREAMERMC32TOKENRING   ,,, Z R_DTKLS

; workstation record fields:
;  1     = adapter id (12 hex digits)
;  2     = workstation name
;  3     =
;  4     = image file for dos (.img), fit file for os2 (.fit)
;  5     = name of rpl server
;  6     = boot drive for OS2, domain name for DOS
;  7,8,9 = parameters for device drivers 1,2,3
;  A     = additional memory for device drivers 1,2,3. Default: ,,,
;  B     =  for os2, Z for dos
;  C     = workstation type; first letter is R -> enabled, D -> disabled
;  D     =
;  E     = volumeid string for dos, IML image file for os2

; workstation records
10OFFFFFFFFF DEFAULT  imagefile    FENWAY FENDOM    ,,, Z R_DET
;08005ADC0089 ACCESS_X  STEVE FENWAY FENDOM    ,,, Z R_DEN1_NDIS
08005ADC0089 ACCESS_Y  SHAW FENWAY FENDOM    ,,, Z R_DEN1_NDIS
```

Figure 14. \ibmlan\rpl\rpl.map. This is the image file from the test RPL server. The bottom lines describe the images for the test 8227.

In this example there are two images both for the same 8227 address. However, only one line is not commented. This one refers to the active image; that is, to the one which will be loaded on the 8227. This same image line could be repeated for different 8227s (using the same RPL server) by simply changing the MAC address.

MAC Addresses

When referring to the MAC address of the 8227, we are referring to the address of the built-in Ethernet interface *not* to the Wireless adapter. The Ethernet address is usually on a label on the face panel of the unit. The adapter address is never referenced by the software, which means the 8227 can use whatever adapter is available without any reconfiguration being necessary.

The MAC address of a workstation always refers to the address of the Wireless adapter it is using. This address is indicated on the underside of the adapter as *Net Address*.

If the MAC address label of a Wireless adapter cannot be read or is not present, there is an easy way to locate it. Put the adapter into a workstation and boot from the *second* Wireless LAN Entry installation diskette. This runs a short diagnostic program which then displays the MAC address in both canonical and non-canonical format. The canonical format is the one to use.

3.8.8 Creating a Generic Remote Boot Image File

In many environments it may be desirable to have a number of 8227s all with exactly the same configuration. It is not necessary to create a different image for each MAC address; one image with a *generic address* is all that is required. To do this, a remote boot image is created in the usual way, but instead of entering a specific 8227 MAC address when requested, the address is replaced by twelve question marks so that the field becomes **????????????**. If this is the only image on the server, then it will be downloaded to any and every 8227 which makes a remote request.

It is also possible to have images for specific 8227s coexisting with a generic image on the same server. When the server hears a remote load request, it checks the MAC address of the requester to see if it has an image specifically for that address, and if so, that is the one which will be downloaded. If not, the generic image will be sent.

Caution

Do not have a generic image on one server and a specific image on another. There is no way to ensure that the specific 8227 will receive the specific image. It all depends on which server hears the request first and will respond with whatever image it believes to be appropriate. The 8227 will load whatever it receives (specific or otherwise).

3.8.9 Booting the 8227

Assuming a valid remote boot image has been created on an available server, it is a simple matter to bring the 8227 online. The following steps will bring the 8227 online:

- Start LAN Server if it is not already running with `net start srv`.
- Start RPL Server if it is not already running with `net start rpl`.
- Push the Wireless adapter into the PCMCIA slot in the front panel of the 8227.
- Connect the 8227 to the LAN.

- Power on the 8227.

The sequence of events is:

- All the lights except the activity light come on briefly. No lights show on the adapter.
- The power, wait and link OK lights remain on; all others go off (POST check).
- After about 10 seconds, the activity light flashes and again after a further 10 seconds.
- The activity light has a couple of bursts of energy and goes off.
- Two lights show on the adapter and remain on.
- The power, OK and link OK lights remain on in the unit.
- The activity light continues to flash periodically.

The 8227 is now ready.

3.8.10 Testing the Cell

A remote boot image specific to the test 8227 was created with a WnetID of *steve*, an image name of *steve* and a machine_id of *access_x*. The operation mode was set to centralized. The WnetID on FEN1 and FEN2 was still set to *steve*. The RPL server function was started, the 8227 was powered on and the workstations were rebooted. FEN2 gave exactly the same message as it waited for FEN1 to become available. Once that happened it became possible to run the same chat function and access the D:\ drive on FEN1 from FEN2 exactly as before.

Leaving the 8227 in place, the workstations were moved away from each other to test the extended range now that the 8227 was effectively retransmitting the signal from one to the other. In the same environment, the range was found to have doubled to about 80 meters.

3.8.11 Testing the Authentication and Authorization Function

To do this, another remote boot image was created for the same 8227; this time it enabled the ASAT function where the MAC addresses of the adapters in FEN1 and FEN2 were added, along with a third address from a spare adapter. Before a new image can be created, it is necessary to edit the rpl.map file and comment out the existing line which contains the same MAC address.

Note: As mentioned earlier, this file should be treated with caution. *Always* take a backup before editing it.

LAN Server is smart enough to know that two different boot images can not exist for the same remote unit, so before a second image can be created, either the first one must be deleted or the file must be edited as described. This new image had a WnetID of *shaw*, an image name of shaw and a machine_id of *access_y*. The PROTOCOL.INI file, from which this image was created, is shown in Figure 15 on page 51.

To load this image, the RPL server was stopped with `net stop rpl` and restarted with `net start rpl`. The 8227 was powered-off and on again, and the new image loaded itself. The workstations were rebooted, and they both came up and worked as normal which was to be expected.

The adapter in FEN2 was swapped for the spare that had also been included in the ASAT table and this worked as expected. When an adapter that was not in the table was used, the workstation in question did not have access to the cell, but there was no indication given as to why this might be. This could be the cause of some confusion. To elaborate further:

When the client FEN2 had the unregistered adapter, LANtastic did not complete its startup sequence but instead displayed the message `Waiting for server FEN1 to come online ...` This is exactly the same message as was generated under the following conditions:

- FEN1 was powered off/unavailable.
- The 8227 was powered off/unavailable.

  There was no indication whatsoever that the problem was security related, instead the impression was that it was environmental.

When the server FEN1 had the unregistered adapter, LANtastic completed its startup sequence without any noticeable difference and no indication that its adapter was not valid for the cell. It was only when chat was attempted to FEN2 that it became obvious something was wrong. The displayed message was `FEN2.. Name not found on network`. Again, no indication was given as to the real nature of the problem.

These messages were generated by LANtastic not by Wireless LAN Entry. Wireless LAN Entry starts up and then goes searching for a cell-leader or 8227. LANtastic seems to start up regardless of whether communication has been established or not. This is true unless the workstation needs access to a server, in which case start up will not complete until contact has been made.

However, the authentication and authorization function obviously works.

```
;*****************************************************************
;*****************
; Protocol Manager
;*****************
 PROTMGR
     DRIVERNAME  = PROTMAN$

;*********************************
; IBM Wireless Network Access Point
;*********************************
 IBMACPT
; IBM Wireless Access Point

; - Comment lines beginning with "; -" must be present !!!
; *** General ***
; - Protocol Driver name          (Ended with $)
     DRIVERNAME = IBMACPT$
; - MAC Drivers being bound       (Wireless,Ethernet)
     BINDINGS   = IBMWIND$,IBMENAP
; - Operation Mode                (Following line & next must be presen.)
     Centralized
; - Wireless Network Identifier   (6 char string, Double quotes require)
     WNETID = "SHAW"

; *** SNMP Agent ***
; - SNMP Agent IP address         ( DoubleQuotes required )
; ---IpAddress--- Config needs this, don't erase!
; - SubNet Mask                   ( DoubleQuotes required )
; ---SubNetMask---Config needs this, don't erase!
; - Default Gateway on Enet side  ( DoubleQuotes required )
; ---DefGateway---Config needs this, don't erase!

; *** Wireless Network / Access Point ***
; - Hopping Pattern name          ( Name, HPxxx format)
     Pattern = HP011

; **** B/Mcast filtering options ***
; The keyword is: FILTER=<R>+<N>+<O|G|B|M>
; R - Rate control on.
; N - NetBios Name on. Use NBNAME="ABCD" and FADDRESS="030000000001"
; O - Open path (no filtering)
; G - Global filter. Both Mcast and Bcast
; B - Broadcast only (filter)
; M - Multicast only (filter)
     FILTER = R
; ---NBNAME--- Config needs this, don't erase!
     FADDRESS = "030000000001"

; - Address specific authorization table ( DoubleQuotes required )
        Authorize001 = "08005ADC006F"
        Authorize002 = "10005A3B002B"
        Authorize003 = "10005A3B0008"

; - Address range authorization table    ( DoubleQuotes required )

;*****************************************************
; NDIS MAC driver - Built-in Ethernet Card
;*****************************************************
 IBMENAP
    DriverName = IBMENAP$

 IBMWIND$
    DriverName = IBMWIND$
    IOBase = 0x340
    RAMAddress= 0xCC000
    Interrupt = 7
    WnetID = "SHAW"

;*****************************************************************
```

Figure 15. \protocol.ini File from the Operational Diskette. This file describes the 8227 configuration used in the authentication and authorization test. It is used to create the Remote Boot Image on the RPL server.

Note: *If you intend to change the WnetID by editing this file, it must be done in two locations.*

3.8.12 Booting from a Novell RPL Server

Using Novell as the RPL server is just as easy as using LAN Server. However, a Novell Client workstation is required to create the image and upload it to the server. The same operational diskette as used with the OS/2 RPL server can be used with the Novell server if there is no need to change configuration parameters for the 8227.

If a different configuration is required, a new diskette can be created or the PROTOCOL.INI file on the diskette can be modified. The instructions for using Novell were in Appendix C in the level of documentation available during the evaluation.

The Novell RPL server used for the test was already attached to an existing development LAN. The remote boot image file, which was created for the test unit, was given a WnetID of *sammy* for reasons which will be explained later. See 3.8.13, " Building a Network of Ethernet-Connected Cells." Loading this new image was simply a matter of powering off the 8227, disconnecting from the test LAN, reconnecting to the development LAN and powering back on. The new image loaded from the Novell server without any problems.

At the workstations FEN1 and FEN2, the *\lantasti\protocol.ini* files were edited to give them a WnetID of *sammy* and rebooted. Both systems worked exactly as before.

This new setup was used to perform roaming tests.

3.8.13 Building a Network of Ethernet-Connected Cells

To do a realistic roaming capability scenario would require a number of 8227s on the same LAN, separated by distances approaching the antenna range for the environment in which they were being used. In other words, a network of Ethernet-connected cells. This was unfortunately not available to us at the time of our work. Our sample environment was as shown in Figure 16 on page 53.

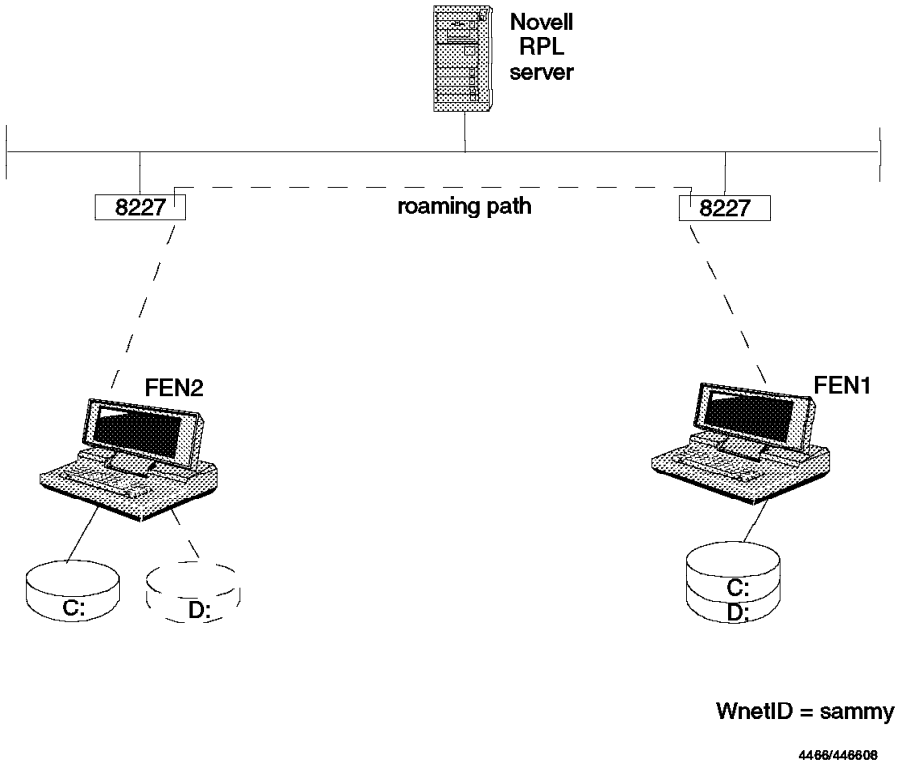


Figure 16. Network of Ethernet-Connected Cells Test Environment. This scenario was used for both the Novell remote boot image load and the roaming examples. FEN1 continues to be the file server (shared D-drive) for FEN2. Neither one of the 8227s had authentication and authorization enabled.

Two access points on the LAN allow roaming to occur. The communication path between workstations can be through either one of the 8227s or through both as shown here. The path switched frequently and seamlessly during the roaming test.

As was explained earlier in this chapter, for roaming to occur there must be at least two cells on the same LAN having the same WnetID. The cell adjacent to the test cell had a WnetID of *sammy*, so the test unit also had to be *sammy*, as did the workstations FEN1 and FEN2.

In this scenario it is likely, but not guaranteed, that a workstation, when it boots, will acquire and register with the nearest 8227 of the right configuration. When FEN1 and FEN2 were booted, they were right beside the test 8227 and it was obvious which one they acquired by watching the lights on the adapters flashing in a synchronized manner. This was also apparent when any kind of communication was happening between FEN1 and FEN2.

Roaming occurs when an 8227 to which a workstation is registered becomes inaccessible, forcing the workstation to search for another. Being *out-of-range* is just a special case of being inaccessible. The test unit was made inaccessible by powering it off. This was done in the middle of a chat session between the workstations to see if it would kill the session, however, it did not do so. It took less than a second for the new 8227, which was about 25 meters away (along a corridor and behind two walls), to be acquired by both workstations. There was a slight delay in the response at the receiving end of the chat session. This was probably due to the retransmission of some characters. However, performance was still perfectly acceptable.

The chat session was kept actively running (by pressing the same key continuously on the sending station) while re-booting the test 8227. Within a few seconds it was apparent by the improved response and the adapter lights that the workstations had both re-acquired the second unit. This seemed to be an effective verification of *seamless roaming*.

After this, one of the workstations was moved around the floor, leaving the other in its usual location (exactly as had been done when testing the single Ethernet-connected cell previously). From the far side of the second 8227 the communication range had been extended by about 10 meters. Presumably this was because each workstation was now registered with a different 8227 and the physical separation between them was providing the greater range.

Had the floor layout and the LAN accessibility allowed for the arrangement of the 8227s and the workstations been in a straight line instead of a *Z-shape*, the effective range in this closed environment would have been increased significantly.

In Figure 16 on page 53, two workstations in different cells are communicating via 8227s on the same LAN. The way this happens is that one workstation initiates a call to the other. The call goes to the 8227 with which it is currently registered. The 8227 checks whether or not it is also servicing the requested workstation. In this case it isn't, so it broadcasts the request onto the LAN. All 8227s on the LAN see the broadcast and check their own dynamic registration tables for the requested address. The second 8227 in the figure would recognize that it was servicing this address and would forward the frames to the second workstation. All subsequent frames in either direction are handled in the same manner.

This sequence of events applies regardless of whether workstations are roaming or fixed.

3.8.14 TCP/IP and Wireless LAN Entry

As already mentioned, Wireless LAN Entry comes bundled with Artisoft LANtastic. As far as networking protocols are concerned, however, TCP/IP is the unchallenged de facto standard for multi-vendor, multi-platform connectivity. The phenomenal growth of the Internet over the last few years is clear proof of this. The demand for TCP/IP enabled products is likely to continue to grow in the foreseeable future. Wireless LAN Entry supports the TCP/IP protocol suite so any application currently using TCP/IP networking protocols in a wired LAN should run unchanged in the Wireless LAN Entry environment.

TCP/IP was installed on the workstations FEN1 and FEN2. No hardware changes were necessary. LANtastic and TCP/IP can coexist on a DOS machine, but only one or the other can be started at any one time. This means that to switch environments, the AUTOEXEC.BAT and CONFIG.SYS files must be edited to select different device drivers and startup files before re-booting. This is a task made easier beginning with PC/DOS 6 which provides a capability to selectively load system files upon IPL. A menu system that does this for the IBM Wireless LAN product is described in C.4, "Using the DOS Menu Function" on page 125. A similar system may be readily adopted for the Wireless LAN Entry with appropriate modifications.

This installation is a little involved but again is well documented in a step by step manner. The *Custom* program from DOS TCP/IP is invoked which installs

the appropriate device drivers from the Wireless LAN Entry diskettes. After this the system is rebooted and TCP/IP is enabled for the Wireless adapter. TCP/IP applications can now be run, providing the TCP/IP parameters have been configured properly,

3.8.15 Connectivity

In our environment, the *ping* command was run between both workstations and between the workstations and the RPL server. This verified that there were communication paths from air-to-air and air-to-wire.

After this, a file transfer was attempted between workstations. Using FTP (File Transfer Protocol) a 1 Mb ASCII file was transferred in both *binary* and *text* mode. It transferred in less than half the time taken by NetBIOS used in LANtastic. The transfer was repeated while roaming between 8227s. If one station or the other roamed beyond a cell boundary while the transfer was taking place, there was a halt in transmission; provided the workstation came back in range before the FTP *time-out period*, transmission would resume. Since these scenarios were not carried out in a reproducible manner or with any kind of consistency, the actual transfer times do not have much value. However, the process did demonstrate the functionality of the Wireless LAN Entry product set.

3.8.16 Tools

There is at least one tool available which can greatly assist the positioning of workstations and 8227s for maximum coverage.

As has been alluded to earlier in this chapter, a workstation will not switch from one 8227 to another on signal strength alone. If the weaker signal is giving uninterrupted transmission, the workstation will continue to use it.

The *SiteTest* tool is part of the product set. It actively monitors the signal-to-noise ratio at any given point and also averages it continuously. This information can be stored and retrieved later. If a number of points are monitored in a specific location, all the saved data can then be plotted onto a plan of the site to produce a map of effective and marginal coverage.

SiteTest also displays information about which 8227 is being accessed. Again, this was found to be a very useful tool on a mobile workstation.

Chapter 4. IBM Wireless LAN

The IBM Wireless LAN (WLAN) is a local area network system that can operate as a completely self-contained system or that can interoperate with traditional wired LANs. It is a limited-distance system that can support upwards of 50 stations or more. It can bridge to functions and services of wired LANs, extending the range of WLANs to access other servers or host systems. IBM Wireless LAN components can be installed in most PC systems and may operate in different LAN environments using different protocols.

The IBM Wireless LAN product includes network management and comprehensive security functions for the wireless network. An SNMP agent function is provided in IBM Wireless LAN.

The IBM Wireless LAN is designed to use advanced radio technology and protocols using spread spectrum, frequency hopping and time division multiplexing, which provides a high level of interference protection.

There are many advantages in using radio waves instead of conventional LAN wiring media such as:

- High flexibility and mobility
- Cost reduction and ease of installation which is beneficial for companies who have several moves per terminal per year
- Ability to extend already existing wired LAN installations:
  - Changes can be done very easily as the number of users grows.
  - If the performance decreases the cells can be split (by adding a new base).

The following are some significant benefits for users:

Reduces cabling costs

Increases reliability and performance

Includes security aspects

Use of mobile applications for portable computers

Easy and flexible extensions for wired LANs

Minimal environmental restrictions

4.1 IBM Wireless LAN Product Functionality

- IBM Wireless LAN uses radio wave propagation in the ISM bands.
- IBM Wireless LAN consists of two unique adapters with external antenna modules; these are installed in client and/or server workstations. ISA or MCA bus systems or those with PCMCIA slots are accommodated. A unique card design enables one adapter to be installed in either an ISA or an MCA bus machine. The adapters handle both the physical and the MAC layer.
- The following are characteristics of the PCMCIA adapter:
  - The IBM Wireless LAN PCMCIA card meets PCMCIA type 2 standard specifications V2.1.

  - The low power radio design and power management minimizes the power usage of a portable stations battery.
  - It runs in the same systems and environments as IBM Wireless LAN ISA/MCA but cannot be configured as a Base station.
  - LAN PCMCIAs can be intermixed with LAN ISA/MCAs.
- A Wireless cell is built by a *base station* and one or more wireless workstations. All traffic goes through the base station. Such a cell acts as a LAN segment and can be stand-alone or bridged with a wired LAN. Cells may also overlap depending on the configuration.
- Wireless network administrators can perform administration for their own cell and for other cells. These functions include management, security and control.
- Security mechanisms, for the IBM Wireless LAN provide several levels of security. The radio uses complex modulation techniques which make the signal difficult to receive with equipment other than the Wireless LAN adapter itself. The built-in and specific security functions include wireless network access control and radio transmission encryption. The encryption mechanism provides adequate protection for most applications. User management is responsible for selection and implementation of security features, administrative procedures and appropriate controls in application systems and communications facilities. See 4.4, “Security of IBM Wireless LAN” on page 63 for more details of security in IBM Wireless LAN.
- LAN/PCMCIA adapters can be configured to be a wireless Base station or wireless workstation (PCMCIA adapters have some restrictions as a Base station).
- Transparent mobility support is provided for roaming stations.
- IBM Wireless LAN uses spread spectrum, frequency hopping, and TDMA (Time Division Multiple Access) with intelligent interference protection.
- Data compression can be done at the base station as well as at the wireless workstation. To be able to decompress the data at the receiver, both stations have to follow the same compression algorithm. Only data information can be compressed. Compression can increase overall data throughput.
- TDM (time division multiplexing) ensures efficient use of the available channel bandwidth and sustained performance when the number of users increases.
- Frequency hopping patterns are used by each cell and are controlled from the network administrator according to an intelligent interference management system which monitors the HF (high frequency) communication and detects interfering signals. The pattern is changed if interference is detected.
- Connectivity is provided for token-ring and Ethernet LANs.
- IBM Wireless LAN in an OS/2 environment
  - To use the IBM Wireless LAN in an OS/2 environment, the base needs to have OS/2 V2.1 or higher installed.
  - For a wireless connection to a wired LAN, the base also needs a wired LAN adapter.

- IBM Wireless LAN provides a *source-route bridging* function to communicate with a token-ring LAN.
- IBM Wireless LAN provides a *transparent bridging* function to communicate with an Ethernet LAN.
- TCP/IP for OS/2 V2 (or higher) is required to allow the IP protocol to be *routed* either within or from a wireless cell.
- The NAP (Network Administrator Program) may be installed in the base of a single cell network or within any cell of a multiple-cell network.
- Wireless workstations can run on DOS (with or without Windows) or on OS/2.

• IBM Wireless LAN in Novell networks

- Using IBM Wireless LAN in a Novell NetWare environment, the base station is the server for a wireless cell and may be connected to a wired LAN. The cell is a LAN segment, and the NetWare routing function performs communication for IPX or TCP/IP clients in the cell.
- The NAP (Network Administration Program) may be installed in a base station or within any other NetWare server in a wired LAN.
- Wireless workstations can run on DOS (with or without Windows) or OS/2 with NetWare requester.

4.2 Enhancements

The IBM Wireless LAN product family has been recently enhanced with significant new functions. These enhancements were released after the completion of our work but before release of this book. We will discuss them briefly here but have not had an opportunity to explore them further.

One of the major functional improvements for the IBM Wireless LAN is in the area of *seamless* roaming. It is now possible for a WLAN client workstation to roam across cells of coverage provided by base stations and to maintain sessions without interruption (stations must still be within their own sub-nets to maintain router-based connections). This requires a hand-off from one base station to another and is accomplished transparently to the end user. This is supported for clients in both ODI and NDIS environments where base stations can be on either token-ring or Ethernet networks.

Ethernet support provides the ability to bridge or to route protocols from the wireless network to a wired Ethernet through a base station. Improvements have been made in the base station token-ring bridge that support a new dynamic filtering capability for broadcast traffic originating on the wired segment of the network.

Software support for LAN Server 4.0 (including the ability to support a server in a Base station) has been added. It is now possible to support multiple NETIDs from a single NAP station, while a full view of remote station status in the WLAN network can now be seen. These new features expand the application and management capabilities of the IBM Wireless LAN.

Lastly, power management for PCMCIA-based wireless stations has been improved to increase battery life.

4.3 IBM Wireless LAN System Architecture

The following description will present how different entities correspond to each other:

- **Devices**

  The following main devices comprise the IBM Wireless LAN architecture:

  Base station
  This is the device through which all communications on the air interface must pass.

  Wireless workstation
  This is the device which offers wireless LAN attachment to the end user.

  Backbone attachment
  This is the device which allows the attachment of the wireless LAN to a communication backbone network.

  Network station
  This is the device which coordinates administration for one or more base stations in a wired LAN.

- **Functions**

  From a functional point of view, the following functions can now be defined:

  RF connectivity function
  This function allows the establishment of a connectivity path on the transmission media (or air interface). This function can be compared to the LAN connectivity function which is provided by the wired LAN adapters.

  Cell controller function
  This function performs the scheduling of the different resources sharing the same communication media (a frequency bandwidth available on the air interface). This function can be compared to the polling function allowing it to share the same multipoint TP line among several stations. The cell controller uses the transmission protocol known as the *French Protocol*. It is a hybrid TDMA/CSMA system for a good balance of performance and fairness.

  Relaying function
  This function allows either bridging of MAC layers or routing of network layers between the Wireless LAN and a Wired LAN. When two wireless workstations of a same cell communicate between each other, the relaying function performs an Inter-cell bridge. The precise level of functionality depends on the type of wired LAN and networking operating system. Please refer to Table 3 on page 67.

  Network control function
  This function is required to define the control functions and is aimed to ensure proper operations at the network level. The network control function addresses various aspects such as registration, access control, frequency hopping pattern control, etc. However, it does not correspond to the steady state data transfer.

- **Layers**

  Considering the IBM Wireless LAN from an architectural perspective, it follows an OSI model using layers similar to common LAN communication technologies.

  Physical layer
  The RF connectivity function belongs in this layer.

  MAC layer
  The cell controller functions (French Protocol) belongs in this layer.

  Upper layer to the application layer
  The relay function corresponds either to a MAC layer - MAC layer relay or an LLC/DLC layer - LLC/DLC layer relay, depending on the level where the relay is performed. The network control functions are spread across the layers above the MAC layer.

To establish a relationship between a device and its function, it is necessary to describe the network. The network can have a single cell or multiple cells. The cells can either overlap or not overlap. Interconnection to a backbone network can be either present or not. Ad hoc networking is not permitted. According to the nature of the network, the following relationships between a device and its function can be defined.

- Base stations and wireless workstations always implement the RF connectivity function.
- Base stations and wireless workstations always implement the cell controller function.

  Some additional distinction must be made on the cell controller function. The multiple access protocol used to control the sharing of the communication media is not a peer-to-peer protocol, but rather an unbalanced protocol.

  We can define the primary and secondary parts of the cell controller functions. The relationship can be refined by associating the base station to the primary part of cell controller function and the wireless workstation to the secondary part of the cell controller function.
- The relaying function is always associated with a base station; it may be implemented in a backbone attachment device.
- The network control function is implemented in a network station by a component called the Wireless Network Controller (WNC) and Wireless Control Agent (WCA). The WCA function is always implemented in the base station to ensure proper operations at the cell network level. The location of WNC can also vary according to the network topology. For a single base station, the WNC will be part of the base station device. For more complex networks having a wired backbone network, the network station can be situated in different locations. They can be located either in a specific base station device or in any other relevant location connected to the backbone. The WLAN architecture has provisions allowing the base station to address and interface the network station regardless of its physical location. The WCA is the functional entity allowing it to interface the WNC.

The following figures summarize the communication architecture for some different network environments.

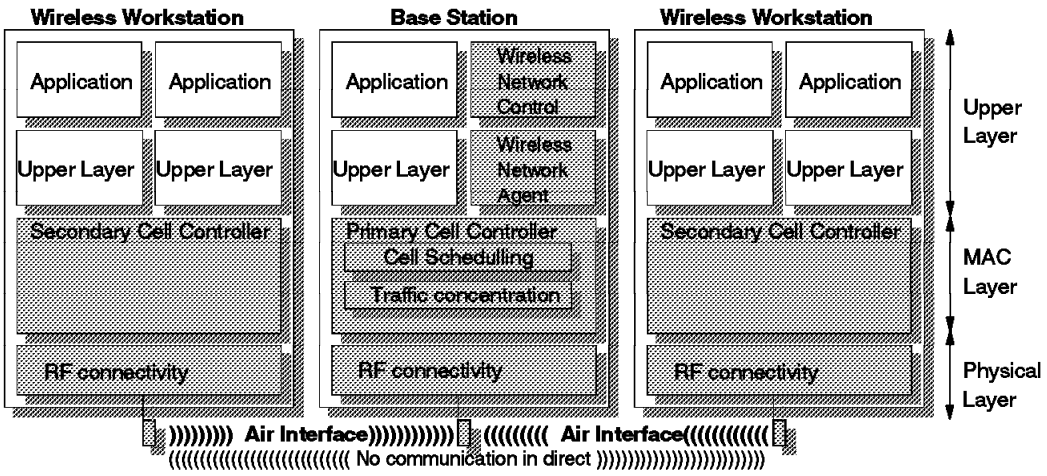


Figure 17. Single Base Station Controlled Network

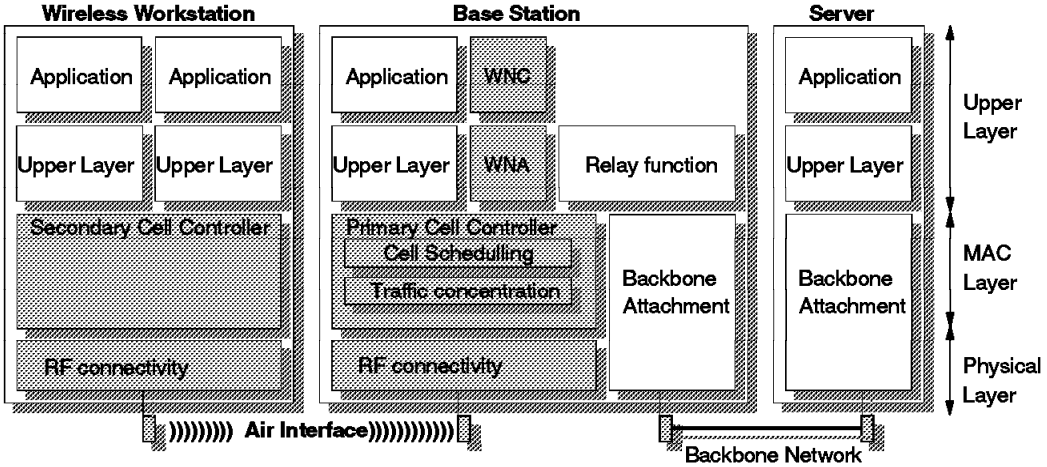


Figure 18. WNC Within the Base Station (Multiple Bridging Base)

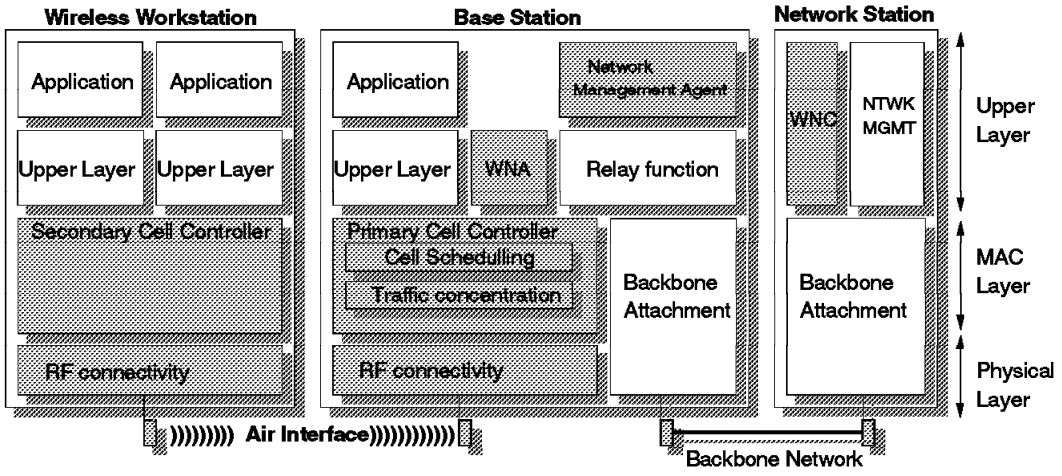


Figure 19. WNC Within the Network Station (Multiple Bridging Base)

4.4 Security of IBM Wireless LAN

There are multiple security objectives incorporated into the design of the IBM Wireless LAN. One is to minimize the risk of an unauthorized intrusion either deliberately or inadvertently. Another is to ensure the integrity of the information transfer.

The security of the IBM Wireless LAN addresses the following three requirements:

1. The user data must be masked at a medium level and not at a higher level to maintain transparency of the wireless LAN to the wired network to which it may be connected. The masked data is confined to the wireless LAN of the network only.
2. Protect the wireless segment against outside influences.
3. Access to the wireless network must be controlled in such a way that only authorized users may enter the network. The authorized users are those who are known by a network control entity and are registered in its data base.

The following mechanisms cover the previous requirements:

Registration: This is the process by which a wireless workstation asks a base station to join a cell.

Authentication: This is the process by which the base station and the wireless workstation ensure that their partner is who it claims to be. This procedure precludes any unknown station trying to pretend to be a proper station.

Access control: This is the process by which the base station verifies that the candidate wireless workstation is authorized to be registered in the network.

Data masking, key building and sharing: This is the process by which both parties share a common data-masking key. To make the process more secure, a new key is used with the establishment of each connection.

Base and wireless workstations: These scramble and de-scramble data streams on the air interface.

Data authentication and integrity: These are the processes used by each party to ensure that any data received has been sent by a recognized and authorized sender.

The IBM Wireless LAN provides the following comprehensive and rigorous security functions as installation-specific implementation options:

- At installation time, stations are registered in the wireless network by the exchange of system-generated software security keys between the station user and the *Wireless Network Administration Program*.
- During network access, wireless stations are automatically authenticated based on these security keys.
- Over and above the preceding, users may choose to have data encrypted for radio transmission.

4.5 IBM Wireless LAN Network Control

The purpose of network control is to provide all operational adapter functions which are over and above normal data transfers.

4.5.1 Location

The network control layer function is split into two components:

1. The **Wireless Network Controller** is a centralized managing function/program operating in a specific station. This station keeps the network resident data, wireless station′s name and address, and the Wireless LAN topology. This application can run in any workstation on the backbone LAN, whether it is a Base station or not. For multi-segment LANs, there is a unique wireless network controller for each wireless LAN network. However, it can be split into several wireless networks, each of them having a separate Network ID and wireless network controller.
2. The **Wireless Control Agent**, located in every base station linked to a wireless network controller, is implemented in the base station or a backbone network and acts as a representative for the Wireless Network Controller in the base station. It works as a cell control by keeping the network data specified to its cell. It is responsible for opening and closing a base station′s wireless adapter and checking a registered wireless workstation according to its access control data. The Wireless Control Agent manages the frequency hopping pattern of its cell.

4.5.2 Network Control Functions

The following functions are performed at the network control level:

- **Registration Control**

  When a base station is activated, it is registered by the Wireless Network Controller program. The wireless network controller returns a confirmation

message carrying the necessary network resident data along with the base station configuration data.

To avoid a wireless workstation hearing more than one base station, adjacent base stations are provided different addresses. The wireless network controller allocates the (radio link) local-identifier address to the base station using the *French protocol*.

At the completion of the authentication procedure, the base station adapter forwards the registration request to the wireless control agent to access network control parameters. The Wireless Control Agent returns the result to the base station adapter. Then the Wireless Control Agent passes this event information to the network management platform in use. When the base station adapter informs the Wireless Control Agent that a wireless workstation is leaving the cell, the Wireless Control Agent again notifies the network management program in use.

- **Frequency Hopping Pattern Control**

  If a base station encounters too much interference, the adapter can ask for a new frequency hopping pattern for the IBM Wireless LAN device driver. The wireless network controller does not perform this function. The IBM Wireless LAN adapter also has interference management resident. The Wireless Control Agent may receive notification from a device driver if any frequency value is experiencing excessive interference resulting in high retransmission units.

- **Network Resident Data Control**

  The network resident data are recorded in the Wireless Network Controller and distributed to the base stations when necessary. The data is identical for all the base stations and is entered at the operator console. The Network Administrator Program consists of the following:

  – Network name
  – Base station name
  – Access control
  – Network key and name

- **Access control**

  This network control function is optional and it allows a restriction of the workstation′s access to the network by specifying that it may communicate on specific days, or at specific times, or with specific base stations, or all of these.

- **Distribution of encrypt network key and name**

  This network control function is optional. The network key and name is used in the authentication procedure and encryption/decryption of data between the base station and wireless workstations. There is one key per network. The network key and name may be determined by Wireless Network Controller and distributed to the base stations. They are stored in an IBM Wireless LAN adapter through the Wireless Control Agent program.

4.6 Requirements

The IBM Wireless LAN is capable of performing in a wide range of conditions, both operational and environmental. There are fundamental requirements from a hardware and software point of view that must be met to ensure proper operation. These are addressed below.

4.6.1 Hardware

- A wireless base station using the IBM Wireless LAN ISA/MCA adapter consists of:
  - An IBM Personal System with ISA or MCA bus with at least a 386 processor (the station does not need to be dedicated).
  - 4 MB RAM or more is required depending on other programs operating with the system. The IBM 32-bit DMA is required if RAM storage is above 16 MB.
  - A 3.5-inch 1.44 MB diskette drive.
  - A hard disk.
  - An available feature slot for the Wireless LAN adapter card.
  - A LAN adapter if attachment to a wired LAN is desired.
- A wireless workstation using the IBM Wireless LAN ISA/MCA adapter consists of:
  - An IBM personal system with an ISA or MCA bus.
  - A 3.5-inch 1.44 MB diskette drive.
  - A diskette drive and/or a hard disk may not be required if RIPL (Remote Initial Program Load) is used.
  - An available feature slot for the Wireless LAN adapter card.
- A wireless workstation using the IBM Wireless LAN PCMCIA adapter consists of:
  - An IBM ThinkPad system with a PCMCIA type II feature slot
  - A 3.5-inch 1.44 MB diskette drive
  - A hard disk
- A wireless network administrator station (if not installed on the wireless base station) requires the following:
  - An IBM personal computer
  - A 3.5-inch 1.44 MB diskette drive
  - A hard disk
  - A LAN adapter attached to the wired LAN

4.6.2 Software

- The Novell NetWare environment consists of:
  - Wireless base station

    NetWare Version 3.11 or above (including the TCP/IP protocol stack if there are multiple wireless cells that are to be managed centrally).

- Wireless workstation

  Either OS/2 Version 2.1 or above and NetWare workstation for OS/2, or DOS 5 or above (DOS 6.0 for the IBM Wireless LAN PCMCIA) and a NetWare requester (NetWare ODI shell for DOS or NetWare Lite or NetWare workstation for DOS/Windows)

- Wireless network administrator (if not installed on a wireless Base station)

  NetWare Version 3.11 or above (including the TCP/IP protocol stack)

• The OS/2 LAN environment consists of:

- Wireless base station which requires:

  OS/2 Version 2.1 and NTS/2 (with CSD WRF7020 if the token-ring bridging is used). If there are multiple wireless cells, TCP/IP for OS/2 Version 2.0 (with CSD UN5.382 if SNMP network management is used)

- Wireless workstation which requires:

  Either OS/2 Version 2.1 and NTS/2 or DOS 5 or above (DOS 6.0 with Wireless LAN PCMCIA) and IBM LAN Support Program Version 1.33 Version 1.35 is required to support NetBIOS and 802.2 double binding).

- Wireless network administrator (if not installed on a wireless base station) requires:

  OS/2 Version 2.1 and TCP/IP for OS/2 Version 1.2.1

4.7 IBM Wireless LAN Connectivity

The wired LAN can include bridges or routers. This allows you to organize groups of users into different cells in different wireless networks. All users share the same resources, regardless of geographical proximity.

Table 3 shows the possible types of bridges to use depending on your environment and the type of wired LAN you are using.

Table 3. LAN Connectivity

Environment	Wired LAN Type	Connectivity to Be Used
NetWare	Token-ring, Ethernet, or any media type supported by NetWare	IPX or TCP/IP routing provided with NetWare
OS/2	Token-ring	Source-route bridge
OS/2	Ethernet	Transparent bridge
OS/2	Token-ring, Ethernet or any communications supported by TCP/IP for OS/2	IP routing provided with TCP/IP for OS/2

4.8 Network Management

If you have several cells connected to a backbone LAN network, we recommend that you manage your wired LAN cells and other resources of your network from a single point. A network management station can be connected to the wired LAN for the following:

- It can efficiently manage your wireless network by displaying alerts and messages received from base stations.
- It can act as a service point.

The network management station must use Simple Network Management Protocol (SNMP). Stations such as IBM NetView for AIX or Novell NMS can be used.

The SNMP protocol defines Traps as a method to send unsolicited notifications from a base station to the network management station. Traps reporting problem conditions include additional information which allows NetView for AIX to convert a Trap into a generic alert. This in turn may be sent to a host NetView (running on a mainframe). A NetView for AIX operator or automation program can also issue SNMP requests which are sent to the base stations.

Note: Although a network management station is optional, it is strongly recommended that you install one in your Wireless LAN.

4.8.1 Novell NetWare Environment

The IBM Wireless LAN extends the facility provided by the Novell Simple Network Management Protocol (SNMP) agent for Novell NetWare. The following Management Information Bases (MIBs) are supported:

- MIB II
- The IBM Wireless LAN-specific MIB

The IBM Wireless LAN-specific MIB contains information about the base station and all wireless workstations connected to the base station. The GET and GET-NEXT SNMP operations are supported on all the management objects and can be issued from any SNMP manager, such as IBM NetView for AIX or Novell NMS. The IBM Wireless LAN initiates SNMP traps in response to various events, such as configuration and security problems. For more information about the IBM Wireless LAN SNMP facility, refer to *Setting Up Network Management for NetWare in IBM Wireless LAN* in *Installing and Operating Your Network* provided with the IBM Wireless LAN product.

4.8.2 OS/2 Environment

The IBM Wireless LAN extends the facility provided by the SNMP agent of TCP/IP for OS/2. The follow MIBs are supported:

- MIB II
- The IBM Wireless LAN specific MIB
- The bridge MIB (RFC1286)

The IBM Wireless LAN-specific MIB contains information about base stations and all wireless workstations connected to the base station. The GET and GET-NEXT SNMP operations are supported on all the management objects and can be issued from any SNMP manager (such as IBM NetView for AIX or Novell NMS).

The IBM Wireless LAN initiates SNMP traps in response to various events, such as configuration and security problems. For more information of IBM Wireless LAN SNMP facility, refer to *Setting Up Network Management for OS/2* in *IBM Wireless LAN Installing and Operating Your Network* provided with the IBM Wireless LAN product.

4.9 IBM Wireless LAN Configuration

The IBM Wireless LAN product offers two basic types of connectivity:

- Stand-alone cell

  In the stand-alone cell, the base station:

  – Is unique.
  – Manages the data traffic in the cell.
  – Contains the Network Administrator Program (NAP), which allows you to perform administration tasks such as access control. For more details of NAP, refer to 4.12, “Network Administrator Program” on page 93.

  In the stand-alone cell, the wireless workstations:

  – Are used as LAN workstations by end users

  – Are identified by the base station

  – Can communicate with the base station and other wireless workstations

  A stand-alone cell is composed of a base station and up to 50 connected wireless workstations. The number of simultaneous users in a cell depends on the type of data traffic.

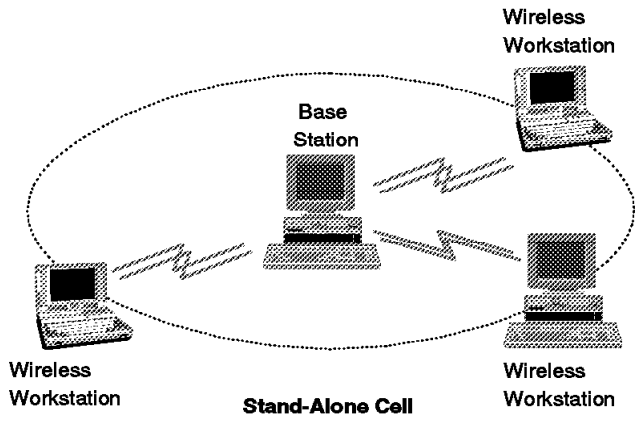


Figure 20. Stand-Alone Cell Configuration

- Backbone-attached cell

  In the backbone-attached cell, the base stations:

  – Are one per cell
  – Are connected to the backbone network
  – Manage the data traffic within their cell

  One base contains the NAP which allows you to perform administration tasks such as access control and base list definitions. For more details of the NAP, refer to 4.12, “Network Administrator Program” on page 93.

In the backbone-attached cell, the wireless workstations:

- Are used as LAN workstations by end users
- Are identified by the base station
- Can communicate with any server or workstation connected to backbone network
- Can communicate with base stations and wireless workstations in any cell

Figure 21 shows an example of token-ring LAN and Ethernet LAN as a mixed network.

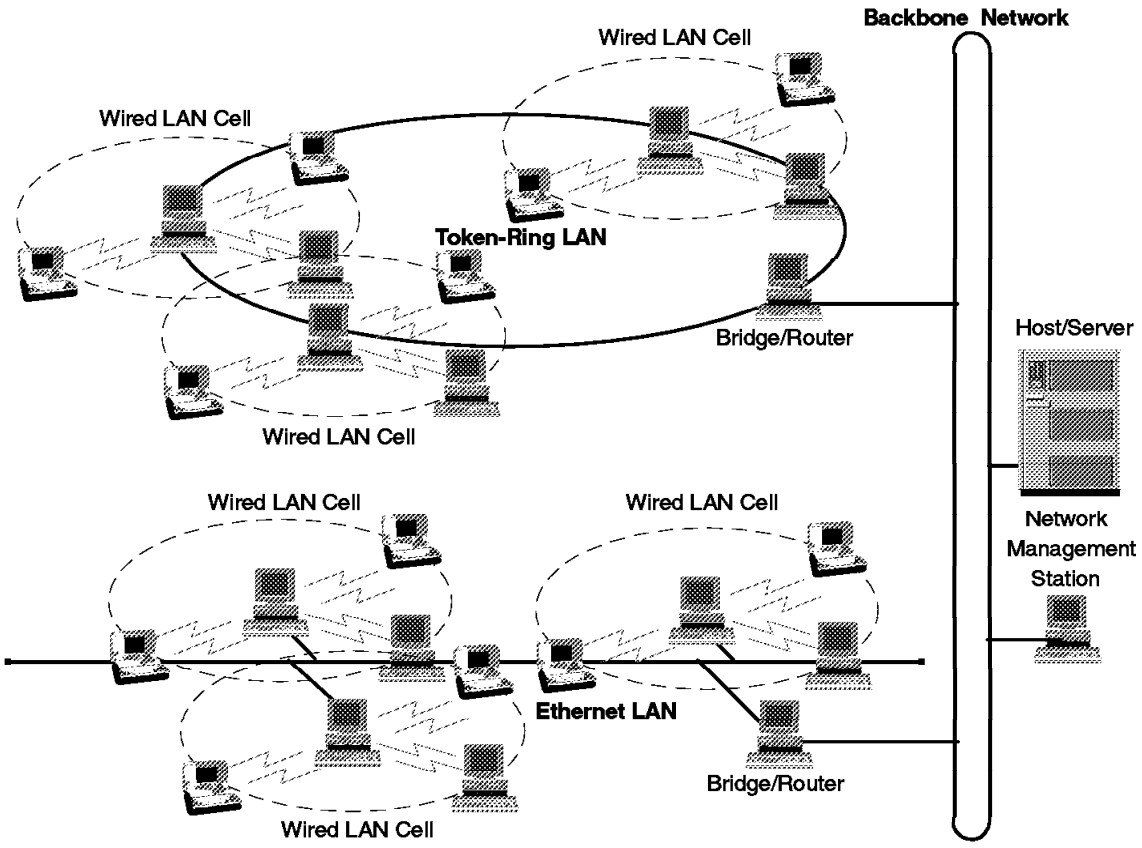


Figure 21. An Example of Wireless Network Using Token-Ring LAN and Ethernet LAN

4.9.1 Stand-Alone Cell

The stand-alone cell is where a base station controls and schedules the traffic of all the wireless workstations which are registered to the wireless LAN network. In this configuration, there is no need for any LAN cabling; it allows for the building of a true Local Area Network with a set of stations which are equipped with the IBM Wireless LAN adapter and radio antenna. The base stations may be located in the center of cell circle, and logically, all traffic in the cell must go through the base station by the inter-cell bridge function.

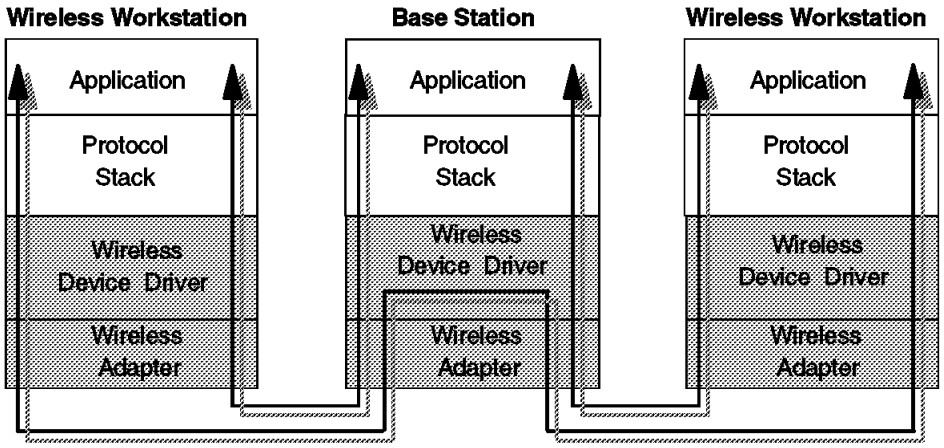


Figure 22. Stand-Alone Cell Configuration

4.9.2 Backbone-Attached Cell

The backbone-attached cell is a cell connected to a wired LAN. In this configuration, each wireless cell appears as a segment attached to the backbone network by the base station. The base station acts as an Access Point between the wireless workstations and the stations connected on the backbone network. The base station allows the offering of different types of interconnectivity according to network media or network operating system.

4.9.2.1 Bridge in Base Station

The base station may act as a MAC source routing bridge if the backbone network media is a token-ring; the function is included with the IBM Wireless LAN product.

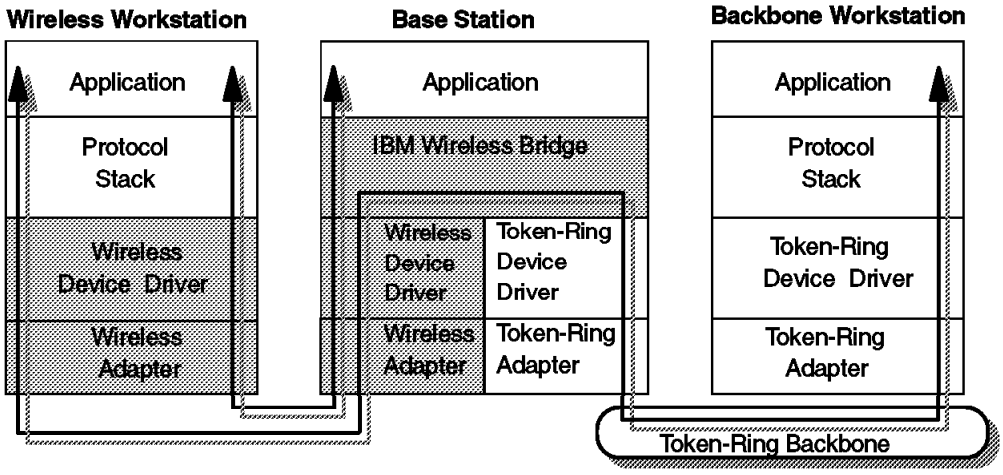


Figure 23. Backbone-Attached Cell with Bridge in the Base Station

4.9.2.2 Router in Base Station

The base stations act as a router if the protocol stack used can be routed (IPX and IP).

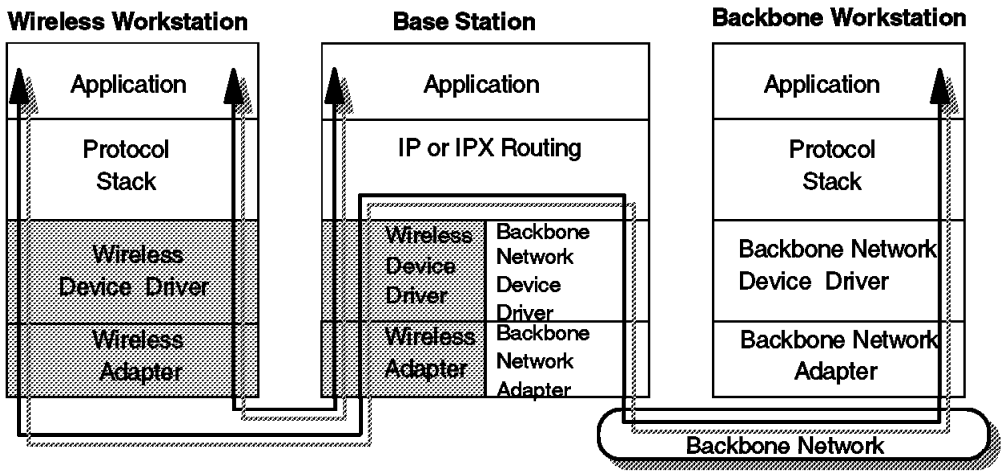


Figure 24. Backbone-Attached Cell with Router in the Base Station

4.9.2.3 SNA Gateway in Base Station

The base stations may act as an SNA gateway to attach the wireless cell on an SNA backbone network. Typically, the SNA application, running in the wireless workstation, may be a 3270 or 5250 emulator accessing an SNA host on the SNA backbone.

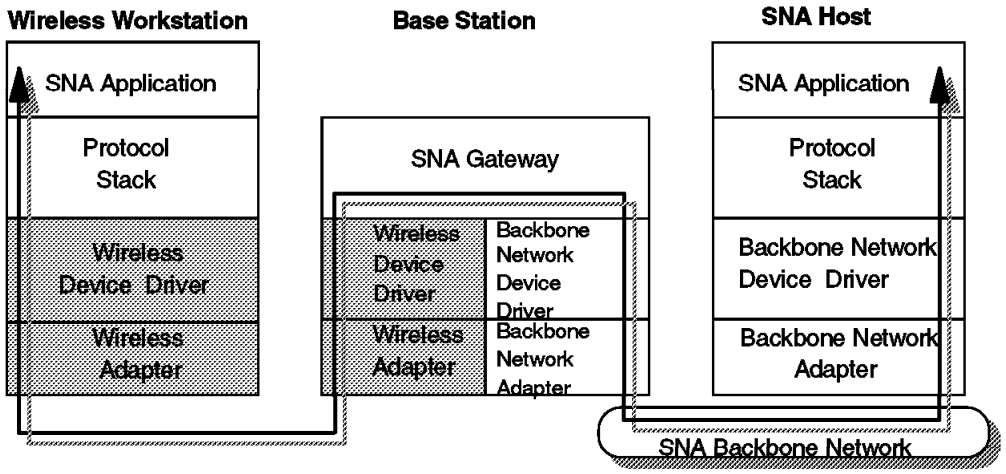


Figure 25. Backbone-Attached Cell with SNA Gateway in the Base Station

The IBM Wireless LAN product complies, for the card interface layer, with the two major standards of industry (ODI and NDIS). It allows the IBM Wireless LAN product to be used in the majority of network operating systems available today.

4.9.3 Novell NetWare Environment

Supported configurations are the stand-alone cell and backbone attached cell. Each cell is controlled by a base station, which is a Novell NetWare server. Wireless workstations are Novell NetWare Requesters (either DOS or OS/2 based).

- Base stations are built on Novell NetWare server, but other Novell NetWare servers on the backbone LAN can of course be accessed by requesters.

  Each base station supports one IBM Wireless LAN ISA/MCA adapter and therefore handles one wireless LAN cell.

- Wireless workstation must have the Novell NetWare Requester software installed, and will be able to access through their attachment Novell NetWare server via SPX/IPX.

  The accessed Novell NetWare server may be base stations or dedicated servers on the backbone network. They can be accessed through IPX routers. (The Base station acts as an IPX router.)

- Novell NetWare Lite is supported in wireless workstations only. Wireless workstations with Novell NetWare Lite installed will be available to either other Novell NetWare Lite wireless workstations in the same cell or the Novell NetWare server of the local base station. Other cells or segments of the network cannot be accessed from Novell NetWare Lite wireless workstations because Novell NetWare Lite does not support IPX routing.

- The Novell LAN Workplace for DOS or OS/2 can be installed in wireless workstations allowing them to communicate using the TCP/IP protocol. The Novell Workplace uses native TCP/IP and therefore is allowed to communicate with TCP/IP devices, possibly through transparent NetWare servers/routers. Note that such a TCP/IP device may be a NetWare server configured as accessible using TCP/IP rather than IPX/SPX. In this configuration, the base station acts as an IP router.

- The base station can be an SNA Gateway, with NetWare for SAA.

  A similarly supported configuration can be obtained by having a base station performing the IPX routing only and a Novell NetWare server on the backbone performing the SNA gateway function with NetWare for SAA.

  NetWare for SAA is required in the wireless workstations to use the SNA application (3270 emulator).

  PC_Support/400 is also required in wireless workstations if wireless workstations try to access the AS/400 host (5250 emulator).

- A cell will appear as a LAN segment of the Novell network. Inter-cell communication will be ensured by the Novell routing functions at the IPX level. It applies to both client/client and client/server traffic via the base station.

- The base station is able to support additional application NLMs.

- A wireless workstation cannot be a Novell NetWare server, but it may occasionally act as a file server for other wireless workstations, in the same cell when it supports the Novell NetWare Lite software.

- A DOS wireless workstation can be a Novell print server by running the print server TSR provided with the NetWare product.

- The overlapping of several independent cells is supported. The overlapping of cells belonging to the same network is also supported.

- One network control station, called the NAP (Network Administrator Program), is mandatory on the network. It runs in the Novell NetWare server environment and may be on any Novell NetWare server, base station or not, attached to the backbone network. There can be only one active network control station for the whole wireless LAN.

  An NAP can control up to 60 base stations. A single IBM Wireless LAN network is, therefore, made of up to 60 cells. It is possible to install several IBM Wireless LAN networks and to be interconnected with each other.

4.9.4 OS/2 Environment

The supported configurations are basically the same as the NetWare environment. There are stand-alone cell and backbone attached cells, but each cell is controlled by an OS/2 Base station. Wireless workstations are either DOS or OS/2 2.0 machines supporting LAN applications such as a LAN requester.

- Base stations *are based* on OS/2 2.1 and higher ISA/MCA systems.
- A cell will appear as a LAN segment to the backbone LAN. Both inter-cell and intra-cell communication is performed at the MAC layer using bridging techniques.

  A base station can only bridge its own cell with one and only one LAN backbone.

  A wireless workstation cannot support a bridge function.
- To connect between Novell NetWare servers attached on a backbone and Novell NetWare requesters in a wireless cell, ROUTE.COM must be loaded in workstations and ROUTE.NLM must be loaded in the Novell NetWare server.
- Base stations *act as* a source routing bridge:
  - All the bridges present between the bridged base and the ring segment that you want to reach will need to have the appropriate hop count.
  - The Wireless LAN Segment number must be unique in the network.
- Base stations can support additional applications such as IBM LAN Server.
- Wireless workstations can be file servers and print servers. However, performance in terms of throughput when accessing a wireless file server cannot be expected to be as good as when accessing a server attached to the backbone network.
- To increase network performance in the wireless network do the following:
  - Use the bridge filtering function provided with IBM Wireless LAN product.
  - If the bridged base station role is only to relay the IPX or IP frame, do not use the bridge function.
  - Use the SNA Gateway function or split a wireless cell if there are over 20 wireless workstations which are using the 3270 emulation in a network cell or disconnecting 3270 sessions frequently.
  - File servers may be installed in a dedicated system on the backbone network, as near as possible.
- The base station can be an IP router, provided with TCP/IP for OS/2, instead of a bridge to communicate with the stations attached to the backbone network.
- The base station can be an SNA gateway, provided with Communication Manager/2, attached to an SNA backbone network. The SNA gateway

function can be in cooperation with the source routing bridge function and the IP routing function in the OS/2 Base station.

- One network control station, called the NAP (Network Administrator Program), is mandatory on the network. It runs in the OS/2 Version 2.1 and higher environment and may be either a dedicated station or any of the base stations of the network, but it cannot be a wireless workstation. There can be only one active network control station for the whole wireless LAN.

  An NAP can control up to 60 base stations A single IBM Wireless LAN network is therefore made of up to 60 cells. It is possible to install several IBM Wireless LAN networks and for them to be interconnected to each other.

  If a base station is configured as a wired stand-alone cell, the NAP in the base station controls the local base station only.

  TCP/IP for OS/2 must be loaded in the base station if the following applies:

  – More than one base station is installed in the network, or the base station is not an NAP station.
  – SNMP-based network management is required in the base station.

4.10 IBM Wireless LAN Installation

This section describes some installation related information. With the help of worksheets provided in *Installing and Operating your Network* provided with IBM Wireless LAN product and *Designing Your Network*, GA33-0189, you can plan your network first.

Note

IBM Wireless LAN product diskettes include several README files describing important information such as attention and limitation for installing, hints and tips of customizing network applications and how to set up network management facilities for each different operating system. Be sure to read and understand those before planning your network.

4.10.1 IBM Wireless LAN Packaging

The IBM Wireless LAN provides two packages to configure a base station or a wireless workstation in a wireless cell. The first package is an ISA/MCA adapter package kit. It includes three hardware components, six software diskettes and one manual to install and configure a base station or a wireless workstation for OS/2 and NetWare. In the Utilities diskette, there are several utilities for the adapter and information on how to configure SNMP Network Management platforms to manage an IBM Wireless LAN. The adapter card can be installed in two ways: on one edge to fit in a PC system with an ISA/AT bus or on the other edge to fit in a Personal System/2 with an MCA bus. The Remote Program Load (RPL) function is provided to download operating system software and applications into a workstation without hard disks and/or diskette drives. This kit consists of the following:

- One ISA/MCA Adapter
- One radio
- One cable 1.5 meters in length
- Six diskettes
  1. Utilities
  2. NetWare Base

3. DOS/Windows Workstation
4. OS/2 Base Workstation Volume 1
5. OS/2 Base Volume 2
6. OS/2 Base Volume 3

- One manual entitled: *Installing and Operating Your Network*, GA33-0188

The second package is a PCMCIA kit. It includes the following three pieces of hardware equipment, and three software diskettes to install and configure a wireless station for DOS, Windows and OS/2. There are different execution codes for each different operating system. However, the PCMCIA card cannot be installed in a base station and cannot support the RPL function. Of course, both cards can be mixed in the same cell.

- One PCMCIA Card
- One radio
- One cable 0.4 meters in length
- Three diskettes

1. Utilities
2. DOS/Windows Workstation
3. OS/2 Base Workstation

4.10.2 Installation Scenario

This section shows how to install and customize an OS/2 bridged base station (wired stand-alone cell). The installation procedure is very easy by using the IBM Wireless LAN installation program. However, it is a little complex to set up a bridged base station because various parameters in the PROTOCOL.INI file related to your network must be customized properly.

Before installing an OS/2 bridged base station program, you should investigate your network and decide on or assign the following parameters:

- **Network Name for This Base Station**

  This is the name that uniquely identifies your network, as specified in the Network Administrator Program (NAP). For more details on NAP, see 4.12, “Network Administrator Program” on page 93. This base station is also an independent NAP station. Even if more than one base station is installed in the network, the NAP cannot recognize base stations other than the local base.

- **Segment Number of Token-Ring on Which IBM Wireless LAN Is Attached**

  The segment number of the IBM Wireless LAN wireless cell must be unique in your network. However, if the number of token-rings has already been assigned by a source such as a source-routing bridge attached on the same ring, you must assign the *same number* on your token-ring side of IBM Wireless LAN bridged base station.

- **Segment Number of IBM Wireless LAN Wireless Cell**

  The segment number of the IBM Wireless LAN wireless cell must be unique in your network.

- **Locally Administered Address for Wireless Adapter in Base Station**

  The IBM Wireless LAN ISA/MCA adapter has an assigned Universally Administered Address (UAA). Of course, it is possible to assign the Local

Administered Address (LAA) on your adapter, but the address can *never* be the same as the token-ring's.

As the result of investigation, the following parameters were assigned to our OS/2 bridged base station:

- Network name is **ITSO01**
- Segment number for the token-ring is **582** (number already assigned by another IBM Token-Ring bridge program)
- Segment number for the wireless cell is **789**
- LAA for the token-ring adapter is **400090002000**
- LAA for the IBM Wireless LAN adapter is **400090002002**

Figure 26 shows the previous configuration.

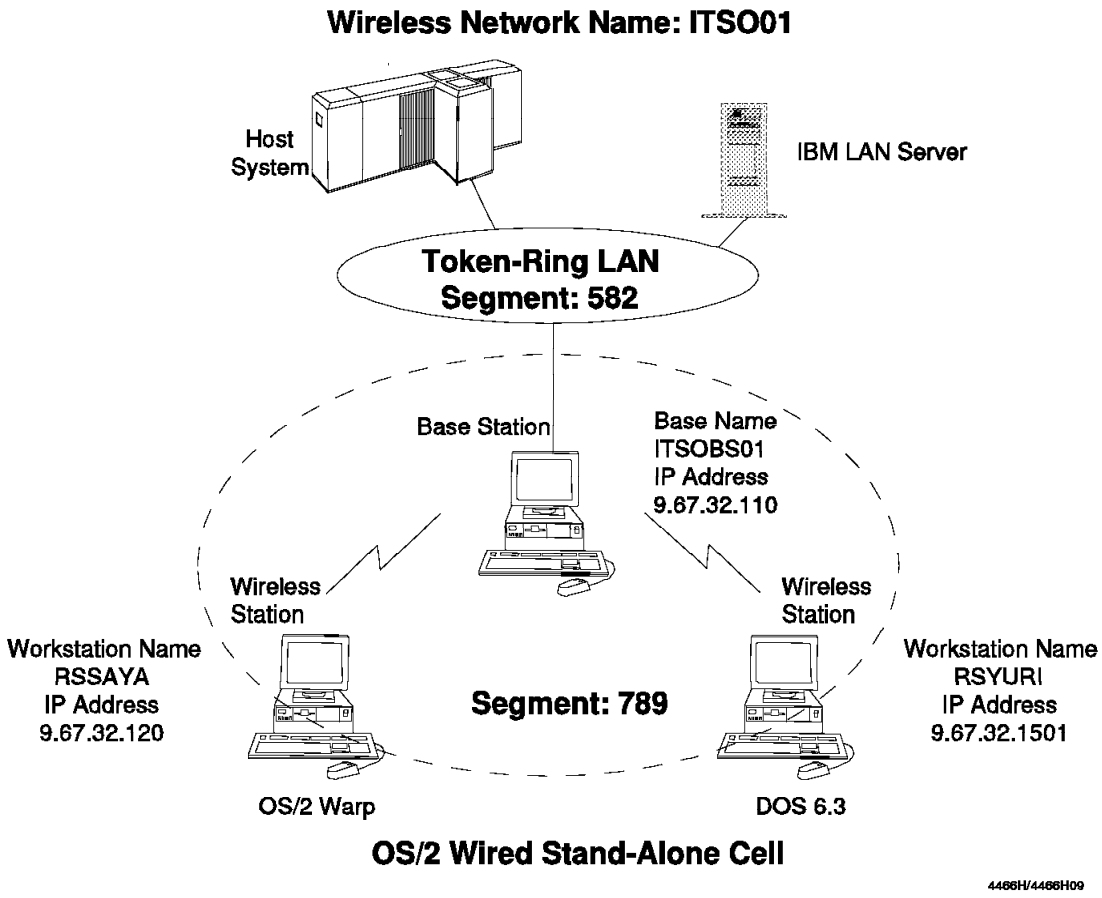


Figure 26. Wired Stand-Alone Cell with Bridge

4.10.3 Installing OS/2 Wired Stand-Alone Cell Base Station

Refer to the *Installing and Operating Your Network* manual provided by the IBM Wireless LAN. During the installation process you need to decide whether or not you are going to use Basic installation or Advanced installation in the OS/2 Base Installation type selection dialog.

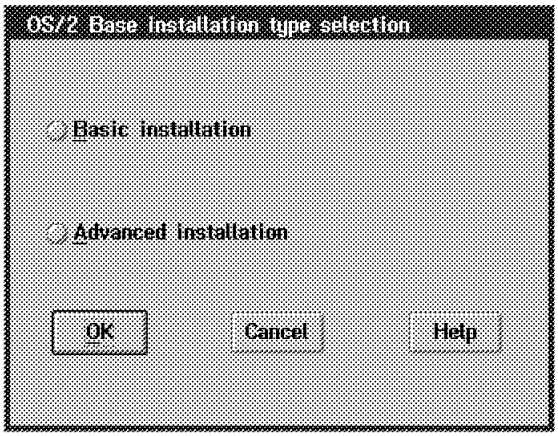


Figure 27. OS/2 Base Installation Type Selection Dialog

- **Basic installation**

  The advantage of this selection is to gather the minimum required device and protocol drivers for the wireless configuration, setting most of the parameter values. Unlike the Advanced installation, if a bridged configuration is chosen, the current LAPS configuration will be overridden. Device and Protocol Drivers are previously installed in the base station and are not kept in the LAPS configuration. You will have to perform additional LAPS actions to retrieve the corresponding support.

  If you have a current LAPS configuration that you want to keep and want to add Wireless support to, we recommend you use the Advanced installation option.

- **Advanced installation**

  The main advantage of this selection is that the current LAPS configuration may be kept and Wireless support will be integrated to it. Unlike the Basic installation, the required wireless protocols (802.2, TCP/IP when needed) should be selected. Also you must set all the device driver parameters (like enable bridges, bridge and segment numbers, and so on for a bridged base or any value required for performance tuning). Refer to *Installing and Operating Your Network*, the README.OS2 file and this book.

Either of the two installation types are capable of configuring the OS/2 bridged base station. If you install the IBM Wireless LAN product in your PC, which does not have any configurations corresponding to the network application, you may select Basic installation.

4.10.3.1 Basic Installation

Select **Basic Installation**, and the OS/2 Base/NAP Station configuration dialog box will be shown. This dialog allows you to set up a base/NAP station.

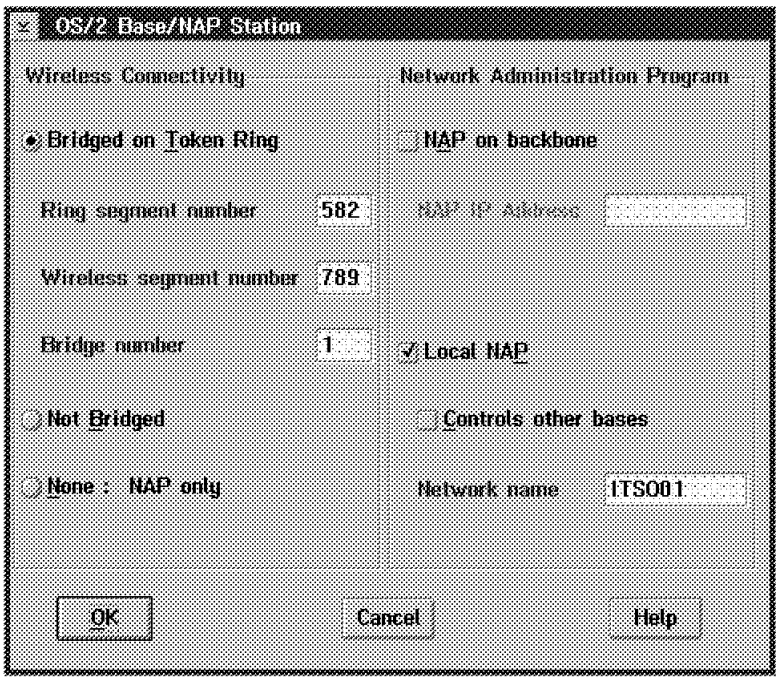


Figure 28. OS/2 Base/NAP Station Configuration Dialog

According to our installation scenario, we selected the **Bridged on Token-Ring** radio button in Wireless Connectivity, and the Ring segment number is set to 582 and the Wireless segment number is set to 789.

Select the **Local NAP** check box and enter the network name ITSO01 in the Network name field in Network Administrator Program.

If the NetBIOS applications, such as IBM LAN Server, have already been installed in the base station, the following message will be shown. If you are going to use the NetBIOS application continuously, select **No** and add the NetBIOS protocol on any driver using LAPS.

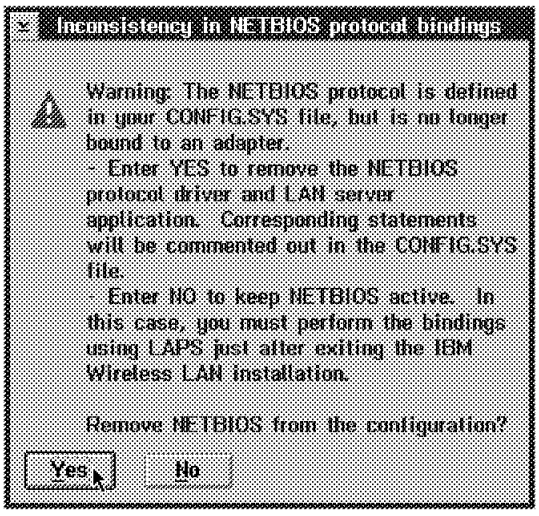


Figure 29. Warning Message in Basic Installation

When the installation process has ended successfully, the PROTOCOL.INI and CONFIG.SYS files in the base station are updated properly. However, Local

Administered Address (LAA) for token-ring and Wireless adapters could not be assigned by using basic installation. To assign LAA, you can edit PROTOCOL.INI using your editor of choice and add the ″NETADDRESS =″ statement with the LAA under both the [IBMTOK_nif] section and the [IBMWLB_nif] section as follows:

```
[IBMTOK_nif]

  DriveName = IBMTOK$
  ADAPTER = ″PRIMARY″
  MAXTRANSMITS = 6
  RECVBUFS = 20
  RECEVBUFSIZE = 256
  XMITBUFS = 1
  XMITBUFSIZE = 4456
  ENABLEBRIDGE
  BRIDGERAM = 5296
  NETADDRESS = ″400090002000″

[IBMWLB_nif]

  DriveName = IBMWL$
  ENABLEBRIDGE = ″YES″
  BUFFERSIZE = 256
  NETADDRESS = ″400090002002
```

Figure 30. Token-Ring and IBM Wireless LAN Adapter Section in PROTOCOL.INI

4.10.3.2 Advanced Installation

In the case when you select **Advanced Installation**, you must set the device driver parameters for a bridged base station by using LAPS. To install additional wireless device drivers, LAPS will be run automatically during the installation process. Select the **Install** button on the LAPS main menu. In the Install Additional Network Driver dialog, select the **OK** button without change. In this process, the following files will be transferred in your PC:

- IBM Wireless LAN Network Adapter for Base with bridge
- IBM Wireless LAN Network Adapter for Base without bridge
- IBM Wireless LAN Bridge

Next, in the Configure Workstation dialog in LAPS, ″IBM Token-Ring Network Adapter″ and ″IBM Wireless LAN Network Adapter″ for a base station bridge may be added in the Current Configuration list and protocols may be added to both network adapters. Edit the adapter and protocol parameters (refer to Table 4).

Table 4 (Page 1 of 2). Network Adapter and Protocol Configuration Parameters

Adapter Driver and Parameters	IBM Token-Ring Network Adapter	
	Network adapter address	400090002000
	Number of receive buffers	20
	Transmit buffer size	4456
	Enable bridge	YES
	Bridge transmit control ram	5296
Protocols and Parameters	IBM Wireless Bridge	
	Ring Number for this LAN..	582
	IBM IEEE 802.2	

Table 4 (Page 2 of 2). Network Adapter and Protocol Configuration Parameters		
Adapter Driver and Parameters	IBM Wireless LAN Network Adapter for base with bridge	
	Bridge activation	YES
	Local Administered Address	400090002002
Protocols and Parameters	IBM Wireless Bridge	
	Ring Number for this LAN..	789
	IBM IEEE 802.2	

To leave LAPS select **OK**, then **Exit**, then **Continue**, then **OK**, then **Exit**.

When you finish with LAPS, the OS/2 Wireless Station Configuration dialog will be shown. Select the **Base (Wired Stand-Alone Cell)** radio button. The Start Bridge Manager and Auto Start NAP check boxes in option may be checked also.

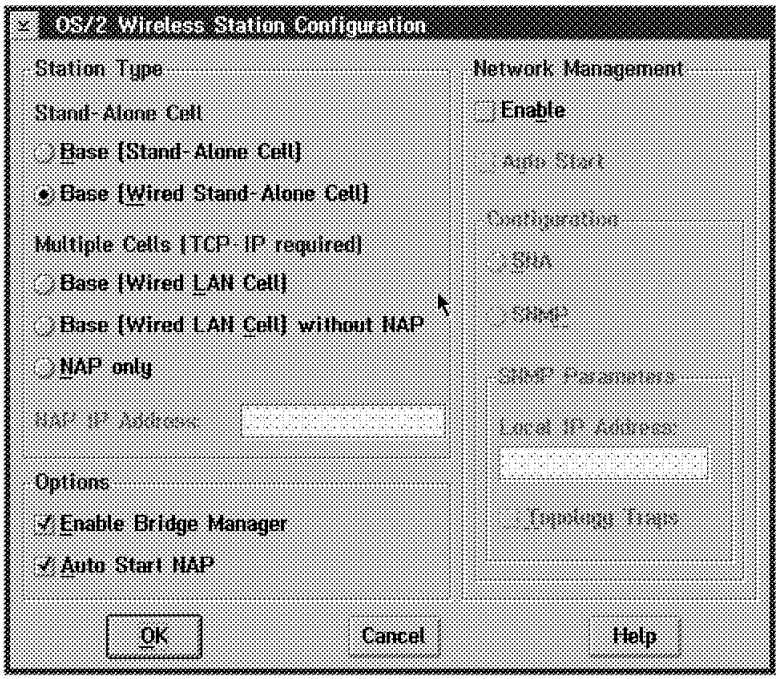


Figure 31. OS/2 Wireless Station Configuration Dialog

4.10.4 Shut Down and Reboot

The rest of the changes that LAPS has made will be in the PROTOCOL.INI in the C:\IBMCOM directory. The CONFIG.SYS file is also changed to enable the IBM Wireless LAN adapter; see C.5, “IBM Wireless LAN System Files” on page 127. After rebooting you will find a folder called IBM Wireless Service on your desktop.

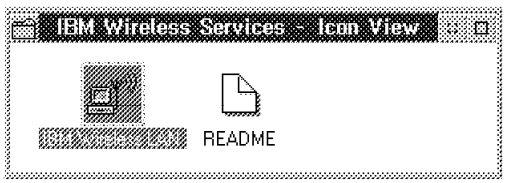


Figure 32. IBM Wireless Service Folder on the OS/2 Desktop

If you selected **Advanced Installation** you must enter your network name (ITSO01) into the Network Name page in the NAP notebook.

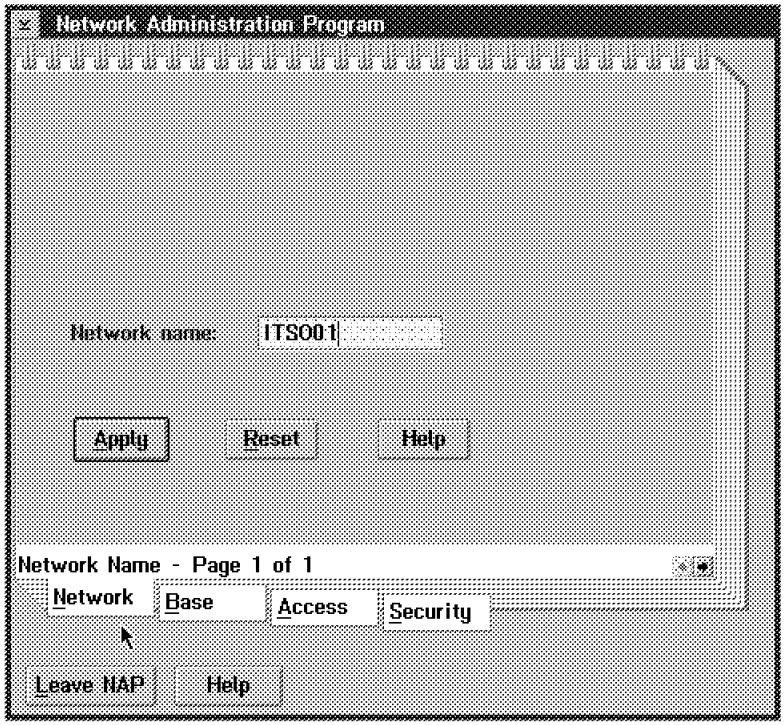


Figure 33. Network Name Page in NAP

4.11 IBM Wireless LAN Configurations

The IBM Wireless LAN product complies at the card interface layer with two major industry standards: ODI and NDIS. Doing so allows the product to be used in a majority of the networking operating systems available:

- Novell NetWare
- IBM LAN Server
- SNA Networks
- Microsoft LAN Manager
- Microsoft Windows NT
- Artisoft LANtastic
- TCP/IP

The following section describes the basic configurations which are known to support the IBM Wireless LAN product. These scenarios are not enough to cover the above network operating systems. There may be helpful information to configure an IBM Wireless LAN network. This scenario (several hardware and software components) is shown in Appendix C, “Wireless Environment Sample Files” on page 119.

Important

If several network applications will be used by wireless workstations, be sure to consider the amount of LAN traffic in a wireless cell. In the case of frequent network errors, it may be necessary to reduce the number of wireless workstations in the wireless cell.

See C.3, “Network Application Coexistence on DOS” on page 122 for more information about protocol stacks on the DOS wireless adapter.

C.5, “IBM Wireless LAN System Files” on page 127 shows you the following system files for base stations and wireless workstations:

- OS/2 Wired Stand-Alone Cell with bridge
  1. CONFIG.SYS for OS/2 Base station
  2. PROTOCOL.INI for OS/2 Base station
  3. CONFIG.SYS for OS/2 wireless workstation
  4. PROTOCOL.INI for OS/2 wireless workstation
  5. PROTOCOL.INI for DOS wireless workstation
- OS/2 Wired LAN Cell with IP routing
  1. PROTOCOL.INI for OS/2 Base station
- NetWare Wired LAN Cell with IPX routing
  1. IBMWL.NCF for NetWare Base station
  2. CONFIG.SYS for OS/2 wireless workstation
  3. NET.CFG for OS/2 wireless workstation
  4. NET.CFG for DOS wireless workstation

4.11.1 OS/2 Stand-Alone Cell

In this scenario, (from DOS and OS/2 FTP, client access to an FTP server in the base station) our base station is not on a wired LAN. Of course, wireless workstations can communicate with each other via the base station.

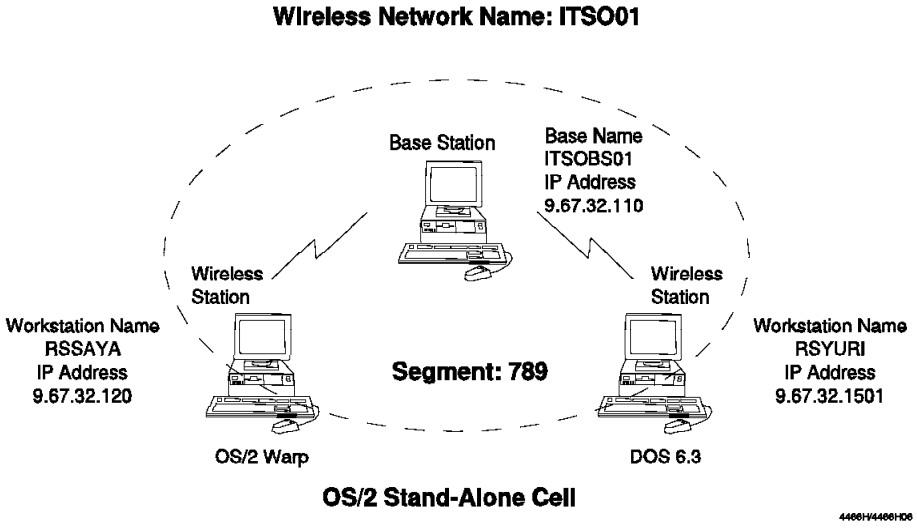


Figure 34. Configuration Stand-Alone Cell

In this configuration, the base station is also an NAP station. Refer to 4.12, “Network Administrator Program” on page 93 for more information about NAP.

4.11.2 Stand-Alone Cell with TCP/IP

Table 5. Stand-Alone Cell with TCP/IP

Ntwk/Ws Name	Operating System	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
ITSO01 ITSOBS01	OS/2	FTP server	• IBM TCP/IP • IBM IEEE 802.2	N/A
ITSO01 RSSAYA	OS/2	FTP server/client	• IBM TCP/IP • IBM IEEE 802.2	N/A
ITSO01 RSYURI	DOS	FTP client	• IBM TCP/IP	N/A
Adapter Drivers:				
Base station	IBM Wireless Network Adapter for base without bridge			
Wireless workstation	IBM Wireless Network Adapter for workstation			

4.11.3 Stand-Alone Cell with NetBIOS

You need to add a NetBIOS protocol stack on the wireless adapter, if the IBM LAN Server coexists in the base station.

Table 6. Stand-Alone Cell with NetBIOS

Ntwk/Ws Name	Operating System	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
ITSO01 ITSOBS01	OS/2	IBM LAN Server	• IBM NetBIOS • IBM IEEE 802.2	N/A
ITSO01 RSSAYA	OS/2	LAN Requester	• IBM NetBIOS • IBM IEEE 802.2	N/A
ITSO01 RSYURI	DOS	LAN Requester	• IBM LSP • IBM NetBIOS • IBM IEEE 802.2	N/A

4.11.4 Stand-Alone Cell with SNA Gateway

If using Communication Manager/2, a base station can offer the SNA gateway function without modification of the wireless network configuration. The host connectivity options for the SNA gateway can be selected from various adapters supported by the CM/2 gateway function. The upstream side of a CM/2-based SNA gateway can use a link as low as a V.24 interface (9.6 Kbps) or a V.35 interface (56 Kbps) with an SDLC leased line.

Table 7. Stand-Alone Cell with SNA Gateway: V.24 Interface

Ntwk/Ws Name	Operating System	Application	Protocols on WL adapter (at least)	Interface
ITSO01 ITSOBS01	OS/2	CM/2 SNA Gateway	• IBM IEEE 802.2	• V.24 interface

In another typical case, if a wired LAN type is Ethernet the configuration of the base station is as follows:

Table 8. Stand-Alone Cell with SNA Gateway: Ethernet Adapter

Ntwk/Ws Name	Operating System	Application	Protocols on WL adapter (at least)	Protocols on Enet adapter (at least)
ITSO01 ITSOBS01	OS/2	CM/2 SNA Gateway	• IBM IEEE 802.2	• IBM IEEE 802.2

4.11.5 OS/2 Wired Stand-Alone Cell with Bridge

In this scenario, the DOS and OS/2 wireless workstations acquire access to a station or a host on a wired LAN with the following network applications via the OS/2 bridged base station:

- Access SNA host from PC3270 for Windows and CM/2
- Access IBM LAN Server on wired LAN from OS/2 LAN Requester and DOS LAN Requester
- Access FTP server on wired LAN from OS/2 and DOS FTP client

The filter facility provided with the IBM Wireless LAN product, allows various broadcast frames from token-ring to be filtered at protocol level. See the README.OS2 file for more information on setting this filter.

Note: If the IP traffic is going to bridge from the wireless cell to a token-ring, then the Max Transmit Unit in TCP/IP should be lower than (RCVBUFS X RCVBUFSIZE) and BRIDGERAM ([IBMTOK_nif] parameters in the base station PROTOCOL.INI file).

4.11.6 Configuration Wired Stand-Alone Cell with a Bridge

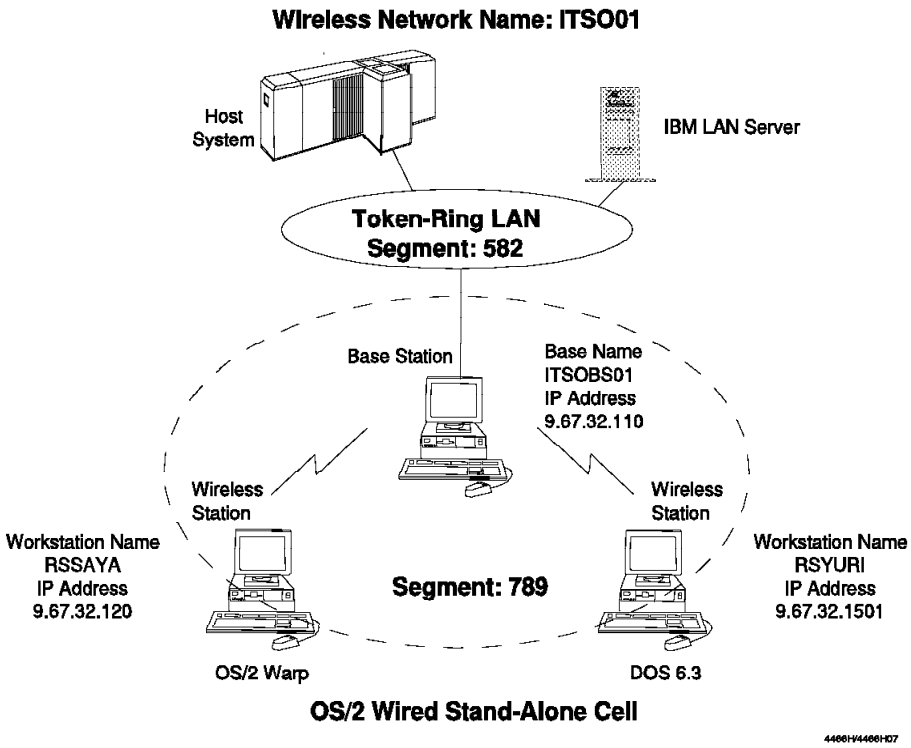


Figure 35. Configuration Wired Stand-Alone Cell with Bridge

In this configuration, the base station is also an NAP station. Refer to 4.12, "Network Administrator Program" on page 93 for more information about NAP.

Table 9 (Page 1 of 2). Wired Stand-Alone Cell with Bridge

Ntwk/Ws Name	Operating System	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
N/A ITSOWLS	OS/2	• LAN Server • FTP Server	N/A	• IBM TCP/IP • IBM NetBIOS • IBM IEEE 802.2
ITSO01 ITSOBS01	OS/2	N/A	• IBM Wireless Bridge • IBM IEEE 802.2	• IBM Wireless Bridge • IBM IEEE 802.2
ITSO01 RSSAYA	OS/2	• LAN Requester • FTP client • Communication Manager/2	• IBM TCP/IP • IBM NetBIOS • IBM IEEE 802.2	N/A

Table 9 (Page 2 of 2). Wired Stand-Alone Cell with Bridge

Ntwk/Ws Name	Operating System	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
ITSO01 RSYURI	DOS	• FTP client • PC3270 for windows • LAN Requester	• IBM TCP/IP • DOS LSP • IBM IEEE 802.2 • IBM NetBIOS	N/A
Adapter Drivers:				
Base station	IBM Wireless Network Adapter for base with bridge			
Wireless workstation	IBM Wireless Network Adapter for workstation			

4.11.7 Novell NetWare over Bridge

Novell NetWare Requester in the wireless workstations can communicate with a Novell NetWare server on a token-ring wired LAN via an OS/2 bridged base station. In this configuration, no modification or addition is necessary in the base station.

Table 10. Novell NetWare over Bridge

Ntwk/Ws Name	Operating System	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
N/A BANK311	NetWare	• NetWare Server	N/A	• NetWare IPX
ITSO01 RSSAYA	OS/2	• NetWare Requester	• NetWare IPX	N/A
ITSO01 RSYURI	DOS	• NetWare Requester	• NetWare IPX	N/A
Adapter Drivers:				
Novell NetWare server	IBM Token-Ring Adapter and ROUTE.NLM			
Wireless workstation	IBM Wireless Network Adapter for workstation and ROUTE.COM			

4.11.8 Multiple OS/2 Wired Stand-Alone Cells with a Bridge

Two wired stand-alone cells exist on a wired LAN. Both base stations are also NAP stations and may be assigned different network names. Wireless workstations cannot obtain access to base stations having different network names. In order to be registered in the base stations, the network name of the wireless workstations must be configured properly. In this scenario, we changed the network name of a wireless workstation named RSYURI to ITSO02 in the PROTOCOL.INI. The wireless workstation can now be registered in the base station named ITSOBS02, instead of the Base station named ITSOBS01. There is no impact on network applications due to a change in the network name of a wireless workstation.

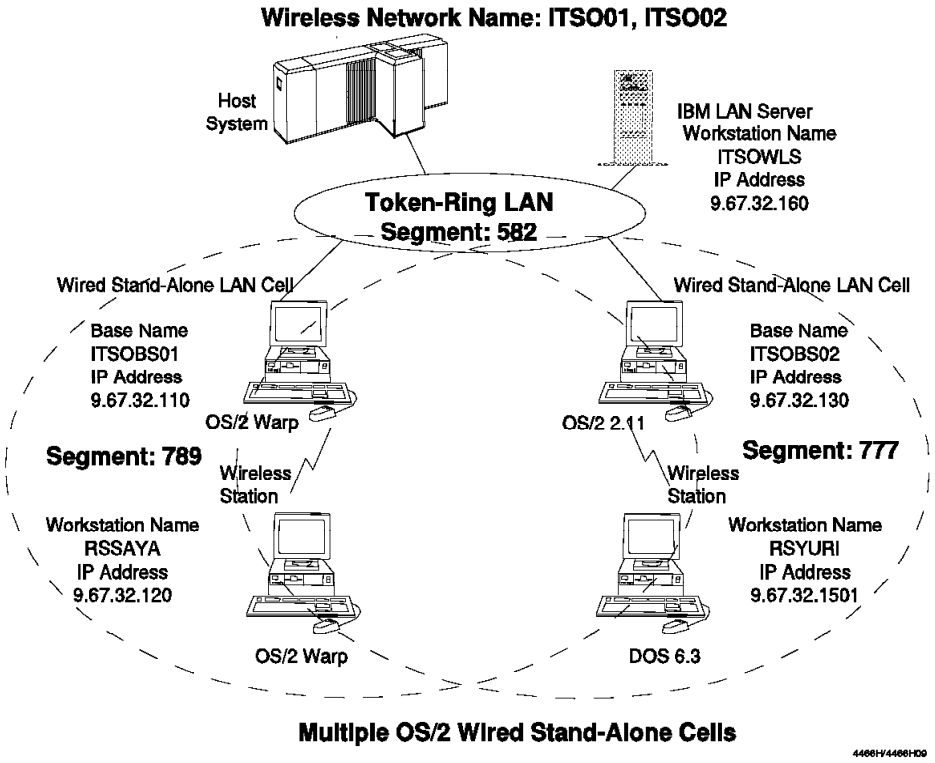


Figure 36. Configuration of Multiple Stand-Alone Cells with a Bridge

4.11.9 Multiple Wired Stand-Alone Cells with a Bridge

In this configuration, both base stations are also NAP stations. Refer to 4.12, "Network Administrator Program" on page 93 for more information about NAP.

Table 11. Multiple Wired Stand-Alone Cells with a Bridge

Ntwk/Ws Name	OS	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
N/A ITSOWLS	OS/2	• LAN Server • FTP Server	N/A	• IBM TCP/IP • IBM NetBIOS • IBM IEEE 802.2
ITSO01 ITSOBS01	OS/2	N/A	• IBM Wireless Bridge • IBM IEEE 802.2	• IBM Wireless Bridge • IBM IEEE 802.2
ITSO02 ITSOBS02	OS/2	N/A	• IBM Wireless Bridge • IBM IEEE 802.2	• IBM Wireless Bridge • IBM IEEE 802.2
ITSO01 RSSAYA	OS/2	• LAN Requester • FTP client • Communication Manager/2	• IBM TCP/IP • IBM NetBIOS • IBM IEEE 802.2	N/A
ITSO02 RSYURI	DOS	• FTP client • PC3270 for windows • LAN Requester	• IBM TCP/IP • IBM LSP • IBM IEEE 802.2 • IBM NetBIOS	N/A
Adapter Drivers:				
Base station	IBM Wireless Network Adapter for base with bridge			
Wireless workstation	IBM Wireless Network Adapter for workstation			

4.11.10 OS/2 Wired LAN Cell With/Without NAP with Bridge/IP Router

When properly configured a Base station of a Wired LAN Cell with the NAP can manage, not only the local Base station, but also other Base stations without a NAP (Wired LAN Cell Without NAP). By using the NAP, it is possible to centralize various management functions including the registration of wireless workstations.

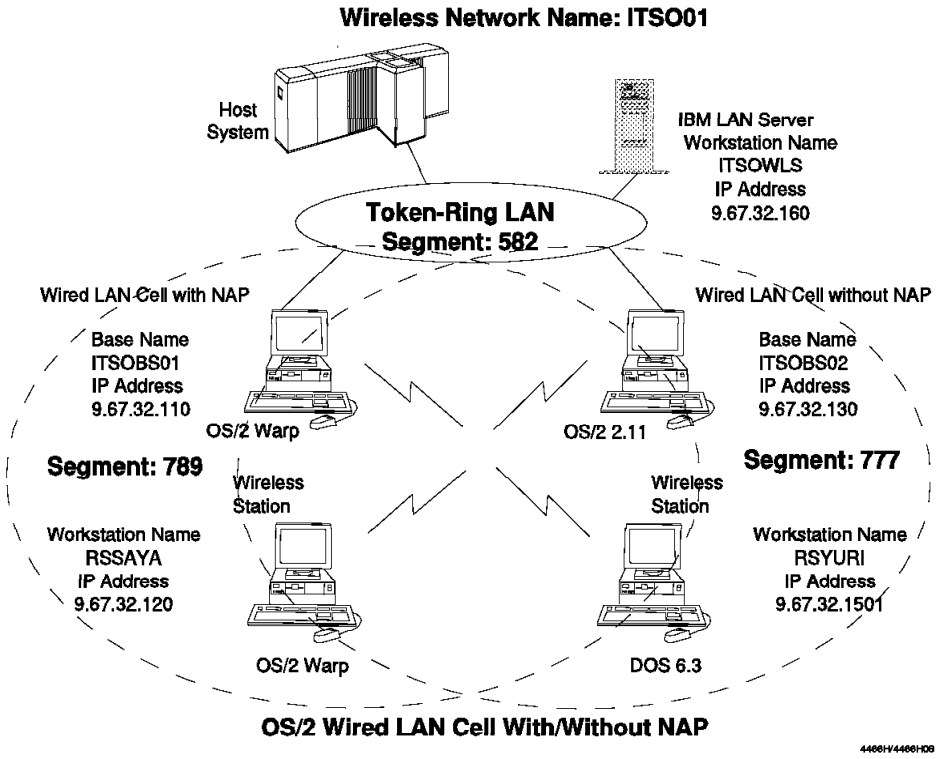


Figure 37. Wired LAN Cell With/Without NAP

In this configuration, one base station is also an NAP station, and another base station is without NAP. Refer to 4.12, “Network Administrator Program” on page 93 for more information about NAP.

4.11.11 Wired LAN Cell without NAP and Wired LAN Cell with Bridge

Table 12 (Page 1 of 2). Wired LAN Cell without NAP and Wired LAN Cell with Bridge

Ntwk/Ws Name	OS	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
N/A ITSOWLS	OS/2	• LAN Server • FTP Server	N/A	• IBM TCP/IP • IBM NetBIOS • IBM IEEE 802.2
ITSO01 ITSOBS01	OS/2	N/A	• IBM Wireless Bridge • IBM IEEE 802.2	• IBM TCP/IP • IBM Wireless Bridge • IBM IEEE 802.2
ITSO01 ITSOBS02	OS/2	N/A	• IBM Wireless Bridge • IBM IEEE 802.2	• IBM TCP/IP • IBM Wireless Bridge • IBM IEEE 802.2

Table 12 (Page 2 of 2). Wired LAN Cell without NAP and Wired LAN Cell with Bridge

Ntwk/Ws Name	OS	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
ITSO01 RSSAYA	OS/2	• LAN Requester • FTP client • Communication Manager/2	• IBM TCP/IP • IBM NetBIOS • IBM IEEE 802.2	N/A
ITSO01 RSYURI	DOS	• FTP client • PC3270 for windows • LAN Requester	• IBM TCP/IP • IBM LSP • IBM IEEE 802.2 • IBM NetBIOS	N/A
Adapter Drivers:				
Base station	IBM Wireless Network Adapter for base with bridge			
Wireless workstation	IBM Wireless Network Adapter for workstation			

With TCP/IP for OS/2, base stations can offer an IP routing function instead of a bridging function. Using IP routing, the MAC broadcast frames from the wired LAN will be decreased, so our air interface performance will be increased. For example, with CM/2 gateway function and IP routing function in the base station installed together, not only will the wireless workstations in the cell be able to use SNA applications, but also the TCP ones as well. In the following configuration, wireless workstations can use IBM LAN Server with TCP/IP for NetBIOS. This configuration is selectable over the various backbone networks, such as Ethernet, FDDI, X.25, in addition to token-ring.

Table 13. Wired LAN Cell without NAP and Wired LAN Cell with IP Routing

Ntwk/Ws Name	OS	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
N/A ITSOWLS	OS/2	• LAN Server • FTP Server • TCP/IP for NetBIOS	N/A	• IBM TCP/IP • IBM IEEE 802.2
ITSO01 ITSOBS01	OS/2	• IP Routing • SNA Gateway	• IBM TCP/IP • IBM IEEE 802.2	• IBM TCP/IP • IBM IEEE 802.2
ITSO01 ITSOBS02	OS/2	• IP Routing • CM/2 SNA gateway	• IBM TCP/IP • IBM IEEE 802.2	• IBM TCP/IP • IBM IEEE 802.2
ITSO01 RSSAYA	OS/2	• LAN Requester • FTP client • Communication Manager/2 • TCP/IP for NetBIOS	• IBM TCP/IP • IBM IEEE 802.2	N/A
ITSO01 RSYURI	DOS	• FTP client • PC3270 for Windows • LAN Requester • TCP/IP for NetBIOS	• IBM TCP/IP • IBM LSP • IBM IEEE 802.2	N/A
Adapter Drivers:				
Base station	IBM Wireless Network Adapter for base without bridge			
Wireless workstation	IBM Wireless Network Adapter for workstation			

4.11.12 NetWare Stand-Alone Cell

In this scenario, DOS and OS/2 Novell NetWare Requesters have access to the Novell NetWare server in the base station. This base station is not connected to the wired LAN.

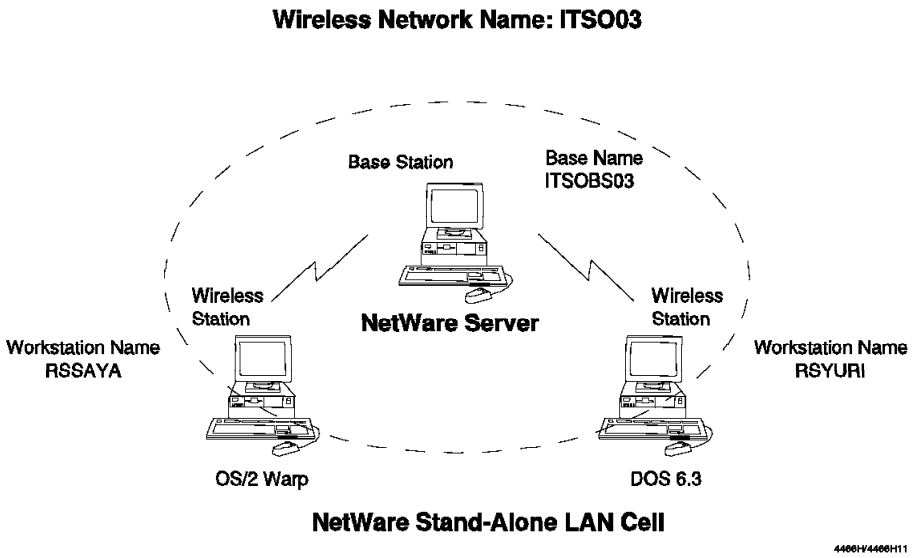


Figure 38. Configuration of a Stand-Alone Cell with Novell NetWare

In this configuration, the base station is also an NAP station. Refer to 4.12, “Network Administrator Program” on page 93 for more information about NAP.

Table 14. Stand-Alone Cell with Novell NetWare

Ntwk/Ws Name	Operating System	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
ITSO03 ITSOBS03	NetWare	Novell NetWare server	Novell IPX	N/A
ITSO03 RSSAYA	OS/2	Novell NetWare Requester	Novell IPX	N/A
ITSO03 RSYURI	DOS	Novell NetWare Requester	Novell IPX	N/A
Adapter Drivers:				
Base station	IBM Wireless Network Adapter for base station			
Wireless workstation	IBM Wireless Network Adapter for workstation			

4.11.13 NetWare Wired LAN Cell with IPX/IP Routing and SNA Gateway

In this configuration the base station is connected with a Wired LAN Cell; wireless workstations in the cell will be able to access other Novell NetWare servers on a wired LAN. The IPX routing facility in the base station is provided by the installed Novell NetWare server. The base station is also an NAP station and it can manage not only the local base station, but also other base stations without a NAP (Wired LAN Cell Without NAP). Backbone networks, based on WAN or LAN, including token-ring/Ethernet are also supported.

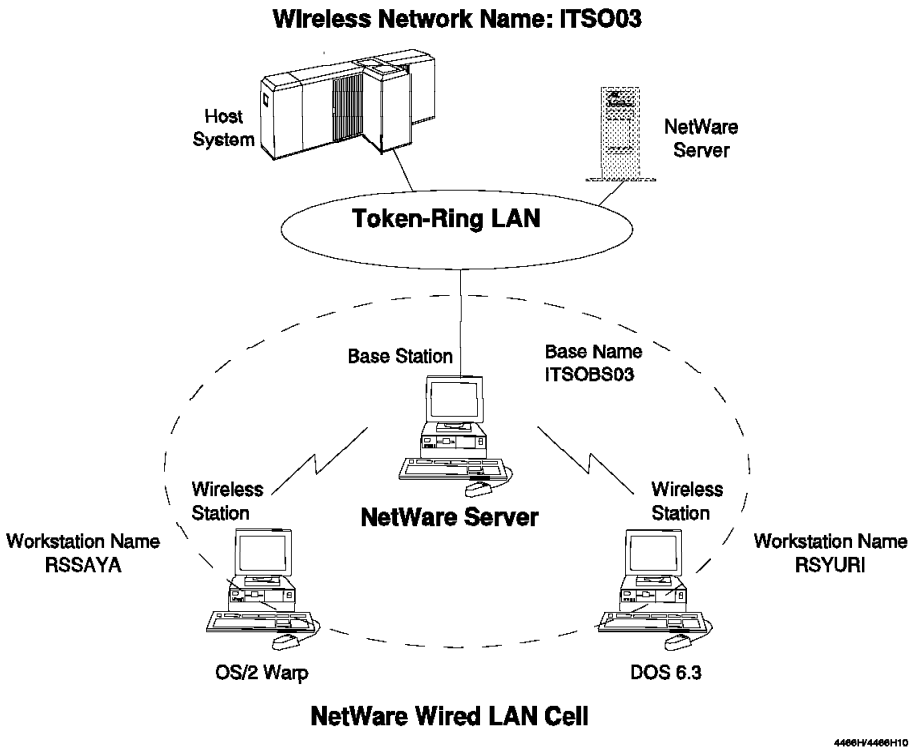


Figure 39. Wired LAN Cell with Novell NetWare

4.11.14 Wired LAN Cell with IPX Routing

In this configuration, the base station is also an NAP station. Refer to 4.12, “Network Administrator Program” on page 93 for more information about NAP.

The configurations of wireless workstations are the same as in the Novell NetWare Stand-Alone Cell.

Table 15. Wired LAN Cell with IPX Routing

Ntwk/Ws Name	Operating System	Application	Protocols on WL adapter (at least)	Protocols on TR adapter (at least)
ITSO03 ITSOBS03	NetWare	Novell NetWare server	Novell IPX	Novell IPX
Adapter Drivers:				
Base station	IBM Wireless Network Adapter for base station			
Wireless workstation	IBM Wireless Network Adapter for workstation			

4.11.15 Wired LAN Cell with IP Routing

The Novell NetWare server can offer an IP routing function instead of IPX routing. NetWare Requester with LAN Workplace for DOS may be installed in wireless workstations to enable IP transport for networking. Using the IP network, wireless workstations can access various TCP/IP-based resources other than Novell NetWare servers.

Table 16. Wired LAN Cell with IP Routing				
Ntwk/Ws Name	**Operating System**	**Application**	**Protocols on WL adapter (at least)**	**Protocols on TR adapter (at least)**
ITSO03 ITSOBS03	NetWare	Novell NetWare server	Novell TCP/IP	Novell TCP/IP
ITSO03 RSSAYA	OS/2	• Novell NetWare Requester • LAN Workplace	Novell TCP/IP	N/A
ITSO03 RSYURI	DOS	• Novell NetWare Requester • LAN Workplace	Novell TCP/IP	

4.11.16 Wired LAN Cell with SNA Gateway

In order to use SNA applications in the Novell NetWare wireless cell, NetWare for SAA may be installed in wireless workstations. If desirable, PC_Support/400 may additionally be installed to supply the 5250 emulator for wireless workstations. If we install NetWare for SAA in a base station, it becomes an SNA gateway for wireless workstations. A similar supported configuration can be obtained by having a base station performing IPX routing only and another Novell NetWare server, on the backbone, performing the SNA gateway function with NetWare for SAA.

Table 17. Wired LAN Cell with SNA Gateway				
Ntwk/Ws Name	**Operating System**	**Application**	**Protocols on WL adapter (at least)**	**Protocols on TR adapter (at least)**
ITSO03 ITSOBS03	NetWare	• Novell NetWare server • NetWare for SAA	Novell IPX	
ITSO03 RSSAYA	OS/2	• Novell NetWare Requester • NetWare for SAA	Novell IPX	N/A
ITSO03 RSYURI	DOS	• Novell NetWare Requester • NetWare for SAA	Novell IPX	

4.12 Network Administrator Program

The Network Administrator Program (NAP) allows you to perform network administration tasks for the wireless network. The NAP may also be installed on a station, connected to the wired LAN, that is not a base station.

The NAP is organized into a notebook. Each type of administrative task appears on a separate page of the notebook.

4.12.1 Scenario

In this section we describe how to use NAP with the following scenario:

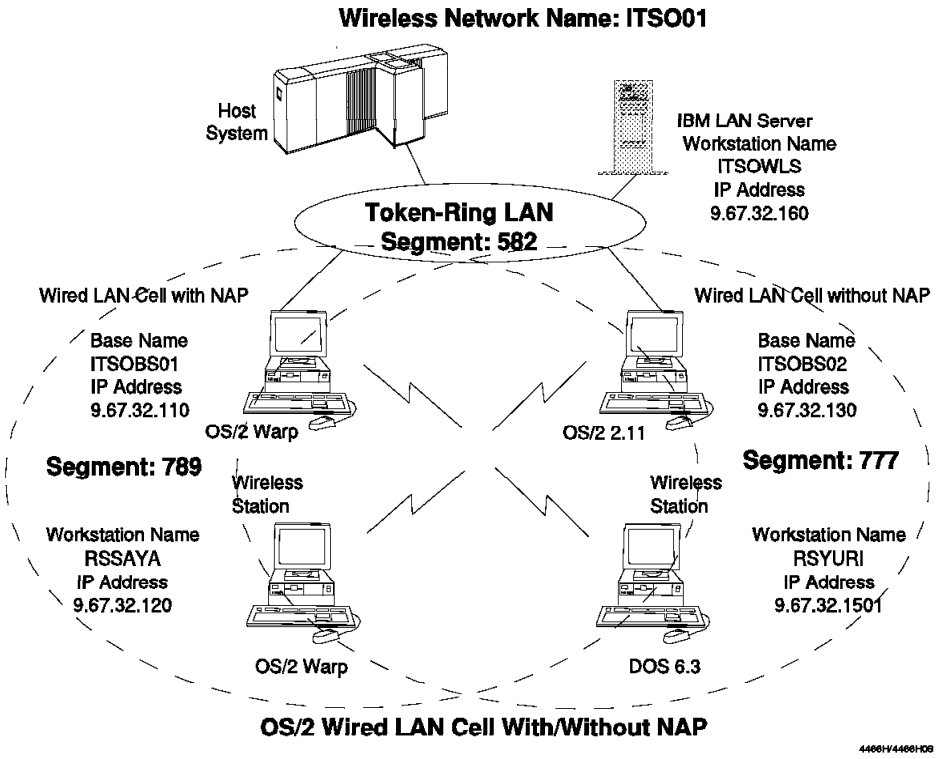


Figure 40. Network Configuration

- There is a wireless network named ITSO01.
- There are two base stations in the network named ITSOBS01 and ITSOBS02. Each has a wired connection to a shared token-ring network. The ITSOBS01 has been configured as a wired LAN cell (with NAP). The ITSOBS02 has been configured as a wired LAN cell (without NAP). See Figure 41 on page 95 and Figure 42 on page 95.
- There are two wireless workstations in the network named RSSAYA and RSYURI. Both wireless workstations are located in close proximity. This means it is possible to receive a signal from both base stations and connect with both base stations.
- RSSAYA will belong in ITSOBS01. RSYURI will belong in ITSOBS02.
- Both wireless workstations will be authorized from Monday to Friday and available from 8:00 to 20:00.
- The security function will be used in the authentication process.

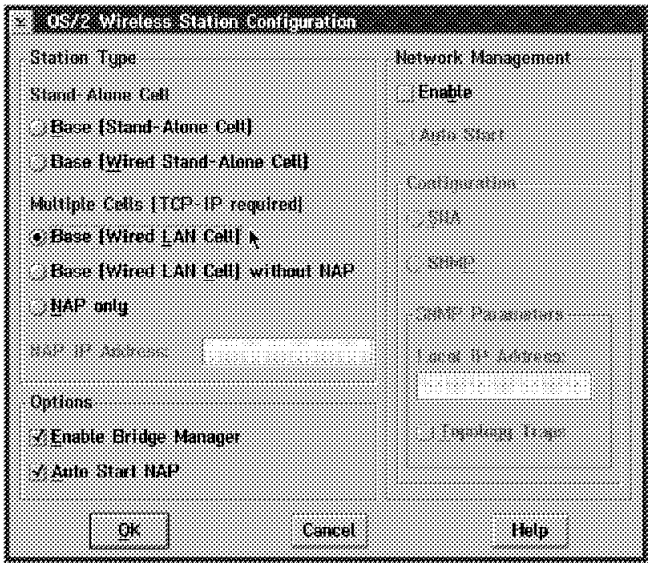


Figure 41. OS/2 Wireless Station Configuration of ITSOBS01

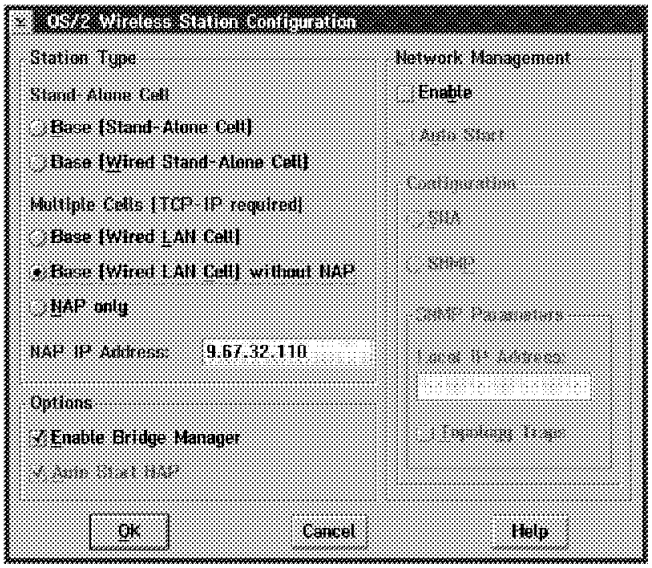


Figure 42. OS/2 Wireless Station Configuration of ITSOBS02

4.12.2 Network Name Page

The Network Name page of the NAP notebook allows you to display and modify the name of the network in which the network is located.

Important

A network name must be supplied to allow wireless LAN operation and uniquely identify your wireless LAN network. The name must contain between five and eight alphanumeric characters. At least two of the characters must be numbers. You cannot use the same character in three consecutive positions.

Our network name is ITSO01 which we have supplied in the field for our premised situation. See Figure 43 on page 96.

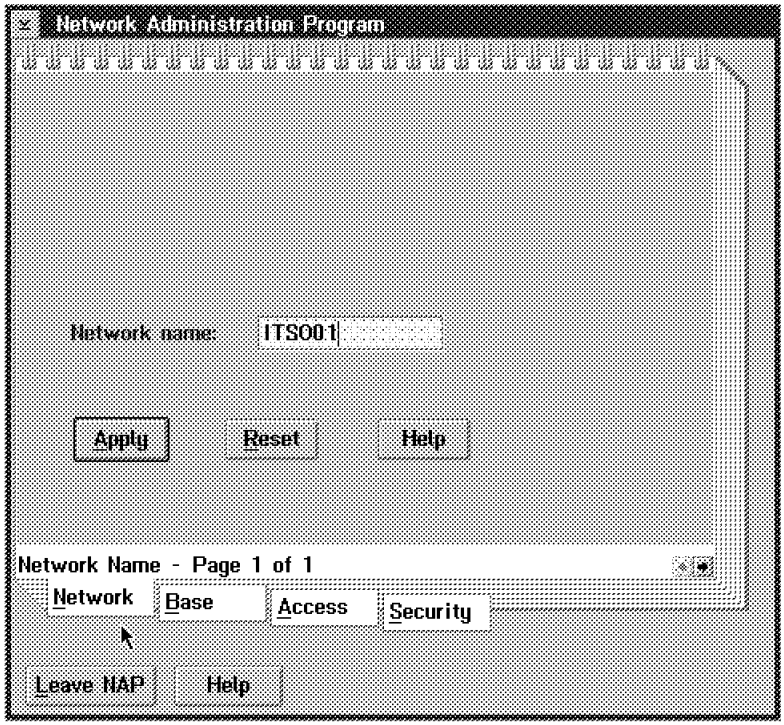


Figure 43. Network Name Page in OS/2 NAP

When you have made the changes on the Network Name page of the NAP notebook, select the **Apply** push button to put your change into effect.

4.12.3 Base Information Page

The Base Information page of the NAP notebook allows you to display and modify the list of base stations in the network. It is possible to add and delete base stations from the network and to modify the name and IP address of any base station in the network. See Figure 44 on page 97.

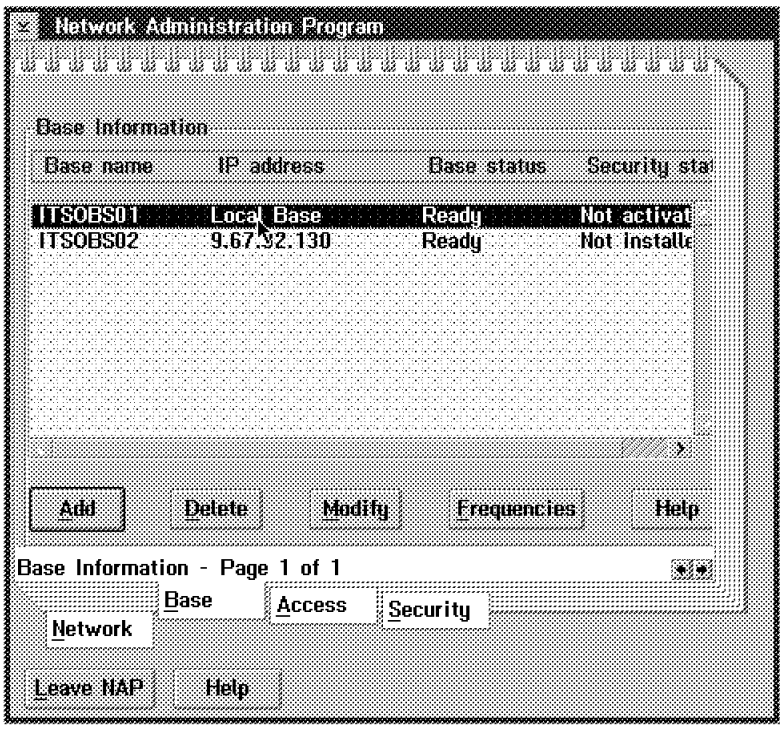


Figure 44. Base Information Page in OS/2 NAP

Important

The Base name must be from 1 to 8 alphanumeric characters without any spaces. The Base name must be unique in the network.

The first base station in the base information list is the local base station with this NAP. The Base name is changed to ITSOBS01 from the default name.

The second base station named ITSOBS02 must be registered in this NAP because its configuration is without NAP and the base station must belong to a NAP in the network.

Controls	Description
Base Information list	This shows the Base name, IP address, Base status and the security status of every base in the network. When the Base status field is Ready, the Base station is operational. When the Base security status field is Activated the security function is installed and active on the base station.
Add push button	This is to add a new base station in this network. It is a necessary IP address of the base station, and it is a unique Base name in this network.
Delete push button	This is to delete a base station selected in the Base list from network. You can not delete the local base station (default name LCACALBS).
Modify push button	This is to modify an IP address or Base name of a base station selected in the Base list. The local base station is not changeable.

Frequency push button This is to change the frequency of a base station selected in the Base list.

4.12.4 Workstation Access Control Page

The Workstation Access Control page of the NAP notebook allows you to restrict a workstation's access to the network by specifying that it may communicate only on specific days, at specific times and with specific base stations. See Figure 45.

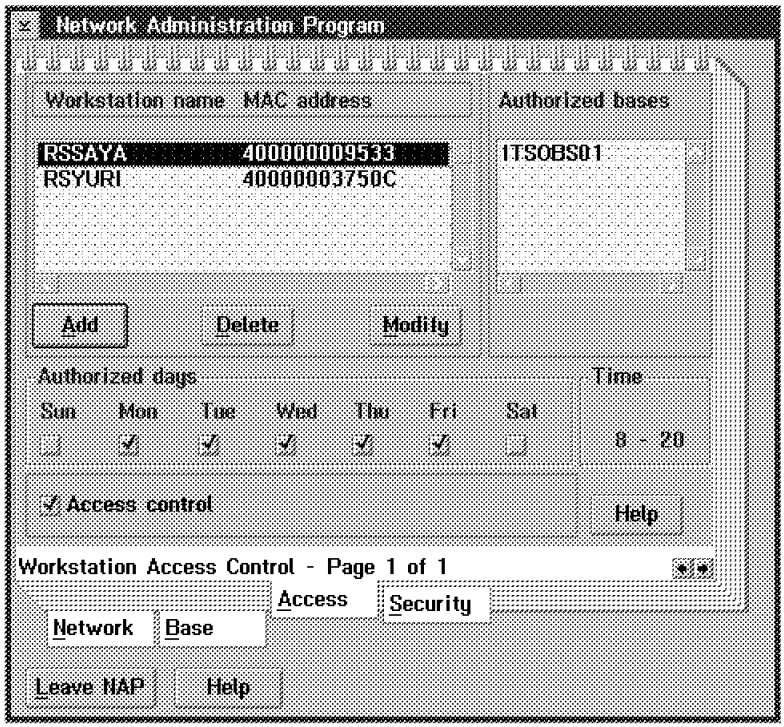


Figure 45. Workstation Access Control Page in OS/2 NAP

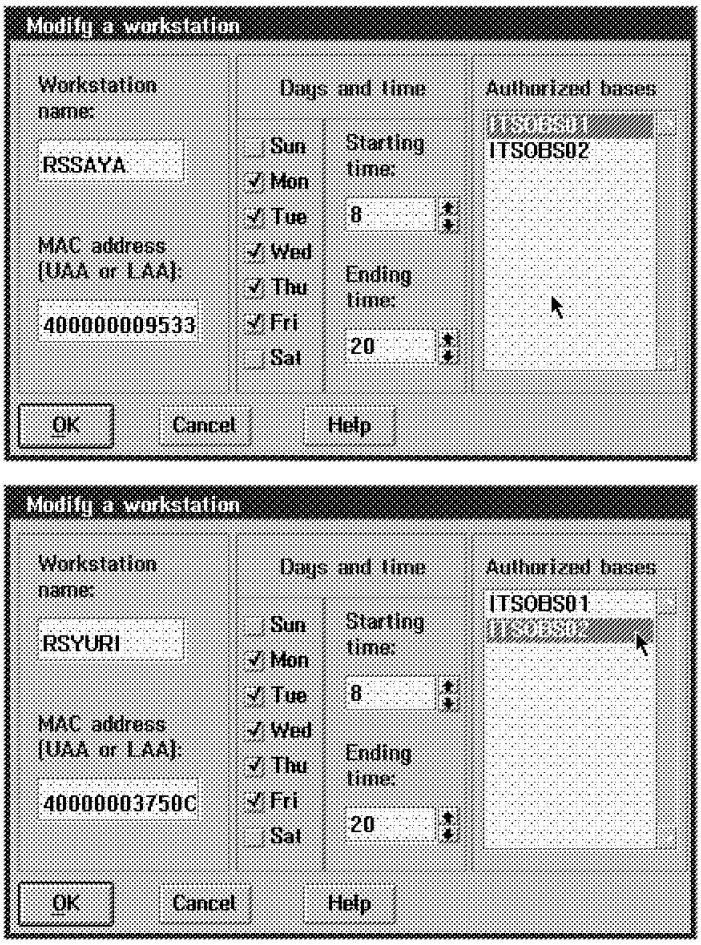


Figure 46. Adding/Modifying Access Control of Workstations. These windows describe adding or modifying the access control of two workstations defined in this configuration scenario.

Important

The Workstation name must be from 5 to 8 alphanumeric characters without any spaces. The Workstation name must be unique in the network. This name is the descriptive name of the workstation (as assigned by the network operator).

The MAC address is the Universally Administered Address (UAA) or the Local Administered Address (LAA) of the IBM Wireless LAN adapter in the workstation. In both cases, the address consists of 12 hexadecimal characters.

Before you enable Access Control, you should create a list of authorized base connections for the workstations. Otherwise, workstations will not be able to access the network.

When you enable/disable Access Control, the changed information will be dispatched to all the base stations in a Base list dynamically. However, the Access Control information will not be dispatched to any wireless remote workstations in your network. If a workstation is already registered with a base, and has been denied access by an Access Control change, the connection remains in place until the workstation is power-on-reset again.

To complete the premised scenario, the Access Control must be installed if:

- There is one base station in each network with identical NETIDs.
- The workstations in each network, located in overlapping cells, have a chance to connect with the wrong base station.
- It may be necessary to balance the network load.

If you do not enable access control, workstations in this scenario can attempt to communicate with both base stations because they are located in close proximity with one another. Therefore, the remote workstations may select the base stations with whom the wireless workstation communicates first.

Note: An advantage of this scenario is that if one of the base stations is not operating, wireless workstations have access to another operational station.

Parameter	Description
Workstation list	This shows the workstation name and MAC address of every workstation in the network.
Authorized base list	This shows the name of each base station to which the selected workstation is allowed to connect.
Access Control check-box	To enable Access Control, select the Access Control check box. To disable Access Control, deselect the Access Control check box.
Authorize days check-boxes	When the check box has a check mark in a day, the workstation is authorized to connect on that day.
Authorize time box	The workstation is authorized to connect during the hours detailed.
Add push button	This is to add a new workstation to the list and define its access rights.
Delete push button	This is to delete a workstation selected in the list.
Modify push button	This is to modify a workstation information and its access rights.

4.12.5 Network/Base Security

The Network and Base Security page of the NAP notebook allows you to install security on the Base stations. Use the 4.12.6, “Workstation Security” on page 102 of the NAP notebook to perform the second step, which is to install security on the workstations.

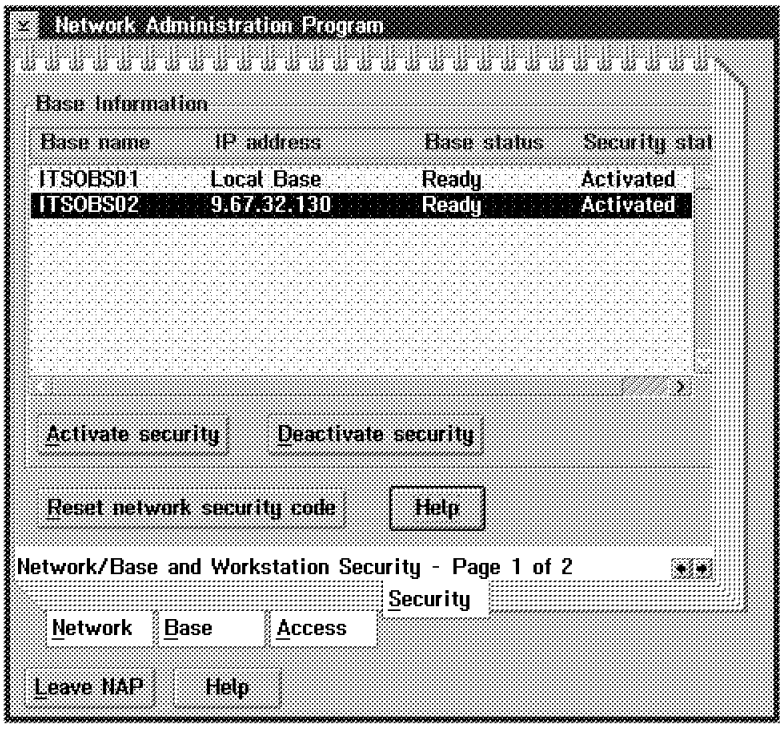


Figure 47. Network/Base and Workstation Security (Page 1 of 2). This shows that the security status of both base stations is activated. This configuration scenario will install the security function (an authentication process between the wireless workstation and the base station).

Important

Security is an optional function of the IBM Wireless LAN. Initially, security is not installed. Activating security is a two-part process and must be done in the following order:

1. Install security on each base station in the network.
2. Compute the security code for each workstation in the network, and then install the security key on the workstation.

   If you select **Reset network security code**, the security status of base stations will change from Active to Action Needed. Each base station controlled by this NAP will reactivate security and then all workstations in the network will have their security status verified.

When you activate/deactivate the security function, the updated status will be dispatched to all base stations in the Base list dynamically. However, the security information will not be dispatched to any wireless workstations in your network. If a workstation is already registered in a base, it is required to use a security code according to the security function change; any existing connection is still continuously available. The change will take place when the workstation is disassociated from the cell.

Functions	Description
Activate security button	To activate security on a base station, select it from the Base list, then select this push button. **Note:** You can activate security on a base station only if its operational state is ready.
Deactivate security button	To deactivate security on a base, select it from the Base list, and then select this push button. **Note:** You can deactivate security on a base station only if its operational status is Ready.
Reset network security	This is used to change the security code for the entire network.

4.12.6 Workstation Security

The Workstation Security page of the NAP notebook allows you to install security on the workstations. A unique workstation security code, based on the workstation name and the Universally Administered Address (UAA) of the IBM Wireless LAN controller card, is computed for each workstation. This security code must be manually entered at the workstation.

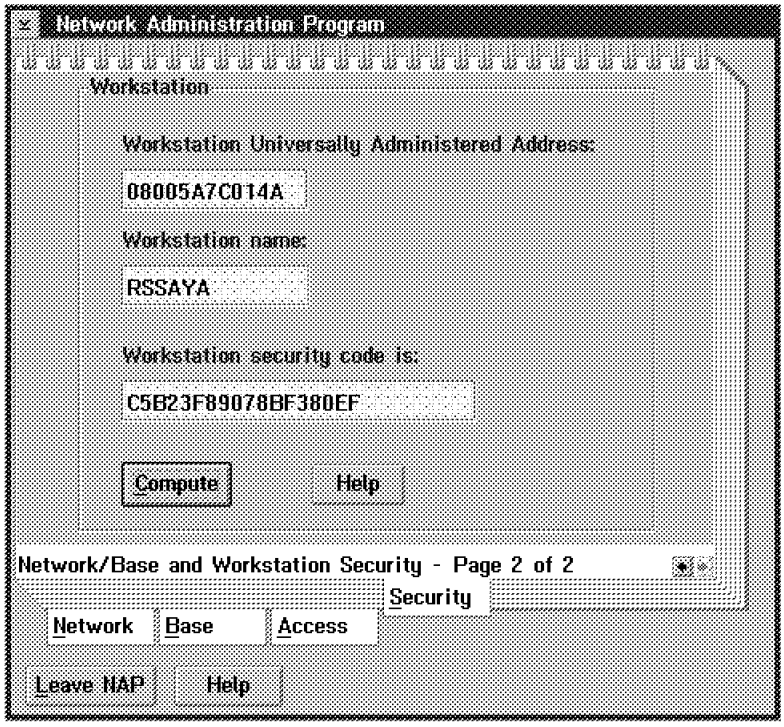


Figure 48. Network/Base and Workstation Security (Page 2 of 2). This shows a calculated security code for a workstation named RSSAYA and a workstation UAA of 08005A7C014A. To enable the authentication process, the security code must be installed in the PROTOCOL.INI file in the wireless workstation. See Figure 49 on page 103 for the wireless section in the PROTOCOL.INI.

```
[IBMWLO_nif]

   DriverName = IBMWL$
   NetWorkId = "ITSO01"
   StationName = "RSSAYA"
   CountryCode = 1
   Compression = "YES"
   DataMasking = "auth"
;  DataMasking = "none" ..default setting
   EncodedName = "C5B23F89078BF380EF"
   NETADDRESS = "400000009533"
```

Figure 49. Installing Authentication Process in Wireless Workstation. The DataMasking section will be changed to auth and the EncodedName will be newly added with the security code calculated in Workstation Security Page (Figure 48).

Important

Before installing security on the workstations you must have already installed security on at least one base station by using the process outlined in 4.12.5, “Network/Base Security” on page 101.

The PROTOCOL.INI or STARTUP.NCF in all workstations must be changed to match the active security function for the base station accessed. The security code is controlled by the Network Administrator.

Functions	Description
Workstation UAA	In the Workstation Universally Administered Address field, type the UAA of the controller card in the workstation for which you are installing security. For the UAA, refer to your Workstation Planning Worksheet in your IBM Wireless LAN manual entitled *Installing and Operating Your Network*.
Workstation name	In the Workstation name field type the name of the workstation for which you are installing security. This is the descriptive name of the workstation.
Workstation security code	The Workstation security code is based on the workstation name and the Universally Administered Address of the IBM Wireless LAN controller card in the workstation. This field displays the code after it has been computed.
Compute	After you have entered the workstation name and workstation UAA, select this button to compute the security code for the workstation.

The security status field in the Base Information page in OS/2 NAP (Figure 44 on page 97) will also be changed as follows.

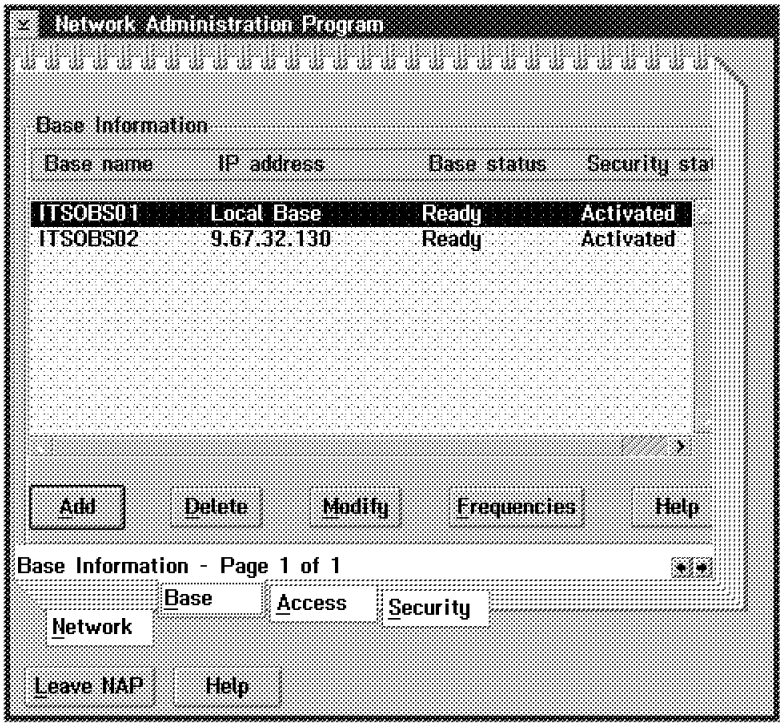


Figure 50. Security Activated in Base Information Page in OS/2

4.12.7 Base Station Registration

The Base Information list (Figure 44 on page 97) in the NAP allows you to set the current status of base stations in the network. In this scenario, the base station named ITSOBS01 is also a NAP station for this network. It is easy to determine whether the base station named ITSOBS02 is operational or not by using the NAP. The base station, without NAP, does not have a graphical user interface, and will log registration information in IBMWLERL.LOG in your IBM Wireless LAN product directory. This file is created in both a base station with a NAP and without a NAP.

```
LogID    : 15
LOGO054  : Mon Apr 10 10:45:40 1995
Component: Wireless Control Agent
Module   : A2NET.C   line 1037
Information: the adapter has been successfully opened (Network Name: ITSO01,
NAP IP Address: 0.0.0.0, Base Name: ITSOBS01 with MAC Address:
400090002002).

LogID    : 18
LOGO057  : Mon Apr 10 10:45:41 1995
Component: Wireless Control Agent
Module   : A2NET.C   line 1349
Information: the base has successfully contacted the NAP station (Network Name:
ITSO01, NAP IP Address: 0.0.0.0, Base Name: ITSOBS01 with MAC Address:
400090002002).
```

Figure 51. Sample Logged Messages of Base Station with NAP (IBMWLERL.LOG)

If the communication between the base station and the NAP station were disconnected for any reason, the base station can continuously and properly perform its role. This is because the base station is keeping cell data, such as Base name, Access Control information and security codes. When

communications with the NAP station is restored, the wireless workstations of the base station are not affected.

```
LogID    : 15
LOG0054  : Mon Apr 10 10:45:40 1995
Component: Wireless Control Agent
Module   : A2NET.C   line 1037
Information: the adapter has been successfully opened (Network Name: ITSO01,
NAP IP Address: 9.67.32.110, Base Name: ITSOBS02 with MAC Address:
400090001001).

LogID    : 18
LOG0057  : Mon Apr 10 10:45:41 1995
Component: Wireless Control Agent
Module   : A2NET.C   line 1349
Information: the base has successfully contacted the NAP station (Network Name:
ITSO01, NAP IP Address: 9.67.32.110, Base Name: ITSOBS01 with MAC Address:
400090001001).

LogID    : 150
ERR0040  : Mon Apr 10 14:46:40 1995
Component: Wireless Control Agent
Module   : A2NET.C   line 676
Alert 9: the base lost contact with the NAP station (Network Name: ITSO01,  NAP
IP Address: 9.67.32.110, Base Name: ITSOBS02 with MAC Address: 4000900010001).

LogID    : 159
LOG2084  : Mon Apr 10 14:52:12 1995
Component: Wireless Control Agent
Module   : A2NET.C   line 500
Information: the base has recovered its communication with the NAP station
(Network Name: ITSO01, NAP IP Address: 9.67.32.110, Base Name: ITSOBS02 with
MAC Address: 400090001001).
```

Figure 52. Sample Logged Messages of Base Station without NAP (IBMWLERL.LOG)

4.12.8 Wireless Workstation Registration

A wireless workstation will attempt to register with a base station when the IBM Wireless LAN adapter driver is loaded by the DEVICE= statement in a DOS or OS/2 CONFIG.SYS. If there were no errors in the device driver loading and binding process, then by using RSSI (Receive Signal Strength Indicator), it is possible to confirm not only the strength of the radio signal but also whether the wireless workstation was registered successfully or not. For more information on RSSI, please refer to *Installing and Operating Your Network*. In a base station it is difficult to know how many wireless workstations are registered, if Access Control is not installed. Wireless workstations can access base stations only if their network names match.

Registration status is not managed in the NAP station but rather in each base station. Wireless workstation registration information will be logged in the IBMWLERR.LOG file. Any registration error, such as an access violation, security mismatch or a security code error will be logged in the IBMWLERL.LOG file.

```
LogID    : 148
LOG0062  : Mon Apr 10 14:39:28 1995
Component: Wireless Control Agent
Module   : A2IDD.C   line 226
Workstation Name: RSSAYA   with MAC address: 400000009533 has been registered
(Network Name: ITSO01, NAP IP Address: 9.67.32.110, Base Name: ITSOBS01 with
MAC Address: 400090002002). Call ID = 8555555555555186.

LogID    : 157
LOG0062  : Mon Apr 10 14:46:55 1995
Component: Wireless Control Agent
Module   : A2IDD.C   line 226
Workstation Name: RSYURI   with MAC address: 40000003750C has been registered
(Network Name: ITSO01, NAP IP Address: 9.67.32.110, Base Name: ITSOBS02 with
MAC Address: 400090001001). Call ID = 8555555555555186.
```

Figure 53. Sample Logged Messages of Base Station (IBMWLERR.LOG)

```
LogID    : 163
LOG1209  : Mon Apr 10 14:57:22 1995
Component: Adapter
Module   : NMDDR.C   line 217
Information: communication with the Workstation Name: RSSAYA   with MAC
Address: 400000009533 through the base with controller card having MAC
Address: 400090001001 is lost due to no response from the workstation.

LogID    : 24
ERR1202  : Mon Apr 10 15:10:02 1995
Component: Adapter
Module   : NMDDR.C   line 177
Alert 22: registration of the Workstation Name: RSSAYA   with MAC Address:
400000009533 through the base adapter with controller card having MAC Address:
400090002002 failed due to authentication failure detected by the base.

Control  : 196
Component: Wireless Control Agent
Module   : A2ACC.C   line 458
Alert 20: registration of Workstation Name: RSYURI   with MAC Address:
40000003750C rejected by NAP due to access control (Network Name: ITSO01 NAP
IP Address: 0.0.0.0, Base Name: ITSOBS01 with MAC Address: 400090002002)
```

Figure 54. Sample Logged Messages of Base Station (IBMWLERR.LOG)

Wireless workstations cannot contact a base station when in certain situations, such as an adapter error, no signal in the air, access violations or security problems. The reason for the fault, depending on the operating system, will be logged in a file or displayed on the screen. If your workstation operating system is OS/2, the message will be logged in LANTRAN.LOG. In the case of DOS, it will be logged in WIRELESS.LOG. Typical messages for wireless workstations are the following:

IWL001 No base heard.
: This message might be caused by the lack of a base station name matching the name that the workstation has attempted to use. This could occur with a configuration typographical error for example.

IWL008 Security mismatch with the base contacted.
: The security function must be installed in the wireless workstation.

IWL009 Registration rejected by the NAP due to access control.
: This message is caused by the wireless workstationtrying to access either the wireless network during an unauthorized service window, or access a base station for which it is unauthorized.

IWL011 Security problem detected by the base.

The security code in the wireless workstation, calculated by NAP, is not correct. It is necessary to confirm the code.

Appendix A. IBM Wireless LAN Frequency Hopping

This section covers some points of interest for the IBM Wireless LAN. A wireless LAN installation will consist of a set of base stations with overlapping coverage areas. Therefore, a key function in successful operation is the control of potential interference by managing frequency hopping patterns used by different base stations.

There are several things to consider in this regard. Each alone is an adequate defense against a range of wireless issues. Taken together they pose a strong guard against such undesirable effects as radio-frequency interference or deliberate intrusion.

A.1 Hopping Pattern Selection

Interference between adjacent cells is minimized by the proper assignment of frequency hopping patterns by the base stations. In our Wireless LAN programs the frequency hopping technique is used for interference management and not for data masking. It is also used to conform to Federal Communication Commission (FCC) Part 15.247 for ISM bands. Each base station follows a cyclical frequency hopping pattern and all base stations operate asynchronously.

The management of inter-cell interference is done through the use of an orthogonal frequency hopping pattern for adjacent cells. Orthogonal FH patterns share the characteristic that even in a worst-case situation only one hop interference (at most) will occur between two hopping patterns when networks overlap geographically.

Base stations will randomly select the hopping pattern for the stations in a cell to use from a set of existing patterns.

Remote stations acquire the hopping sequence by listening to the base station's broadcast of the MAC protocol headers on a given frequency. This allows the remote stations to contend for access and to later transmit signals on their own using the acquired frequency hopping pattern in a given time slot dictated by the base station. The base stations in turn manage a dynamic hopping pattern that allows for the insertion/deletion of frequencies as well as a complete pattern replacement. This acquisition and control is embedded within the robust MAC used by the IBM Wireless LAN products.

A.2 Interference Management

In an environment with multiple autonomous networks there is a probability greater than zero that two collocated base stations (with different logical LANs) will use the same frequency hopping pattern. If two base stations are using the same pattern, the WLAN protocol detects this situation and performs a *hop advance* (advance the pattern by half a pattern). In the presence of a narrow band interferer, the base station adapter detects the interference. It requests a new FH pattern (minus the offending frequency) from the Wireless Control Agent and starts using the new FH pattern immediately once it is acquired.

In the USA, this approach will allow the following:

- One channel interference (same channel): 66 patterns.
- One channel and one adjacent channel on each side interference (total of three interfering channels): 22 patterns (however, with topology information it would be possible to have 66 patterns without significant degradation).
- There are *n* frequency channels (23 in Japan, 79 in the USA) available for use in hopping patterns. The number of frequencies that may be used is a factor of the range or frequency spread mandated by regulation, the maximum frequency bandwidth allowed, the minimum/maximum number of frequencies that may be used and a mathematical algorithm that determines the patterns based on the use of a prime number (23, 79).

  Suppose that a given frequency channel is interfered with by another station using a hopping pattern that overlaps occasionally on the same or an adjacent channel (for any *k* adjacent channels, channel 10 is interfered with by channels 10-k, 10-k+1, ...,9, 10, 11..., 10+k-1, 10+k). The design of the hopping patterns used by the IBM Wireless LAN ensures that successive channels in a pattern are at least 7 MHz away from each other. Thus there are (n-13)/(2k+1) frequency-insensitive hopping patterns in the absence of topology information.
- As stated in FCC Part 15.247 the minimum number of frequencies to be used in a frequency hopping pattern is 75 (stations may use no more than 1 MHz of bandwidth). This does not mean you must use 75 hops but rather that the design must be frequency-agile across a signal range that is 75 MHz wide. As there is room for 82 x 1 MHz of those frequencies (2.4-2.483 GHz and 2.4 GHz is not used) there are 7 frequencies left over for use as spares. These may be substituted into a hopping pattern in order to contend with narrow-band interferers.
- In the unlikely case that a user is affected by IBM Wireless LAN interference, the network operator can also insert and delete specific frequencies from the Network Administrator Program console.

Appendix B. Wireless LAN Performance

The following section describes issues in the optimization of performance for wireless LANs.

B.1 Optimizing Network Performance

For wireless LANs, well-defined areas simply do not exist, as radio wave propagation characteristics are dynamic and unpredictable; small changes in position or direction can result in drastic difference in signal strength. In fact propagation patterns will change dynamically as stations, people and objects in the environment move. Generally, we refer to *areas of coverage* when talking about Wireless LANs. However a more appropriate term would be to use the term ″volume.″ For convenience reasons we will use the term ″area″ as this concept is more familiar and therefore easier to work with.

As in any other analog transmission system, a radio-frequency local area network is impaired by signal attenuation and noise. Unlike its wired counterpart, which may incur a Bit Error Rate (BER) of less than 10^{-12}, a wireless LAN may have a BER that is typically in the range of 10^{-5}. 10 to the negative 5th. During normal operation special attention should be paid to minimize errors which will reduce overall network throughput.

The challenge for indoor communications, where base and remote stations are either stationary or slowly moving, is to calculate the probability of signal impairment and what counter-measures are available. Radio channels may suffer from distortion of the transmitted signal due to amplitude attenuation, fading, time delay, phase shifts or some combination of any or all of these.

B.1.1 Path Loss

Path loss is the attenuation of signal strength over distance. When there are no obstacles (as in free space), signal strength decreases as the square of the distance between transmit and receive antenna (inverse square law in free space).

But for indoor transmissions, in a modern partitioned office building for example, signal strength can be reduced up to the fifth power of the distance or greater. In addition to path loss, electromagnetic barriers may exist between a transmit and receive antenna pair, such as:

- Metal surfaces surrounding the antenna
- Reinforced concrete walls, floor, ceiling
- Metallic furniture
- Metallic poles may shadow some area

In addition to the above parameters which are pertinent in any transmission system there are other parameters: radio waves can be reflected, absorbed, or blocked. Therefore radio conditions can vary significantly from site to site and even moment to moment. However these issues can often be addressed by simply adjusting antenna placement and positioning.

B.1.1.1 Propagation Laws

The well-known formula for determining path loss is a R^{-n} law, where R is the distance between transmitter and receiver (you may think of *R* as the radius of a circle). In free space the path loss exponent is considered to be 2. However, for indoor transmission different values can be used depending on the environment. For example, within building hallways, channel RF energy may experience less loss than free space propagation. But the exponent may increase from 2 to 12 with increasing values of *R*, depending on the obstacles between the transmitter and receiver. In case of obstructed transmissions the following exponent law may be used:

2 for 1 < R < 10m

3 for 10< R < 20m

6 for 20< R < 40m

12 for R > 40m

The larger values of *n* are due to the likelihood of an increasing number of signal attenuators (notably walls and partitions) between the transmitter and receiver when *R* increases.

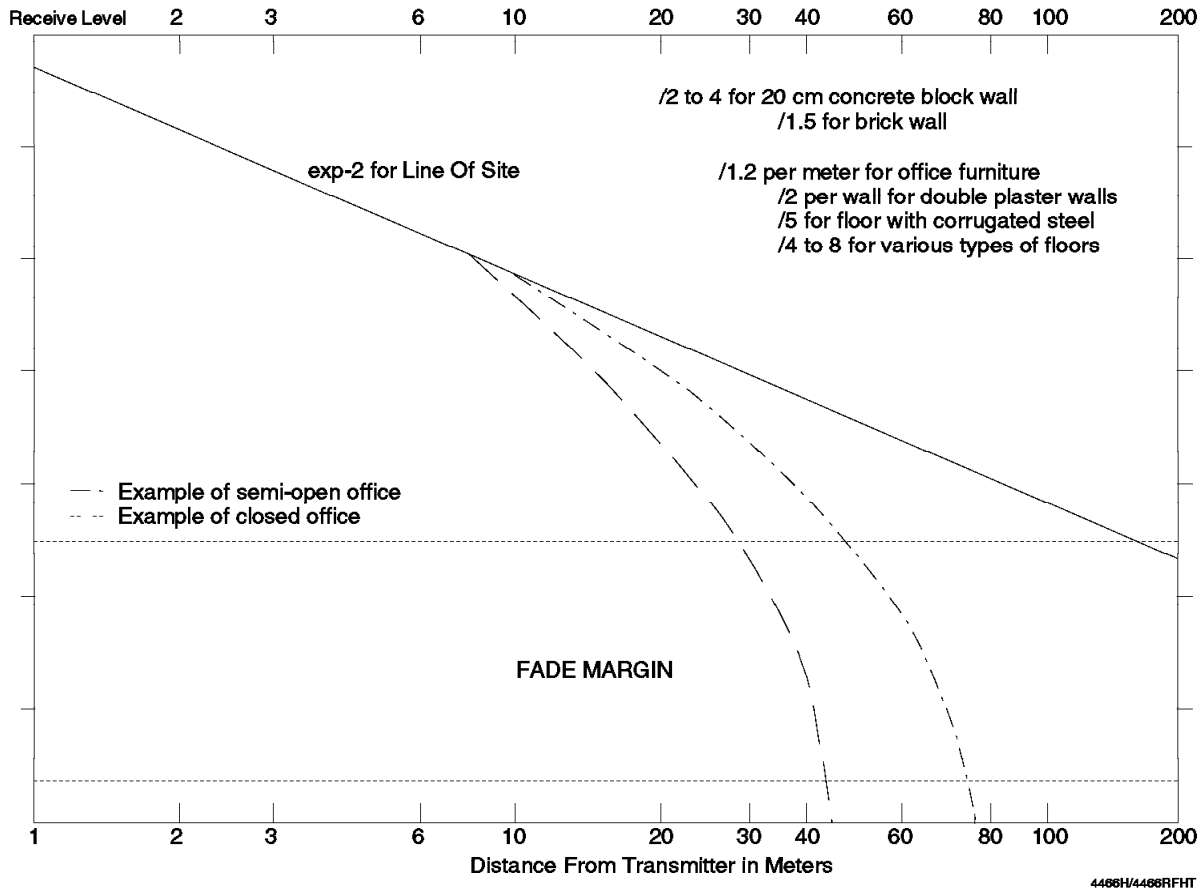


Figure 55. Receive Level versus Distance from Transmitter at 100 mW/2.4 GHz

Table 18. Typical Values of Multiplicative Path Loss versus Free Space	
Environment/obstacle description	**Path loss ratio versus free space (exponent 2)**
Office LOS	1
Office OBS	1 to 2
Concrete block wall	3 to 5
One floor separation	3 to 4
Storage rack with textile products	1.5 to 3
Storage rack with paper products	1.2 to 2
Storage rack with metal parts	2 to 4
Note: LOS: Line of sight OBS: Obstructed	

B.1.1.2 Propagation through Floors

Although propagation through floors is possible under certain conditions, it is not recommended in most circumstances, since overall path loss will be very high. Path loss is not directly a multiple of the number of floors, as other phenomena will occur, including diffraction or reflection from buildings on the other side of the street, for example.

B.1.2 Multipath Fading

Multipath channels cause signals to experience fading due to constructive and destructive interference between replicas of the transmitted signal. Walls, metallic tinted windows, and office cubicles can attenuate signals while inducing multiple reflections that arrive tenths to hundreds of nanoseconds after the first signal component reaches the receiver. Small movements can produce phase shifts in individual multipath components that result in large variations of their coherent sum. Therefore, fading describes small scale variations that occur over short distances (on the order of a meter or less) and small time intervals (on the order of seconds or milliseconds).

B.1.2.1 Flat Fading

Flat fading can occur when the delay spread, which corresponds to the difference in arrival time due to different paths, is significantly less than the bit duration. Here the time dispersion of the channel has a negligible effect on the shape of the transmitted signal, and only the signal gain of the channel varies with time. The amplitude patterns of flat fading signals are often modeled by one or several probability distributions, such as:

Weibull Appropriate for line-of-sight topographies and when there is motion around portable stations.

Nakagami Appropriate when there is motion around base stations.

Log-normal Appropriate for shadow fading which corresponds to blockage and attenuation of signal by walls or doors.

Ricean More applicable to obstructed, but still applicable with a strong direct path and to cellular coverage.

Rayleigh Occurs when a direct path is blocked, and transmitter and receiver are immersed in highly scattering surroundings.

In office buildings where the environment is divided into separate rooms, fading occurs in bursts lasting tens of seconds, with a dynamic range of about 30 dB.

For an open space office, fading has been observed to be rather continuous with a dynamic range of 7 to 10 dB.

As the distance between two possible fades is about lambda/2, if a mobile station moves at 3.6 km/h, then the number of possible fades per second will be about 1/(3/24x2) = 16. Fortunately, fading with significant amplitude does not occur that often. When it does occur it is predicted by statistical distributions which vary with the environment.

B.1.2.2 Frequency Selective Fading

This corresponds to a channel response at time *t* resulting from an impulse applied τ seconds in the past. This can be modeled by the Doppler spread and scattering functions.

- Simple Doppler effect (absence of scatterers)
  - Variation in frequency of the received frequency due to the movement of the mobile relative to the fixed transmitter
  - Random frequency shift modulation
  - Doppler-induced random FM is correlated with vehicle speed $f_d = f_m$ cos, where f_m= V/lambda is the maximum Doppler frequency (8 Hz at 3.6 km/h for 2.4 GHz)
  - Affects all multiple modulation paths: some with a positive shift and some with a negative shift, depending upon the arrival angle
- Doppler effect with a single scatterer

  When reflected by a perfect scatterer, a received signal will present nulls proportional to the velocity of the transceiver.
- Doppler effect with multi-scatterers in the vicinity of a mobile station

  In this case the resultant received signal is the sum of all scattered waves from different angles. However, it has been shown that it is the frequency modulation resulting from the highest direct Doppler frequency for a given velocity that is the most probable cause of a Doppler shift in a mobile receiver.

For in-building transmissions there will be a lot of scatterers. Some of them will be highly attenuated due to the beamwidth of the receiving antenna. Due to the relatively low velocity of roaming mobile stations the effect of a Doppler shift should not be of concern at WLAN data rates.

When both transceivers (base and mobile) are stationary, motion of people and equipment around the antennae results in multipath disturbances and fading effects.

B.1.3 Interference

Free space used by wireless LANs is sometimes noisy and occupied by various potential and actual sources of interference. Signal interference or radio frequency noise is an environmental signal that is not readily detected and therefore not always considered. Nevertheless if signal interference is present in your environment, then this RF noise will be detected by the receiving antenna of your station. This kind of interference is monitored by the IBM Wireless LAN and is tracked in an event log (IBMWLERL.LOG for Novell). The source of an interfering signal may be:

- Another radio-frequency network from another vendor
- An adjacent IBM Wireless LAN network with a different network ID
- Microwave ovens
- Security systems
- Elevators motors
- Photocopiers
- Known sources of strong electromagnetic disturbance

The effect of these noise sources can be mitigated by proper antenna placement.

B.1.3.1 Co-located Networks

Interference from co-channel and adjacent channel users is a major source of channel impairment in mobile communications and the ratio between the desired signal and the interfering signal might often be in the range of 1000. The presence of people in a room impacts the path loss primarily if the antenna height is low. Placing an antenna in a higher position will usually obtain a gain of 4 to 6 dB in path loss.

Because propagation in buildings is difficult to predict and will vary constantly, interference from other networks/users can be a serious problem. The IBM Wireless LAN has a dynamic monitoring capability to detect interference through continuous sampling of the Bit Error Rate per channel. If a particular channel demonstrates consistently high levels of interference it is dynamically replaced by another one. Thus, with dynamic channel assignment, interference does not affect the reliability of the system as long as there are quiet channels available. Dynamic channel assignment cannot work if there is interference on every channel.

Another technique to reduce interference among users is power control. As discussed above, within a coverage area the signal attenuation between receiver and transmitter can vary widely, by as much as 60 dB or more. If all Base stations and remote stations transmitted at the same power level, received and transmitted signals may differ in power, again by as much as 60 dB. This creates an adjacent channel interference problem.

To counteract this problem, a remote station′s transmit power is adaptively controlled. This should have the effect of minimizing the amount of interference generated within physically proximate networks. Over and above the dynamic capability of the IBM Wireless LAN, there is a manual facility as well which may be used to reduce the transmit power. This function not only reduces interference between cells or networks but also increases the average number of cells and users per square meter. Still another action is possible for stationary systems which consists in antenna focusing. The transceiver uses a patch antenna. This design offers some directional sensitivity (more gain in one direction). Aiming the antenna towards the transceiver/receiver will minimize the interference, while it improves the overall signal quality and strength for both stations.

B.1.3.2 Impulse Noise

In the 2.4 Ghz band a primary source of noise is the microwave oven. The spectrum of noise generated by microwave ovens has a bandwidth greater than 30 MHz. The noise bursts produced by the microwave oven have a duration (16ms or 20ms) that is linked to the power source, 50 Hz or 60 Hz AC with a duty cycle of 50%. Most microwaves operate at a nominal frequency of 2.45 GHz, although this drifts over many tens of MHz in a few seconds.

Other sources of interference include impulse noise produced by copiers, elevator door switches and so forth. Typically, noise peaks are about 2 to 18 dB higher in the 900 MHz band than in the 2.4 GHz band. The occurrence of noise is typically an order of magnitude lower at 2.4 GHz than it is at 900 MHz. Impulse noise generated by a photocopier is significantly higher than that produced by elevator door switches. The average impulse noise duration is less than 200 ns and the average between two pulses is in the range of 1 to 10 ms for the interference sources of particular interest in wireless LAN applications.

B.1.4 Delay Spread

Delay spread is a factor that impacts both reliability and the BER. Delay spread is characterized by channel frequency selective fading. This can occur anywhere but is of primary concern in very large warehouses, atriums, and facilities surrounded by metal walls. As the distance between antennae increases so does the delay spread. If antennae are 5 meters apart then the delay spread is typically 20 ns, while at 30 meters apart it might be 35 ns but values over 100 ns have been reported. The counter-measure for stationary remote stations is selective antenna positioning, which breaks the reflection causing the frequency selective fading.

B.1.5 Cell Arrangement

The placement of the base station is of primary importance when planning the installation of your network. The clearance around the antenna should be sufficient to allow propagation of radio waves in all directions. However, if you want to radiate in a preferred direction you should position the front of the antenna (the side with the IBM logo) in that direction. The highest directional sensitivity is oriented along this plane. To maximize the cell coverage area place the base station antenna as close to the center of your cell as practical. The following radiation pattern is typical for the IBM Wireless LAN antenna design.

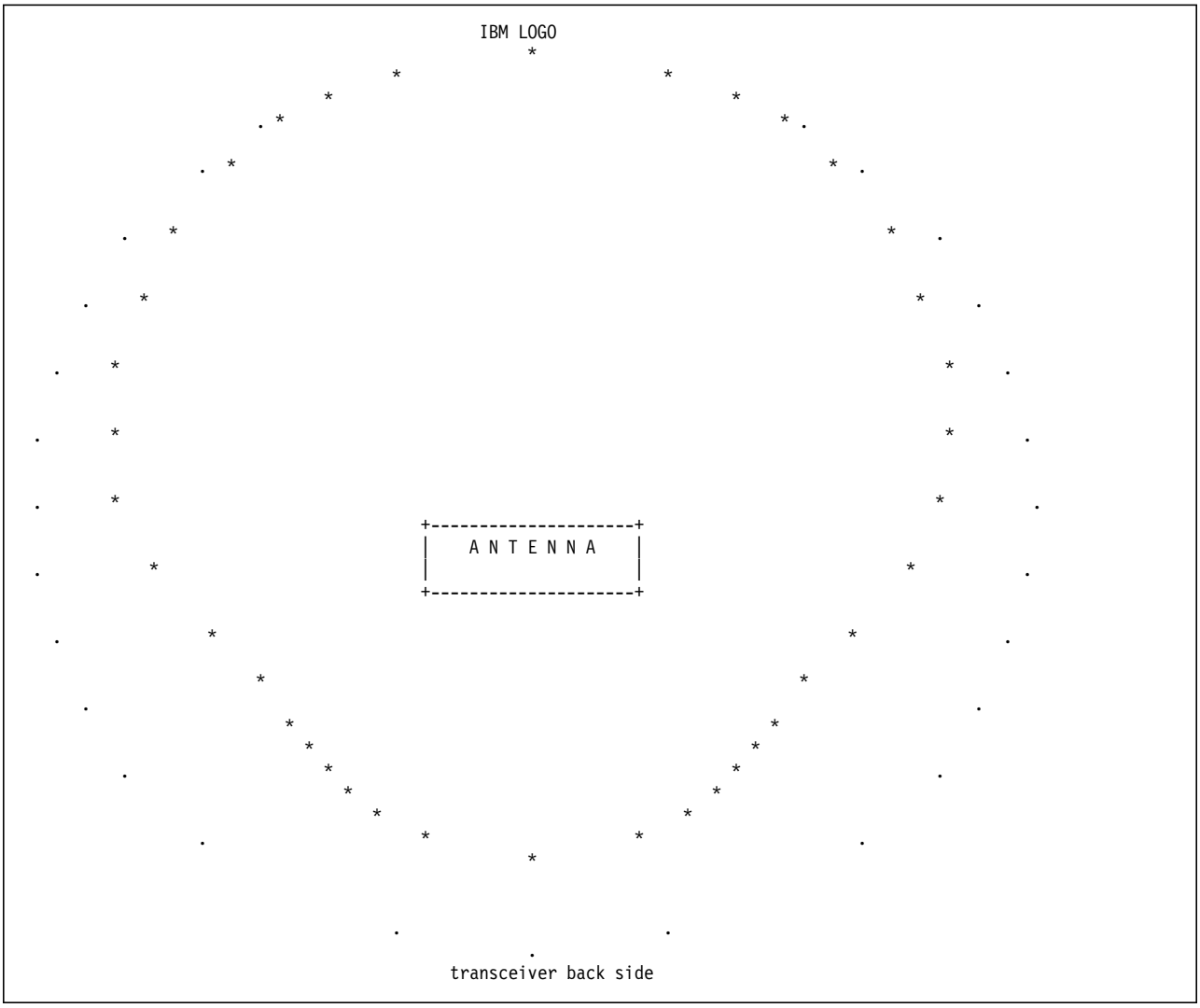


Figure 56. Antenna Directivity in Azimuth and Elevation

The power radiated by the antenna is proportional to its radiation pattern distributed over the *surface* of a large *sphere* with the antenna located at its center.

B.1.6 Trouble Shooting List

The following items are potential sources of signal integrity problems. Review this list when you are experiencing difficulty transceiving or receiving with stations in your wireless LAN.

B.1.6.1 Antenna Positioning

The patch antenna (5 cm by 5 cm) of the transceiver is placed just behind the IBM logo.

- The IBM logo must be visible. If the transceiver is mounted on a desk, do not place the transceiver upside down. Best propagation results are obtained when directing the IBM logo toward the base station. Directing the transceiver in the proper direction may improve the signal strength by a factor of 2 to 3.
- Clear the area (in front of the IBM logo) surrounding the antenna to improve propagation.
- Avoid placing large objects around the transceiver.
- If it is a stationary unit, place the transceiver in the highest convenient position. This will reduce signal degradation from furniture and moving people as well as modular partitions if they do not go up to the ceiling. But don′t place it next to the ceiling; maintain at least 30 cm of clearance.
- In case of weak signal strength look for any large metallic items (white board, cabinet, water cooler) in the signal path.
- Do not place the transceiver close to moving objects such as large fans, moving doors, conveyor belts.
- Do not place the transceiver close to any sources of electromagnetic or radio frequency interference such as a microwave oven, radar, or any other wireless system.
- The radio is not waterproof; don′t place it outside a building.
- Do not use metal items to mount the transceiver.
- Do not glue anything on the antenna side (IBM logo) of the radio.
- For the base station use the following additional guidelines:
  - Place the base station transceiver close to the center of your cell. Bear in mind that the propagation path behind the radio is less than half as long as it is in front. Use the intersection of corridors to broadcast in all directions of the corridors (corridors *guide the waves*).
  - Place the radio vertically; do the same thing for the radios of the remote workstations.
  - Orient the transceiver in the direction of the furthest workstation.

The above are suggested remedies that may help you in your environment. The IBM Wireless LAN product has many built-in features to overcome a variety of problems. You can help it do so by keeping these tips in mind when you are installing and/or trouble-shooting your network.

Appendix C. Wireless Environment Sample Files

This section documents the equipment and their applicable parameter settings that were used in our examples.

C.1 IBM Wireless LAN OS/2 Base Station

All IBM Wireless LAN scenarios for the OS/2 Base stations were conducted with the following products:

C.1.1 Wireless Base Station ITSO01

Hardware	*Specification and addressing*
Machine type and model	8565-321
Memory	16 MB
Hard disk	80 MB
Wired LAN adapter	IBM Token-Ring 16/4 Adapter
Wireless LAN adapter	IBM Wireless LAN ISA/MCA Adapter
MAC address of wired LAN	0x400090000002
MAC address of wireless LAN	0x400090002002
IP address	9.67.32.110

Software	*Version*	*CSD Level*
OS/2	3.0	XR03001
LAPS	2.20.2	WR07045
Wireless LAN	1.00.1	I91
TCP/IP for OS/2	2.00	UN56401

C.1.2 Wireless Base Station ITSO02

Hardware	*Specification and addressing*
Machine type and model	8580-071
Memory	16 MB
Hard disk	65 MB
Wired LAN adapter	IBM Token-Ring 16/4 Adapter
Wireless LAN adapter	IBM Wireless LAN ISA/MCA Adapter
MAC address of wired LAN	0x400090000002
MAC address of wireless LAN	0x400090002002
IP address	9.67.32.130

Software	*Version*	*CSD Level*
OS/2	2.11	XR06200
LAPS	2.20.2	WR07045
Wireless LAN	1.00.1	I91
TCP/IP for OS/2	2.00	UN56401

C.1.3 Server on Wired LAN Named SAMBADOM

Hardware	*Specification and addressing*
Machine type and model	8565-321
Memory	16 MB
Hard disk	320 MB
Wired LAN adapter	IBM Token-Ring 16/4 Adapter
MAC address of wired LAN	0x400090000002
MAC address of wireless LAN	0x400090002002
IP address	9.67.32.160
Domain name	SAMBADOM

Software	*Version*	*CSD Level*
OS/2	3.0	XR03001
LAPS	2.20.2	WR07045
OS/2 LAN Server	3.0	IP07000
OS/2 LAN Requester	3.0	IP07000
TCP/IP for OS/2	2.00	UN56401

C.1.4 Wireless Workstation RSSAYA

Hardware	*Specification and addressing*
Machine type and model	PS/2 E
Memory	8 MB
Hard disk	120 MB
Wireless LAN Adapter	IBM Wireless LAN PCMCIA Adapter
MAC Address of Wireless LAN	0x400000009533
IP Address	9.67.32.120

Software	*Version*	*CSD Level*
OS/2	3.0	XR03001
LAPS	2.20.2	WR07045
Wireless LAN	1.00.1	I91
TCP/IP for OS/2	2.00	UN56401
OS/2 LAN Requester	3.0	IP0700
CM/2	1.10	WR06150

C.1.5 Wireless Workstation RSYURI

Hardware	*Specification and addressing*
Machine type and model	ThinkPad 750C
Memory	4 MB
Hard disk	340 MB
Wireless LAN Adapter	IBM Wireless LAN PCMCIA Adapter
MAC Address of Wireless LAN	0x40000003750C
IP Address	9.67.32.150

Software	*Version*
PCDOS	6.3
Windows	3.11
LSP	1.35
TCP/IP for DOS	2.11
Wireless LAN	1.01

PC/3270	4.0
DOS LAN Requester	3.0

C.2 NetWare Base

All the IBM Wireless LAN scenarios of the OS/2 Base were built by the following materials:

C.2.1 Wireless Base Station ITSO03

Hardware	***Specification and addressing***
Machine type and model	8580-321
Memory	16 MB
Hard disk	80 MB
Wired LAN Adapter	IBM Token-Ring 16/4 Adapter
Wireless LAN Adapter	IBM Wireless LAN ISA/MCA Adapter
MAC Address of Wired LAN	0x10005AF80F9A
MAC Address of Wireless LAN	0x400090003003
Server name	BANK311

Software	***Version***	***CSD Level***
PC-DOS	5.0	UR37387
NetWare Server	3.11	
Wireless LAN	1.10	

C.2.2 Wireless Workstation RSSAYA

Hardware	***Specification and addressing***
Machine type and model	8565-321
Memory	16 MB
Hard disk	320 MB
Wireless LAN adapter	IBM Wireless LAN ISA/MCA Adapter
MAC address of IBM Wireless LAN	0x400000008565

Software	***Version***	***CSD Level***
OS/2	3.0	XR03001
NetWare for OS/2	2.11	
Wireless LAN	1.00.1	I91

C.2.3 Wireless Workstation RSYURI

Hardware	***Specification and addressing***
Machine type and model	Thinkpad 750C
Memory	4 MB
Hard disk	340 MB
Wireless LAN adapter	IBM Wireless LAN PCMCIA Adapter
MAC address of IBM Wireless LAN	0x40000003750C

Software	***Version***
PCDOS	6.3
Wireless LAN	1.01
Windows	3.11

C.3 Network Application Coexistence on DOS

The following sections detail some useful information on our environment.

C.3.1 Protocol Drivers and Memory Usage

The DOS wireless workstation uses the following LAN drivers to enable various network operating systems:

DXMA0MOD.SYS	IBM Local Area Network Support Program
DXME0MDO.SYS	802.2 Protocol Device Driver
DXMT0MOD.SYS	NetBIOS Protocol Device Driver
TCPDOS.SYS	TCP/IP Protocol Device Driver

We were successful in loading and binding the above protocols on IBMWL.DOS (IBM Wireless LAN DOS Device Driver) at the same time. The output of the used and free memory is in Figure 57. It would appear to be enough memory for many, if not most, DOS applications.

```
Modules using memory below 1 MB:

  Name             Total       =   Conventional      +  Upper Memory
  --------    ----------------     ----------------     ----------------
  SYSTEM      19,245   (19 KB)     19,101   (19 KB)         144    (0 KB)
  HIMEM        1,072    (1 KB)      1,072    (1 KB)           0    (0 KB)
  EMM386       4,096    (4 KB)      4,096    (4 KB)           0    (0 KB)
  IBMDOSCS    27,264   (27 KB)     27,264   (27 KB)           0    (0 KB)
  POWER        4,560    (4 KB)      4,560    (4 KB)           0    (0 KB)
  IBMWL       50,688   (50 KB)     50,688   (50 KB)           0    (0 KB)
  DXMEOMOD    40,096   (39 KB)     40,096   (39 KB)           0    (0 KB)
  DOSTCP       9,312    (9 KB)      9,312    (9 KB)           0    (0 KB)
  COMMAND      3,184    (3 KB)      3,184    (3 KB)           0    (0 KB)
  NETBIND      2,624    (3 KB)      2,624    (3 KB)           0    (0 KB)
  SMARTDRV    26,784   (26 KB)     26,784   (26 KB)           0    (0 KB)
  IBMDSS01     5,456    (5 KB)          0    (0 KB)       5,456    (5 KB)
  $ICPMDOS     3,344    (3 KB)          0    (0 KB)       3,344    (3 KB)
  AUTODRV     12,368   (12 KB)          0    (0 KB)      12,368   (12 KB)
  ANSI         4,208    (4 KB)          0    (0 KB)       4,208    (4 KB)
  PROTMAN         96    (0 KB)          0    (0 KB)          96    (0 KB)
  DXMAOMOD     1,312    (1 KB)          0    (0 KB)       1,312    (1 KB)
  DXMTOMOD    23,680   (23 KB)          0    (0 KB)      23,680   (23 KB)
  DOSKEY       4,096    (4 KB)          0    (0 KB)       4,096    (4 KB)
  FREE       472,128  (461 KB)    466,560  (456 KB)       5,568    (5 KB)

Memory summary:

  Type of Memory       Total   =    Used    +    Free
  ----------------  ----------   ----------   ----------
  Conventional         655,360      188,800      466,560
  Upper                 60,272       54,704        5,568
  Reserved             196,608      196,608            0
  Extended (XMS)     3,282,064    1,270,928    2,011,136
  ----------------  ----------   ----------   ----------
  Total memory       4,194,304    1,711,040    2,483,264

  Total under 1 MB     715,632      243,504      472,128

  Largest executable program size        466,352    (455 KB)
  Largest free upper memory block          5,376      (5 KB)
  PC DOS is resident in the high memory area.
```

Figure 57. Used and Free Memory in the IBM WLAN Station

C.3.2 PC/3270 for Windows

PC/3270 for Windows does not require any other drivers.

C.3.3 TCP/IP Enable

To enable TCP/IP, you have to add CALL TCPSTART as a new line in your AUTOEXEC.BAT file or type:

```
TCPSTART
```

and enter it from the DOS command line. The batch file will add one driver (INET.SYS) in memory. This driver will load itself from the free upper memory first. The size of the TCP/IP driver is 48784 bytes. The used and free memory will change.

```
Memory Type         Total  =   Used   +   Free
----------------  --------   --------   --------
Conventional        640 KB     227 KB     413 KB
Upper                59 KB      59 KB       0 KB
Reserved            192 KB     192 KB       0 KB
Extended (XMS)    3,205 KB   3,205 KB       0 KB
----------------  --------   --------   --------
Total memory      4,096 KB   3,683 KB     413 KB

Total under 1 MB    699 KB     285 KB     413 KB

Largest executable program size        413 KB  (423,104 bytes)
Largest free upper memory block          0 KB        (0 bytes)
PC DOS is resident in the high memory area.
```

Figure 58. The Used and Free Memory Map after Loading TCP/IP Drivers

As illustrated in Figure 58, this driver uses all available extended memory in our system. There is little room to use TCP/IP applications on Windows because our system memory is tight. However, some TCP/IP application tests have been done successfully with PC/DOS. Please refer to the *Installation Guide of TCP/IP for DOS* for more details.

C.3.4 DOS LAN Requester

The NetBIOS protocol is already available because DXME0MOD.SYS has been installed in the memory and bound to the driver successfully. If you intend to use applications that access a NetBIOS API directly, a fair amount of memory still remains (shown as Figure 57 on page 122). However, if you use the DOS LAN Requester, two drivers would be additionally loaded. One is NET and its size is 4336 bytes. Another is REDIR40 and its size is 76544 bytes (DOS LAN Requester Version 3.0). Both of these install themselves in conventional lower memory.

The used and free memory will be changed as follows:

```
Memory Type        Total   =   Used   +   Free
----------------  --------   --------   --------
Conventional        640 KB     263 KB     377 KB
Upper                59 KB      53 KB       5 KB
Reserved            192 KB     192 KB       0 KB
Extended (XMS)    3,205 KB   1,241 KB   1,964 KB
----------------  -------    -------    -------
Total memory      4,096 KB   1,750 KB   2,346 KB

Total under 1 MB    699 KB     317 KB     382 KB

Largest executable program size        386 KB (385,200 bytes)
Largest free upper memory block          5 KB   (5,376 bytes)
PC DOS is resident in the high memory area.
```

Figure 59. The Used and Free Memory Map after Loading Requester Drivers

C.3.5 Other NDIS Network Drivers

In the case of using other network NDIS drivers provided by IBM or Non-IBM, the memory problem still remains. Be sure to read the individual installation guide and check the required memory.

C.3.6 The Present Limitations

Minimizing memory usage is always a struggle. There is seldom, if ever, a solution that will work in every circumstance. The configurations shown in our scenarios may or may not be applicable in your circumstances. When using DOS, it may not be practical to bind several different network protocols to the wireless driver and to use different applications at the same time. Each adapter has varying memory requirements and depending on which adapter is in use will determine the total memory available to applications.

We found that typical network protocols could install and bind to the IBM Wireless LAN driver successfully. Depending on the combination, different network applications could connect with a host or server concurrently. However, while it is possible to run multiple protocols, some wireless transmission overhead may cause unacceptable levels of performance (due primarily to retransmissions of ′chatty′ protocols, such as IPX or NetBIOS). If your circumstances require the use of IBM Wireless LAN with several network protocol stacks on DOS be sure to test and understand the limitations of memory utilization and performance prior to implementation in a production environment.

C.4 Using the DOS Menu Function

This technique involves using a function of PC/DOS 6.3 or higher. Beginning with this release DOS allows the use of multiple, selectable boot files upon startup of a personal computer. If it is desirable to have multiple protocols on a DOS system, it might be acceptable to run different environments on an as-needed basis. Thus, one might boot with files to support TCP/IP, or IPX, NetBIOS, SNA and so forth.

Below is sample code to use as a template for coding such a menu system. The selection menu screen shown in Figure 62 on page 126 will appear before the workstation loads any configuration files. The user can select the appropriate environment and thus avoid loading more drivers than is necessary. The manual *PC DOS 6.3 Installation and Operation Guide* describes this facility in more detail.

C.4.1 Sample CONFIG.SYS File

```
[MENU]
MENUITEM=TCPIP, TCP/IP Applications
MENUITEM=PC3270, PC/3270 for Windows
MENUITEM=LANREQ, Dos LAN Requester
MENUCOLOR=7,1
MENUDEFAULT=TCPIP,20

[COMMON]
FILES=50
BUFFERS=30
STACKS=9,256
DOS=HIGH,UMB
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\dos\EMM386.EXE NOEMS ram X=C000-CFFF
DEVICEHIGH=C:\THINKPAD\IBMDSS01.SYS /S0=2
DEVICE=C:\THINKPAD\IBMDOSCS.SYS
DEVICE=C:\THINKPAD\DICRMU01.SYS /MA=C000-CFFF
DEVICEHIGH=C:\THINKPAD\$ICPMDOS.SYS
DEVICEHIGH=C:\THINKPAD\AUTODRV.SYS C:\THINKPAD\AUTODRV.INI
DEVICE=C:\DOS\POWER.EXE
SHELL=C:\COMMAND.COM /E:512 /P
LASTDRIVE=Z
DEVICEHIGH=C:\DOS\ANSI.SYS
DEVICEHIGH=C:\TCPDOS\BIN\PROTMAN.DOS /I:C:\TCPDOS\ETC
DEVICE=C:\TCPDOS\BIN\IBMWL.DOS

[TCPIP]
DEVICEHIGH= C:\TCPDOS\BIN\DOSTCP.SYS

[PC3270]
DEVICEHIGH=C:\LSP\DXMA0MOD.SYS 001
DEVICEHIGH=C:\LSP\DXME0MOD.SYS

[LANREQ]
DEVICEHIGH=C:\LSP\DXMA0MOD.SYS 001
DEVICEHIGH=C:\LSP\DXME0MOD.SYS
DEVICEHIGH=C:\LSP\DXMT0MOD.SYS  ES=1 EST=1 C=16 N=16 O=N TC=8 T1=9
 T2=10 TI=10
```

Figure 60. The CONFIG.SYS File for Enabling Menu Function

C.4.2 Sample AUTOEXEC.BAT File

```
@ECHO OFF
\LSP\NETBIND
PROMPT $p$g
PATH=C:\DOS;C:\THINKPAD;C:\WINDOWS;C:\TCPDOS\BIN;C:\DOSLAN;C:\WIRELESS;
LH C:\WINDOWS\SMARTDRV.EXE
LH DOSKEY
SET ETC=C:\TCPDOS\ETC
SET TEMP=C:\DOS

IF "%CONFIG%" == "TCPIP" GOTO TCPIP
IF "%CONFIG%" == "LANREQ" GOTO LANREQ
GOTO EXIT

:TCPIP
CALL TCPSTART
GOTO EXIT

:LANREQ
CALL NET START
CALL INITFSI
GOTO EXIT

:EXIT
VER
```

Figure 61. The AUTOEXEC.BAT File for Enabling Menu Function

C.4.3 Main Menu Panel

```
PC DOS 6.3 Setup Menu
=====================

  1. TCP/IP Applications
  2. PC/3270 for Windows
  3. DOS LAN Requester

Enter a choice: 1      Time remaining: 20









F5=Bypass startup files F8=Confirm each line of CONFIG.SYS and AUTOEXEC.BAT [N]
```

Figure 62. PC DOS 6.3 Setup Menu Panel

C.5 IBM Wireless LAN System Files

C.6 OS/2 Wired Stand-Alone Cell with Bridge

C.6.1 CONFIG.SYS for OS/2 Base Station

This CONFIG.SYS file is for the OS/2 Base station in Table 9 on page 86.

```
IFS=C:\OS2\HPFS.IFS /CACHE:512 /CRECL:4 /AUTOCHECK:D
PROTSHELL=C:\OS2\PMSHELL.EXE
SET USER_INI=C:\OS2\OS2.INI
SET SYSTEM_INI=C:\OS2\OS2SYS.INI
SET OS2_SHELL=C:\OS2\CMD.EXE
SET AUTOSTART=PROGRAMS,TASKLIST,FOLDERS,CONNECTIONS,LAUNCHPAD
SET RUNWORKPLACE=C:\OS2\PMSHELL.EXE
SET COMSPEC=C:\OS2\CMD.EXE
LIBPATH=%PATH%;
SET PATH=%PATH%;C:\WIRELESS;
SET DPATH=%PATH%;
SET PROMPT=$i[$p]
SET HELP=%PATH%;
SET GLOSSARY=C:\OS2\HELP\GLOSS;
SET IPF_KEYS=SBCS
PRIORITY_DISK_IO=YES
FILES=20
BASEDEV=IBMKBD.SYS
DEVICE=C:\IBMCOM\PROTOCOL\LANPDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANVDD.OS2
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
DEVICE=C:\OS2\BOOT\TESTCFG.SYS
DEVICE=C:\OS2\BOOT\DOS.SYS
DEVICE=C:\OS2\BOOT\PMDD.SYS
BUFFERS=90
IOPL=YES
DISKCACHE=D,LW,AC:C
MAXWAIT=3
MEMMAN=SWAP,PROTECT
SWAPPATH=C:\OS2\SYSTEM 2048 4096
BREAK=OFF
THREADS=256
PRINTMONBUFSIZE=134,134,134
COUNTRY=001,C:\OS2\SYSTEM\COUNTRY.SYS
SET KEYS=ON
SET BOOKSHELF=C:\OS2\BOOK;
DELDIR=C:\DELETE,512;D:\DELETE,512;
BASEDEV=PRINT02.SYS
BASEDEV=IBM2FLPY.ADD
BASEDEV=IBM1FLPY.ADD
BASEDEV=IBM2SCSI.ADD /LED
BASEDEV=XDFLOPPY.FLT
BASEDEV=OS2DASD.DMD
SET EPMPATH=C:\OS2\APPS;
PROTECTONLY=NO
SHELL=C:\OS2\MDOS\COMMAND.COM C:\OS2\MDOS
FCBS=16,8
RMSIZE=640
BASEDEV=OS2SCSI.DMD
DEVICE=C:\OS2\BOOT\POINTDD.SYS
DEVICE=C:\OS2\BOOT\MOUSE.SYS
DEVICE=C:\OS2\BOOT\COM.SYS
CODEPAGE=437,850
```

Figure 63 (Part 1 of 2). The CONFIG.SYS File for OS/2 Base Station ITSOBS01

```
DEVINFO=KBD,US,C:\OS2\KEYBOARD.DCP
DEVINFO=SCR,VGA,C:\OS2\BOOT\VIOTBL.DCP
SET VIDEO_DEVICES=VIO_VGA
SET VIO_VGA=DEVICE(BVHVGA)
DEVICE=C:\OS2\MDOS\VVGA.SYS
RUN=C:\IBMCOM\PROTOCOL\NETBIND.EXE
RUN=C:\IBMCOM\LANMSGEX.EXE
DEVICE=C:\IBMCOM\PROTOCOL\LANDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDLLDD.OS2
DEVICE=C:\IBMCOM\MACS\IBMTOK.OS2
RUN=C:\IBMCOM\PROTOCOL\LANDLL.EXE
DEVICE=C:\IBMCOM\PROTOCOL\GSDSRB.200
DEVICE=C:\IBMCOM\MACS\IBMWLB.OS2
```

Figure 63 (Part 2 of 2). The CONFIG.SYS File for OS/2 Base Station ITSOBS01

C.6.2 PROTOCOL.INI for OS/2 Base Station

This PROTOCOL.INI file is for the OS/2 base station in Table 9 on page 86.

```
[PROT_MAN]
   DRIVERNAME = PROTMAN$

[IBMLXCFG]
   GSDSRB_nif = GSDSRB.NIF
   LANDD_nif = LANDD.NIF
   IBMTOK_nif = IBMTOK.nif
   IBMWLB_nif = IBMWLB.nif

[GSDSRB_nif]
   DriverName = GSDSRB$
   Bindings = IBMTOK_nif,IBMWLB_nif
   RING = 0x582,0x789
   LINESPEED = 2048000,2048000
   BRIDGENUM = 1
   PRIORITY = 32768
   MSDU = 4472
   MAXAGE = 20
   HELLOTIME = 2

[LANDD_nif]
   DriverName = LANDD$
   Bindings = IBMTOK_nif,IBMWLB_nif
   ETHERAND_TYPE = "I","I"
   SYSTEM_KEY = 0x0,0x0
   OPEN_OPTIONS = 0x2000,0x2000
   TRACE = 0x0,0x0
   LINKS = 8,8
   MAX_SAPS = 3,3
   MAX_G_SAPS = 0,0
   USERS = 3,3
   TI_TICK_G1 = 255,255
   T1_TICK_G1 = 15,15
   T2_TICK_G1 = 3,3
   TI_TICK_G2 = 255,255
   T1_TICK_G2 = 25,25
   T2_TICK_G2 = 10,10
   IPACKETS = 250,250
   UIPACKETS = 100,100
   MAXTRANSMITS = 6,6
   MINTRANSMITS = 2,2
   TCBS = 64,64
   GDTS = 30,30
   ELEMENTS = 800,800

[IBMTOK_nif]
   DriverName = IBMTOK$
   ADAPTER = "PRIMARY"
   NETADDRESS "400090002000"
   MAXTRANSMITS = 6
   RECVBUFS = 20
   RECVBUFSIZE = 256
   XMITBUFS = 1
   XMITBUFSIZE = 4456
   ENABLEBRIDGE
   BRIDGERAM = 5296

[IBMWLB_nif]
   DriverName = IBMWL$
   ENABLEBRIDGE = "YES"
   BUFFERSIZE = 256
   NETADDRESS = "400090002002"
```

Figure 64. The PROTOCOL.INI File for OS/2 Base Station ITSOBS01

C.6.3 LANTRAN.LOG for OS/2 Base Station

This LANTRAN.LOG file is for the OS/2 base station in Table 9 on page 86.

```
IBM OS/2 LANMSGDD [04/13/94] 2.01 is loaded and operational.
IBM OS/2 LAN Protocol Manager
IBM OS/2 LANDD [04/13/94] 2.20.12
IBM OS/2 LANDLLDD 2.01
IBM OS/2 LANDLLDD is loaded and operational.
IBM - IBM Token-Ring Network Driver, Version V.2.02
IBM - GSD Source Route Bridge V 1.0 21:51:09, Mar  1 1995
IBM - IBM Wireless Network Driver, Version V.1.01
IBM LANVDD is loaded and operational.
IBM OS/2 LAN Netbind
IBM Token-Ring adapter data rate is 4 mbps.
IBM LANDD is accessing IBM 802.5 LAN Interface.
Adapter 0 was initialized and opened successfully.
Adapter 0 is using node address 400090002000
IBM LANDD was successfully bound to MAC: IBMTOK_nif.
IBM LANDD is accessing IBM 802.5 LAN Interface.
Adapter 1 was initialized and opened successfully.
Adapter 1 is using node address 400090002002.
IBM LANDD was successfully bound to MAC: IBMWLB_nif.
Binding MAC: [IBMTOK_NIFB] as Port #1
Binding MAC: [IBMWLB_NIFB] as Port #2
Wireless adapter successfully open.
Spanning Tree Bridge 8000400090002000 Port 01 Lan 0582 Node 400090002000 started
Spanning Tree Bridge 8000400090002000 Port 02 Lan 0789 Node 400090002002 started
Port #1 starting bridge operation
Port #2 starting bridge operation
```

Figure 65. The LANTRAN.LOG File for OS/2 Base Station ITSOBS01

C.6.4 CONFIG.SYS for OS/2 Wireless Workstation

This CONFIG.SYS file is for the OS/2 wireless workstation in Table 9 on page 86.

```
IFS=C:\OS2\HPFS.IFS /CACHE:64 /CRECL:4
PROTSHELL=C:\OS2\PMSHELL.EXE
SET USER_INI=C:\OS2\OS2.INI
SET SYSTEM_INI=C:\OS2\OS2SYS.INI
SET OS2_SHELL=C:\OS2\CMD.EXE
SET AUTOSTART=PROGRAMS,TASKLIST,FOLDERS,CONNECTIONS,LAUNCHPAD
SET RUNWORKPLACE=C:\OS2\PMSHELL.EXE
SET COMSPEC=C:\OS2\CMD.EXE
LIBPATH=%PATH%;
SET PATH=%PATH%;C:\WIRELESS
SET DPATH=%PATH%;
SET PROMPT=$i[$p]
SET HELP=%PATH%;
SET GLOSSARY=C:\OS2\HELP\GLOSS;
SET IPF_KEYS=SBCS
PRIORITY_DISK_IO=YES
FILES=20
BASEDEV=IBMKBD.SYS
DEVICE=C:\IBMCOM\PROTOCOL\LANPDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANVDD.OS2
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
DEVICE=C:\OS2\BOOT\TESTCFG.SYS
DEVICE=C:\OS2\BOOT\DOS.SYS
DEVICE=C:\OS2\BOOT\PMDD.SYS
BUFFERS=90
IOPL=YES
DISKCACHE=D,LW,AC:C
MAXWAIT=3
MEMMAN=SWAP,PROTECT
SWAPPATH=C:\OS2\SYSTEM 2048 8192
BREAK=OFF
THREADS=256
PRINTMONBUFSIZE=134,134,134
COUNTRY=001,C:\OS2\SYSTEM\COUNTRY.SYS
SET KEYS=ON
SET BOOKSHELF=%PATH%
SOMIROMIR=C:-OS2-ETC-SOM.IR;C:-OS2-ETC-WPSH.IR;C:-OS2-ETC-WPDSERV.IR
SET SOMDDIR=C:-OS2-ETC-DSOM
BASEDEV=PRINT01.SYS
BASEDEV=IBM1FLPY.ADD
BASEDEV=IBM2FLPY.ADD
BASEDEV=IBM1S506.ADD
BASEDEV=XDFLOPPY.FLT
BASEDEV=OS2DASD.DMD
SET EPMPATH=C:\OS2\APPS;
PROTECTONLY=NO
SHELL=C:\OS2\MDOS\COMMAND.COM
C:\OS2\MDOS
FCBS=16,8
RMSIZE=640
DEVICE=C:\OS2\MDOS\VEMM.SYS
DOS=LOW,NOUMB
DEVICE=C:\OS2\MDOS\VXMS.SYS /UMB DEVICE=C:\OS2\MDOS\VDPMI.SYS
DEVICE=C:\OS2\MDOS\VDPX.SYS
DEVICE=C:\OS2\MDOS\VWIN.SYS
DEVICE=C:\OS2\MDOS\VW32S.SYS
DEVICE=C:\OS2\MDOS\VMOUSE.SYS DEVICE=C:\OS2\BOOT\POINTDD.SYS
DEVICE=C:\OS2\BOOT\MOUSE.SYS
CODEPAGE=437,850
```

Figure 66 (Part 1 of 2). The CONFIG.SYS File for OS/2 Wireless Workstation RSSAYA

```
DEVINFO=KBD,US,C:\OS2\KEYBOARD.DCP
BASEDEV=PCMCIA.SYS /P
DEVICE=C:\OS2\MDOS\VPCMCIA.SYS
DEVICE=C:\OS2\BOOT\COM.SYS
DEVICE=C:\OS2\MDOS\VCOM.SYS
BASEDEV=IBM2SSO1.SYS /s0=4
BASEDEV=XGA.SYS
DEVICE=C:\OS2\BOOT\XGARINGO.SYS
DEVINFO=SCR,VGA,C:\OS2\BOOT\VIOTBL.DCP
SET VIDEO_DEVICES=VIO_XGA
SET VIO_XGA=DEVICE(BVHVGA,BVHXGA)
DEVICE=C:\OS2\MDOS\VVGA.SYS
DEVICE=C:\OS2\MDOS\VXGA.SYS
SET MMBASE=C:\MMOS2;
SET DSPPATH=C:\MMOS2\DSP;
SET NCDEBUG=4000
DEVICE=C:\MMOS2\SSMDD.SYS
DEVICE=C:\MMOS2\ROSTUB.SYS
SET ETC=C:\TCPIP\ETC
SET TMP=C:\TCPIP\TMP
SET READIBM=C:\TCPIP\DOC
SET HOSTNAME=SAYA
RUN=C:\TCPIP\BIN\CNTRL.EXE
RUN=C:\IBMCOM\PROTOCOL\NETBIND.EXE
RUN=C:\IBMCOM\LANMSGEX.EXE
DEVICE=C:\IBMCOM\PROTOCOL\INET.SYS
DEVICE=C:\IBMCOM\PROTOCOL\IFNDIS.SYS
DEVICE=C:\IBMCOM\PROTOCOL\NETBEUI.OS2
DEVICE=C:\IBMLAN\NETOROG\RDRHELP.200
IFS=C:\IBMLAN\NETOROG\NETWKSTA.200 /I:C:\IBMLAN /N
DEVICE=C:\IBMCOM\PROTOCOL\NETBIOS.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDLLDD.OS2
DEVICE=C:\IBMCOM\MACS\IBMWLO.OS2
RUN=C:\IBMCOM\PROTOCOL\LANDLL.EXE
RUN=C:\IBMLAN\NETPROG\LSDAEMON.EXE
DEVICE=C:\CMLIB\ACSLANDD.SYS
DEVICE=C:\CMLIB\CMKFMDE.SYS
SET CMPATH=C:\CMLIB
DEVICE=C:\OS2\LOG.SYS
RUN=C:\OS2\SYSTEM\LOGDAEM.EXE
DEVICE=C:\OS2\EPWDD.SYS
RUN=C:\OS2\EPWDDR3.EXE
RUN=C:\OS2\EPWROUT.EXE 1
RUN=C:\OS2\EPW.EXE
```

Figure 66 (Part 2 of 2). The CONFIG.SYS File for OS/2 Wireless Workstation RSSAYA

C.6.5 PROTOCOL.INI for OS/2 Wireless Workstation

This PROTOCOL.INI file is for the OS/2 wireless workstation in Table 9 on page 86.

```
[PROT_MAN]
   DRIVERNAME = PROTMAN$

[IBMLXCFG]
   LANDD_nif = LANDD.NIF
   NETBEUI_nif = NETBEUI.NIF
   TCPIP_nif = TCPIP.NIF
   IBMWLO_nif = IBMWLO.nif

[LANDD_nif]
   DriverName = LANDD$
   Bindings = IBMWLO_nif
   ETHERAND_TYPE = "I"
   SYSTEM_KEY = 0x0
   OPEN_OPTIONS = 0x2000
   TRACE = 0x0
   LINKS = 8
   MAX_SAPS = 3
   MAX_G_SAPS = 0
   USERS = 3
   TI_TICK_G1 = 255
   T1_TICK_G1 = 15
   T2_TICK_G1 = 3
   TI_TICK_G2 = 255
   T1_TICK_G2 = 25
   T2_TICK_G2 = 10
   IPACKETS = 250
   UIPACKETS = 100
   MAXTRANSMITS = 6
   MINTRANSMITS = 2
   TCBS = 64
   GDTS = 30
   ELEMENTS = 800
[NETBEUI_nif]

   DriverName = netbeui$
   Bindings = IBMWLO_nif
   ETHERAND_TYPE = "I"
   USEADDRREV = "YES"
   OS2TRACEMASK = 0x0
   SESSIONS = 40
   NCBS = 95
   NAMES = 21
   SELECTORS = 5
   USEMAXDATAGRAM = "NO"
   ADAPTRATE = 1000
   WINDOWERRORS = 0
   MAXDATARCV = 4168
   TI = 30000
   T1 = 4000
   T2 = 2000
   MAXIN = 1
   MAXOUT = 1
   NETBIOSTIMEOUT = 500
   NETBIOSRETRIES = 8
   NAMECACHE = 0
   PIGGYBACKACKS = 1
   DATAGRAMPACKETS = 2
   PACKETS = 350
   LOOPPACKETS = 1
   PIPELINE = 5
   MAXTRANSMITS = 6
   MINTRANSMITS = 2
   DLCRETRIES = 8
   FCPRIORITY = 5
   NETFLAGS = 0x0
```

Figure 67 (Part 1 of 2). The PROTOCOL.INI File for OS/2 Wireless Workstation RSSAYA

```
[TCPIP_nif]
   DriverName = TCPIP$
   Bindings = IBMWLO_nif

[IBMWLO_nif]
   DriverName = IBMWL$
   NetWorkId = "ITSO01"
   StationName = "RSSAYA"
   CountryCode = 1
   Compression = "YES"
   DataMasking = "none"
   NETADDRESS = "400000009533"
```

Figure 67 (Part 2 of 2). The PROTOCOL.INI File for OS/2 Wireless Workstation RSSAYA

C.6.6 PROTOCOL.INI for DOS Wireless Workstation

This PROTOCOL.INI file is for the OS/2 wireless workstation in Table 9 on page 86.

```
[PROTMAN]
DriverName=PROTMAN$

[DXMAIDXCFG]
        DXMEO_NIF = DXMEO.NIF
        DXMJOMOD_NIF = DXMJOMOD.NIF
        IBMWL_NIF = IBMWL.NIF
        IBMWL2_NIF = IBMWL.NIF
[TCPIP_V21]
DriverName=DOSNDIS$
Bindings=IBMWL_NIF,,,

[DXMEO_NIF]
        DriverName = DXMEO$
        Bindings = IBMWL_NIF

[IBMWL_NIF]
        DriverName = IBMWL$
        NETWORKID = "ITSO01"
        STATIONNAME = "RSYURI"
        COUNTRYCODE = 1
        COMPRESSION = "YES"
        DATAMASKING = "NONE"
        NETADDRESS = "40000003750C"
```

Figure 68. The PROTOCOL.INI File for DOS Wireless Workstation RSYURI

C.7 OS/2 Wired LAN Cell with IP Routing

C.7.1 PROTOCOL.INI for OS/2 Base Station

This PROTOCOL.INI file is for the OS/2 base station in Table 13 on page 90.

```
[PROT_MAN]
   DRIVERNAME = PROTMAN$

[IBMLXCFG]
   LANDD_nif = LANDD.NIF
   TCPIP_nif = TCPIP.NIF
   IBMTOK_nif = IBMTOK.nif
   IBMWLS_nif = IBMWLS.nif

[LANDD_nif]
   DriverName = LANDD$
   Bindings = IBMTOK_nif,IBMWLS_nif
   NETADDRESS = "t400090001000",
   ETHERAND_TYPE = "I","I"
   SYSTEM_KEY = 0x0,0x0
   OPEN_OPTIONS = 0x2000,0x2000
   TRACE = 0x0,0x0
   LINKS = 8,8
   MAX_SAPS = 3,3
   MAX_G_SAPS = 0,0
   USERS = 3,3
   TI_TICK_G1 = 255,255
   T1_TICK_G1 = 15,15
   T2_TICK_G1 = 3,3
   TI_TICK_G2 = 255,255
   T1_TICK_G2 = 25,25
   T2_TICK_G2 = 10,10
   IPACKETS = 250,250
   UIPACKETS = 100,100
   MAXTRANSMITS = 6,6
   MINTRANSMITS = 2,2
   TCBS = 64,64
   GDTS = 30,30
   ELEMENTS = 800,800

[TCPIP_nif]
   DriverName = TCPIP$
   Bindings = IBMTOK_nif,IBMWLS_nif

[IBMTOK_nif]
   DriverName = IBMTOK$
   ADAPTER = "PRIMARY"
   NETADDRESS = "400090001000"
   MAXTRANSMITS = 6
   RECVBUFS = 20
   RECVBUFSIZE = 256
   XMITBUFS = 1
   XMITBUFSIZE = 4456

[IBMWLS_nif]
   DriverName = IBMWL$
   NETADDRESS = "400090001001"
```

Figure 69. The PROTOCOL.INI File for OS/2 Base Station ITSOBS02

C.8 NetWare Wired LAN Cell with IPX Routing

C.8.1 IBMWL.NCF for NetWare Base Station

This IBMWL.NCF file is for NetWare base station in Table 15 on page 92.

```
# ---------------------- IBM Wireless LAN Begin Statements ------------------
LOAD IBMWLCOM CONFIG=NSBS
LOAD IBMWLERL
LOAD IBMWL FRAME=Token-Ring NAME=IBMWL_TOKEN
LOAD IBMWL FRAME=Token-Ring_SNAP NAME=IBMWL_TOKEN_SNAP
LOAD IBMWLWCA
LOAD IBMWLWNC
BIND IPX TO IBMWL_TOKEN NET=76B9O6DC
BIND WLNM TO IBMWL_TOKEN_SNAP
BIND WLNC TO IBMWL_TOKEN_SNAP
LOAD IBMWLNAP
# ---------------------- IBM Wireless LAN End Statements --------------------
```

Figure 70. The IBMNET.NCF File for NetWare Base Station ITSOBS03

C.8.2 CONFIG.SYS for OS/2 Wireless Workstation

This CONFIG.SYS file is for the OS/2 wireless workstation in Table 15 on page 92.

```
IFS=C:\OS2\HPFS.IFS /CACHE:64 /CRECL:4
PROTSHELL=C:\OS2\PMSHELL.EXE
SET USER_INI=C:\OS2\OS2.INI
SET SYSTEM_INI=C:\OS2\OS2SYS.INI
SET OS2_SHELL=C:\OS2\CMD.EXE
SET AUTOSTART=PROGRAMS,TASKLIST,FOLDERS,CONNECTIONS,LAUNCHPAD
SET RUNWORKPLACE=C:\OS2\PMSHELL.EXE
SET COMSPEC=C:\OS2\CMD.EXE
LIBPATH=%PATH%;
SET PATH=%PATH%;C:\WIRELESS
SET DPATH=%PATH%;
SET PROMPT=$i[$p]
SET HELP=%PATH%;
SET GLOSSARY=C:\OS2\HELP\GLOSS;
SET IPF_KEYS=SBCS
PRIORITY_DISK_IO=YES
FILES=20
BASEDEV=IBMKBD.SYS
DEVICE=C:\OS2\BOOT\TESTCFG.SYS
DEVICE=C:\OS2\BOOT\DOS.SYS
DEVICE=C:\OS2\BOOT\PMDD.SYS
BUFFERS=90
IOPL=YES
DISKCACHE=D,LW,AC:C
MAXWAIT=3
MEMMAN=SWAP,PROTECT
SWAPPATH=C:\OS2\SYSTEM 2048 4096
BREAK=OFF
THREADS=256
PRINTMONBUFSIZE=134,134,134
COUNTRY=001,C:\OS2\SYSTEM\COUNTRY.SYS
SET KEYS=ON
SET BOOKSHELF=C:\OS2\BOOK;
SET SOMIR=C:\OS2\ETC\SOM.IR;C:\OS2\ETC\WPSH.IR;C:\OS2\ETC\WPDSERV.IR
SET SOMDDIR=C:\OS2\ETC\DSOM
REM SET DELDIR=C:\DELETE,512;
BASEDEV=PRINT02.SYS
BASEDEV=IBM2FLPY.ADD
BASEDEV=IBM1FLPY.ADD
BASEDEV=IBM2SCSI.ADD /LED
BASEDEV=XDFLOPPY.FLT
BASEDEV=OS2DASD.DMD
SET EPMPATH=C:\OS2\APPS;
PROTECTONLY=NO
SHELL=C:\OS2\MDOS\COMMAND.COM C:\OS2\MDOS
FCBS=16,8
RMSIZE=640
rem DEVICE=C:\NETWARE\VIPX.SYS
rem DEVICE=C:\NETWARE\VSHELL.SYS PRIVATE
DEVICE=C:\OS2\MDOS\VEMM.SYS
DOS=LOW,NOUMB
DEVICE=C:\OS2\MDOS\VXMS.SYS /UMB
DEVICE=C:\OS2\MDOS\VDPMI.SYS
DEVICE=C:\OS2\MDOS\VDPX.SYS
BASEDEV=OS2SCSI.DMD
DEVICE=C:\OS2\MDOS\VMOUSE.SYS
DEVICE=C:\OS2\BOOT\POINTDD.SYS
DEVICE=C:\OS2\BOOT\MOUSE.SYS
DEVICE=C:\OS2\BOOT\COM.SYS
DEVICE=C:\OS2\MDOS\VCOM.SYS
CODEPAGE=437,850
DEVINFO=KBD,US,C:\OS2\KEYBOARD.DCP
DEVINFO=SCR,VGA,C:\OS2\BOOT\VIOTBL.DCP
SET VIDEO_DEVICES=VIO_VGA
SET VIO_VGA=DEVICE(BVHVGA)
DEVICE=C:\OS2\MDOS\VVGA.SYS
```

Figure 71 (Part 1 of 2). The CONFIG.SYS File for OS/2 Wireless Workstation RSSAYA

```
REM --- NetWare Requester statements BEGIN ---
SET NWLANGUAGE=ENGLISH
DEVICE=C:\NETWARE\LSL.SYS
RUN=C:\NETWARE\DDAEMON.EXE
REM -- ODI-Driver Files BEGIN --
DEVICE=C:\WLESSNET\IBMWL.SYS
REM -- ODI-Driver Files END --
REM DEVICE=C:\NETWARE\ROUTE.SYS
DEVICE=C:\NETWARE\IPX.SYS
DEVICE=C:\NETWARE\SPX.SYS
RUN=C:\NETWARE\SPDAEMON.EXE
rem DEVICE=C:\NETWARE\NMPIPE.SYS
rem DEVICE=C:\NETWARE\NPSERVER.SYS
rem RUN=C:\NETWARE\NPDAEMON.EXE
DEVICE=C:\NETWARE\NWREQ.SYS
IFS=C:\NETWARE\NWIFS.IFS
RUN=C:\NETWARE\NWDAEMON.EXE
DEVICE=C:\NETWARE\NETBIOS.SYS
RUN=C:\NETWARE\NBDAEMON.EXE
REM DEVICE=C:\OS2\MDOS\LPTDD.SYS
REM --- NetWare Requester statements END ---
```

Figure 71 (Part 2 of 2). The CONFIG.SYS File for OS/2 Wireless Workstation RSSAYA

C.8.3 NET.CFG for OS/2 Wireless Workstation

This NET.CFG file is for the OS/2 wireless workstation in Table 15 on page 92.

```
Link support
  buffers 15 4210

link driver ibmwl
  NODE ADDRESS 400000008565
  network_id ITSO03
  country_code 1 3 0 81 3
  station_name RSSAYA
  encoded_name 0000000000000000000
  compression yes
  data_masking none
```

Figure 72. The NET.CFG File for OS/2 Wireless Workstation RSSAYA

C.8.4 NET.CFG for DOS Wireless Workstation

This NET.CFG file is for the DOS wireless workstation in Table 15 on page 92.

```
link driver ibmwl
  enabler C:\WIRELESS\IBMWLENA.EXE

  NODE ADDRESS 40000003750C
  network_id ITSO03
  country_code 1 3 0 81 3
  station_name RSYURI
  encoded_name
  compression yes
  data_masking none
```

Figure 73. The NET.CFG File for the DOS Wireless Workstation RSYURI

List of Abbreviations

AM	Amplitude Modulation
AMTS	Advanced Mobile Telephone System
ARAT	Address Range Authorization Table
ASAT	Address Specific Authorization Table
CDMA	Code Division Multiple Access
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DAMPS	Digital Advanced Mobile Telephone System
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FM	Frequency Modulation
FTP	File Transfer Protocol
GSM	Global System for Mobile communication
Hz	Hertz
IBM	International Business Machines Corporation
ISA	Industry Standard Architecture
ITSO	International Technical Support Organization
JDC	Japan Digital Cellular
LAA	Locally Administered Address
LLC	Logical Link Control
MAC	Media Access Control
MCA	Micro Channel Architecture
NAP	Network Administrator Program
NMT	Nordic Mobile Telephone
PCMCIA	Personal Computer Memory Card International Association
PROFS	Professional Office System
PSTN	Public Switched Telephone Network
RPL	Remote Program Load
RSSI	Remote Signal Strength Indicator
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
TACS	Total Access Control System
TDMA	Time Division Multiple Access
TCP/IP	Transmission Control Protocol/Internet Protocol
UAA	Universally Administered Address
WCA	Wireless Control Agent
WNC	Wireless Network Controller
WnetID	Wireless network IDentifier

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

ITSO Technical Bulletin Evaluation RED000

International Technical Support Organization
Wireless LAN Communications
January 1996

Publication No. SG24-4466-00

Your feedback is very important to help us maintain the quality of ITSO Bulletins. **Please fill out this questionnaire and return it using one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246
- Send a note to REDBOOK@VNET.IBM.COM

Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction	____		
Organization of the book	____	Grammar/punctuation/spelling	____
Accuracy of the information	____	Ease of reading and understanding	____
Relevance of the information	____	Ease of finding information	____
Completeness of the information	____	Level of technical detail	____
Value of illustrations	____	Print quality	____

Please answer the following questions:

a) If you are an employee of IBM or its subsidiaries:

Do you provide billable services for 20% or more of your time? Yes____ No____

Are you in a Services Organization? Yes____ No____

b) Are you working in the USA? Yes____ No____

c) Was the Bulletin published in time for your needs? Yes____ No____

d) Did this Bulletin meet your needs? Yes____ No____

If no, please explain:

_____

_____

What other topics would you like to see in this Bulletin?

_____

_____

What other Technical Bulletins would you like to see published?

_____

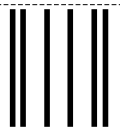
Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

_____ _____
Name Address

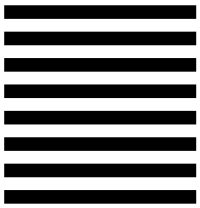
_____ _____
Company or Organization

_____ _____
Phone No.

Fold and Tape **Please do not staple** Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Organization
Department HZ8, Building 678
P.O. BOX 12195
RESEARCH TRIANGLE PARK NC
USA 27709-2195

Fold and Tape **Please do not staple** Fold and Tape

Printed in U.S.A.