

**User's
Manual**

0100 Access Point

P/N 062367-002

Intermec® Corporation
6001 36th Avenue West
P.O. Box 4280
Everett, WA 98203-9280

U.S. technical and service support: 1-800-755-5505
U.S. media supplies ordering information: 1-800-227-9947

Canadian technical and service support: 1-800-688-7043
Canadian media supplies ordering information: 1-800-268-6936

Outside U.S. and Canada: Contact your local Intermec service supplier.

The information contained herein is proprietary and is provided solely for the purpose of allowing customers to operate and/or service Intermec manufactured equipment and is not to be released, reproduced, or used for any other purpose without written permission of Intermec.

Information and specifications in this manual are subject to change without notice.

© 1995 by Intermec Corporation
All Rights Reserved

The word Intermec, the Intermec logo, JANUS, IRL, DURATHERM, Virtual Wedge, and CrossBar are trademarks of the Intermec Corporation.

Throughout this manual, trademarked names may be used. Rather than put a trademark symbol (™) in every occurrence of a trademarked name, we state that we are using the names only in an editorial fashion, and to the benefit of the trademark owner, with no intention of infringement.

Contents

***Before You Begin* vii**

Warranty Information vii

Safety Summary vii

Cautions and Notes viii

About This Manual viii

Other Related Manuals ix

1

Learning About the Access Point

***Introduction* 1-3**

***About Network Operating Systems* 1-3**

***Network Operating Systems and the RF Network* 1-5**

Simple Network 1-5

Moderately Complex Network 1-6

Roaming 1-7

***About Peer-to-Peer Network Operating Systems* 1-9**

***Peer-to-Peer and the RF Network* 1-10**

2

Installing the Access Point

***Unpacking the Access Point* 2-3**

***System Requirements* 2-4**

***Access Point LEDs* 2-4**

Access Point Reset Button 2-5

Making a Backup Copy of the Boot Disk 2-6

Performing a Quick Installation 2-6

3

Configuring the Access Point

Navigating Through the Configuration Application 3-3

Before You Run the Configuration Application 3-3

Configuring the Access Point Locally 3-4

Editing the SLIP.BAT File 3-5

Configuring the Access Point Remotely 3-6

Configuring the Access Point Using SNMP Management Packages 3-7

Starting the Configuration Application 3-10

Configuring a Local Access Point 3-10

Adding a New Remote Access Point 3-11

Editing a Remote Access Point 3-12

Deleting an Access Point 3-12

Using the Configuration Dialog Box 3-12

Configuring the Radio Parameters 3-13

Configuring the Spanning Tree Protocol Parameters 3-14

Configuring Filters 3-15

Setting the Security ID 3-17

Resetting the Access Point 3-18

4

Helpful Hints 4-3

Running Large Executable Files Efficiently 4-3

Novell's VLM Technology 4-3

Determining Master Stations and Alternate Master Stations 4-3

Microwave Ovens 4-4

Antenna Placement 4-5

Troubleshooting 4-5

A

Appendix A

Specifications A-3

How the 2.4 GHz RF Network Fits in the OSI Model A-4

Access Point as an Ethernet Segment Bridge A-5

Access Point as a One-Hop Repeater A-5

The AUTOEXEC.BAT File for the Access Point A-6

The NET.CFG File for the Access Point A-6

The CFG.CFG File for the Access Point A-8

B

Appendix B

Understanding the Radio Parameters B-3

Station Type B-3

Master Name B-4

Channel B-4

Subchannel B-4

Domain B-5

Security ID B-5

Understanding the Spanning Tree Protocol Parameters B-6

Spanning Tree Priority B-6

Bridge Max Age B-7

Bridge Hello Timer B-7

Bridge Forward Delay B-7

Aging Time B-7

RF Port Priority and Ethernet Port Priority B-8

RF Port Enabled and Ethernet Port Enabled B-8

RF Port Path Cost and Ethernet Port Path Cost B-8

G

Glossary

I

Index

Before You Begin

This section introduces you to standard warranty provisions, safety precautions, warnings and cautions, document formatting conventions, and sources of additional product information.

Warranty Information

To receive a copy of the standard warranty provision for this product, contact your local Intermec sales organization. In the U.S. call (800) 755-5505, and in Canada call (800) 688-7403. Otherwise, refer to the Worldwide Sales & Service list shipped with this manual for the address and telephone number of your Intermec sales organization.

Safety Summary

Your safety is extremely important. Read and follow all warnings and cautions in this manual before handling and operating Intermec equipment. You can be seriously injured, and equipment and data can be damaged if you do not follow the safety warnings and cautions.

Do Not Repair or Adjust Alone Do not repair or adjust energized equipment alone under any circumstances. Someone capable of providing first aid must always be present for your safety.

First Aid Always obtain first aid or medical attention immediately after an injury. Never neglect an injury, no matter how slight it seems.

Resuscitation Begin resuscitation immediately if someone is injured and stops breathing. Any delay could result in death. To work on or near high voltage, you should be familiar with approved industrial first aid methods.

Energized Equipment Never work on energized equipment unless authorized by a responsible authority. Energized electrical equipment is dangerous. Electrical shock from energized equipment can cause death. If you must perform authorized emergency work on energized equipment, be sure that you comply strictly with approved safety regulations.

Cautions and Notes

The cautions and notes in this manual use the following format.



Caution

A caution alerts you to an operating procedure, practice, condition, or statement that must be strictly observed to prevent equipment damage or destruction, or corruption or loss of data.

Conseil

Une précaution vous avertit d'une procédure de fonctionnement, d'une méthode, d'un état ou d'un rapport qui doit être strictement respecté pour empêcher l'endommagement ou la destruction de l'équipement, ou l'altération ou la perte de données.

Notes either provide extra information about a topic or contain special instructions for handling a particular condition or set of circumstances.

About This Manual

The *0100 Access Point User's Manual* provides information on what networks are, how to install the Access Point and how to configure it. To set up an Access Point, you must be familiar with your PC and your network.

Terms and Conventions

This manual uses the following conventions to emphasize keypad input, screen messages, and command syntax.

Keypad Input

Keystrokes to be entered into the PC are emphasized in **bold**. "Press **Enter**" means you press the key labeled "Enter" on your keyboard.

When you need to press and release a series of keys in order, the keys are listed in order with no connectors. "Press **Shift A**" means you press and release the Shift key, and then press A.

When you must press more than one key at the same time, the keys are connected by a dash in the text. "Press **Ctrl-Alt-Del**" means that to perform a warm boot on the PC, you need to hold down the **Ctrl**, **Alt**, and **Del** keys at the same time. When the keys are connected by a dash, you must press and hold the keys in the order they are listed in the text.



Commands

Command syntax is shown in the text as it should be entered into the PC or JANUS reader. For example, to see a listing of directories on the reader, type:

```
dir
```

If a command line includes both required and optional parameters, the required parameters are enclosed in braces { } and the optional parameters are enclosed in brackets [].

Other Related Manuals

You may need to refer to additional information when working with the Access Point in a data collection network. To order additional manuals, contact your local Intermec representative.

Intermec Manuals	Part No.
<i>0100 Access Point Mounting Bracket Instruction Sheet</i>	062475
<i>JANUS 2.4 GHz Installation Utility User's Manual</i>	062368
<i>JANUS 2020 Hand-Held Data Collection Computer User's Manual</i>	062366
<i>JANUS 2020 User's Manual Addendum</i>	062474
<i>JANUS 2020 Hardware and Documentation Roadmap</i>	059953

Other Manuals

NetWare Administrator's Guide

1

Learning About the Access Point

This chapter explains what the 0100 Access Point is and how it fits into your network operating system.

Introduction

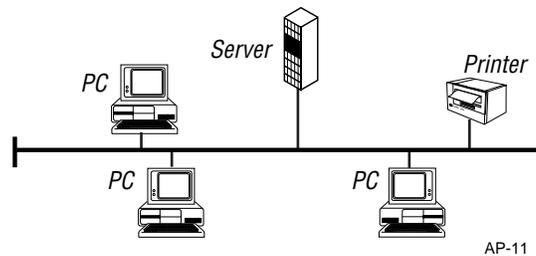
The 0100 Access Point acts as a wireless bridge for JANUS RF readers and other wireless LAN products that run in the 2.4 GHz network to communicate with your Ethernet network. It allows easy expandability of your wireless network by increasing range and facilitating mobile applications. It operates at the Data Link level (layer 2) of the OSI model, providing protocol-independent access for JANUS reader users in an existing IEEE 802.3 wired Ethernet LAN. See the Appendix for a diagram of how the Access Point fits into the OSI model.

The Access Point is designed as a “plug-and-play” product. In many cases, you will not even need to configure it. If you need to use the configuration software, it is simple to understand and has online help.

About Network Operating Systems

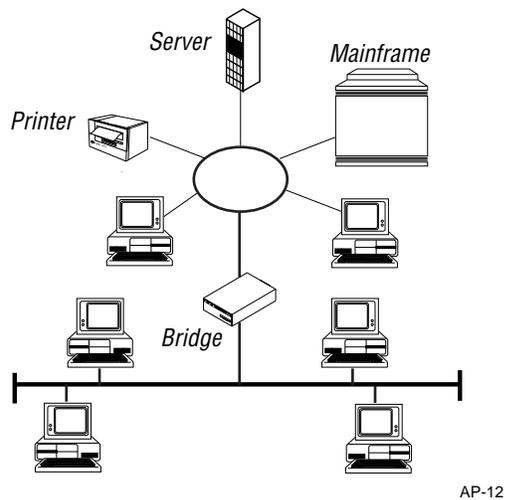
The first network operating systems provided a way for a few PCs to share files and printers connected to the same network.

A Simple Network



As the growth of personal computers proliferated throughout business environments, network operating systems expanded to provide the ability for different types of network equipment (bridges, PCs, mainframes, etc.) to operate in a wide variety of networks. Current network operating systems are an integral part of the corporate network, providing access between the smallest personal computers and the largest mainframe system.

A Moderately Complex Network



Network operating systems can be broken into three functions:

- The server is the core of the network operating system and provides memory management, the network filing system, and task scheduling.
- Network applications provide the functions of the network, such as e-mail and database capabilities.
- The client (workstation) provides the ability for the user to attach to the network and access the client-server applications or server functions.

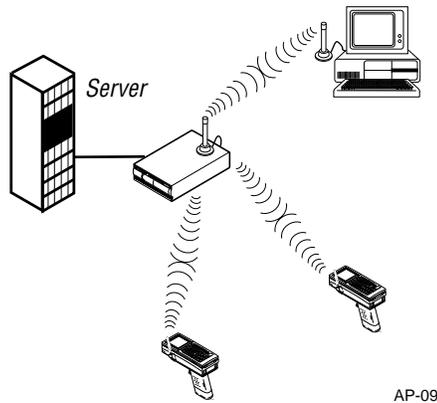
Network Operating Systems and the RF Network

Radio frequency (RF) products exist on your LAN as a standalone network or as an additional subnetwork, and operate within a variety of network operating system environments.

Simple Network

For a network with only one RF subnetwork, use the default settings for all Access Points.

A Simple Wireless Network



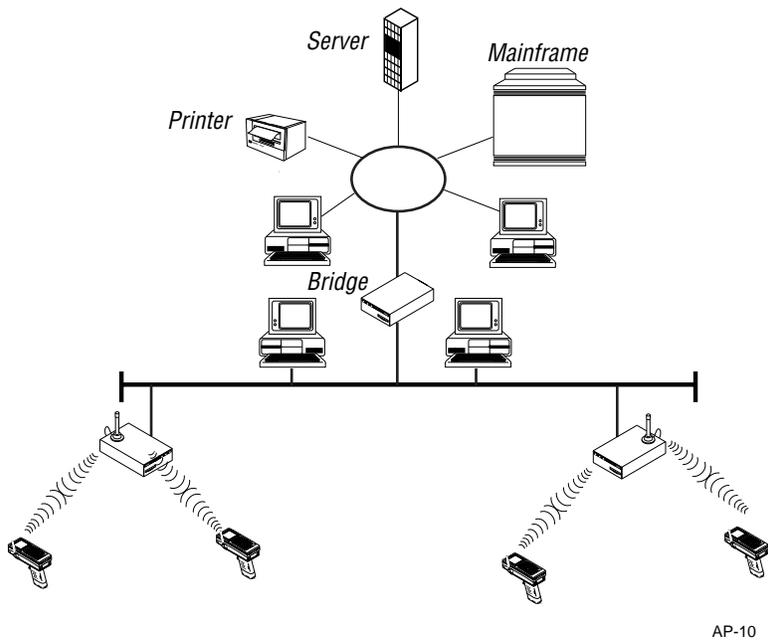
Moderately Complex Network

In a moderately complex network, you may need the additional capabilities of multiple Access Points:

- Transparent bridging, which supports all protocols.
- Spanning tree protocol support (IEEE 802.1d), which supports the IEEE standard for interoperability and dynamically reconfigures the network if a link is broken or if you add products.
- Simple Network Management Protocol (SNMP) capability, which can be managed by an SNMP management package.

If you want to establish two independent RF subnetworks, you can use different channels and domain numbers to isolate the subnetworks. Only adapters with the same domain can establish communications.

A Moderately Complex Network With Two RF Subnetworks



Roaming

With the Access Point's roaming capability, you can break the wireless distance barrier by installing them throughout your building. The Access Points act as "cells," similar in concept to those of a cellular phone network. Make sure that the coverage of each Access Point overlaps to provide uninterrupted wireless access at any location within the building.

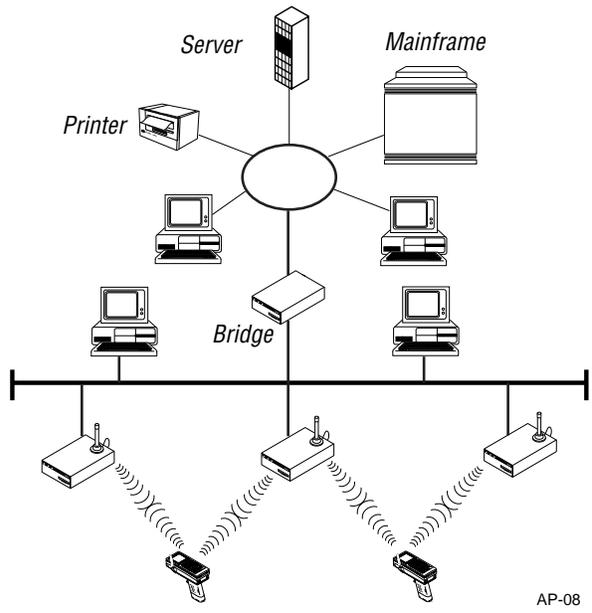
Note: The cells must overlap to ensure that there are no gaps in coverage and that the roaming JANUS reader will always have a connection available.

In a roaming network, you should configure each Access Point for a different channel/subchannel pair, but you must configure each one with the same domain number and security ID. You must also configure the JANUS readers with the same domain. These configurations ensure that the JANUS readers can switch from Access Point to Access Point while preserving wireless connectivity. When the roaming JANUS reader leaves the transmission range of one Access Point, the software automatically polls the other Access Points in the same domain to continue the network connection.

Note: Roaming stations will only roam among Access Points with the same domain and security ID.

The following illustration displays an example of a moderately complex network that has been set up with a roaming domain.

A Network With Roaming Capability

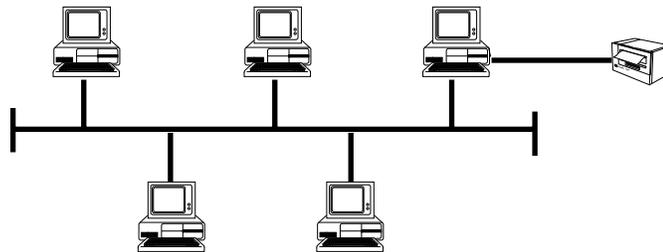


AP-08

About Peer-to-Peer Network Operating Systems

Today's network operating systems can support multiple servers and hundreds of workstations in the same LAN environment. Since, these server-based network operating systems are often too sophisticated and expensive for the needs of the small office or work group, a variety of companies developed peer-to-peer network operating systems. These new products offer affordable prices, easy installation and operation, and flexibility for future growth.

A Peer-to-Peer Network Operating System

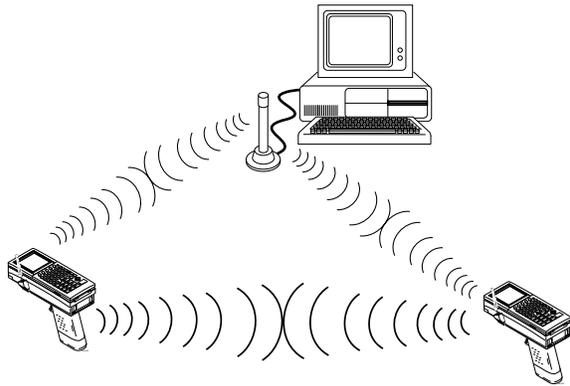


With a peer-to-peer NOS, each PC can be configured as a client, a server, or both. Peer-to-peer means that each PC can share all of its resources, such as files or printers, with any other PC on the network. This type of network operating system differs from traditional network operating systems where one product, a dedicated server, is required for sharing resources. Client PCs, using traditional network operating systems, cannot share data with other clients without storing the information on a server.

Peer-to-Peer and the RF Network

Wireless peer-to-peer networks are easier to install than wired peer-to-peer networks.

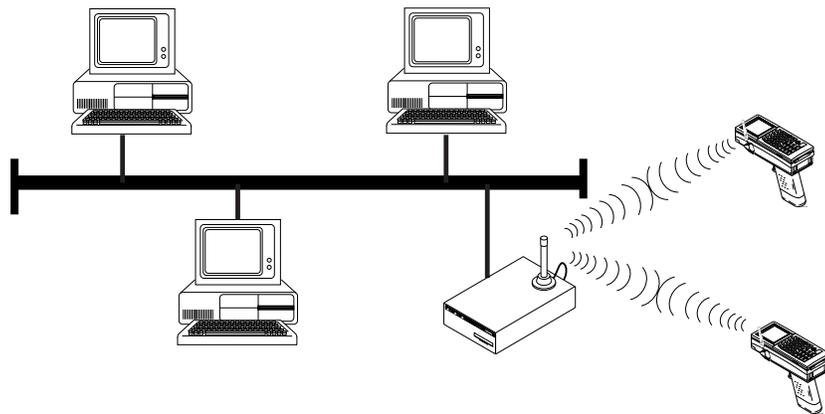
Wireless Peer-to-Peer Network



AP-05

However, many peer-to-peer networks consist of both wired and wireless clients. To establish communication between wired and wireless peer-to-peer networks, use the Access Point to bridge between the two subnetworks. After installing Access Points and a peer-to-peer network operating system, you can establish a network that can share files and printer resources instantly.

Peer-to-Peer Wireless to Wired Subnetworks



AP-06

2

Installing the Access Point

This chapter provides an overview of the product package and system requirements, and explains how to install the Access Point in your network.

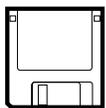
Unpacking the Access Point

Each Access Point package contains:

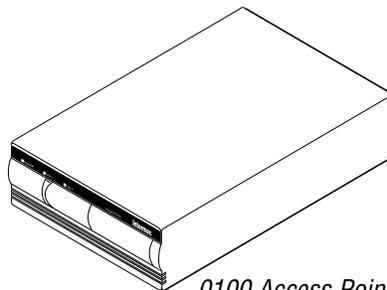
- One 0100 Access Point
- One 3.5 inch disk containing the configuration software
- One 3.5 inch disk containing the Access Point boot software
- One antenna
- One 110V power cable for North America
(International power cables are purchased separately.)

If any of these items are missing or damaged, please contact your local Intermec representative. Additional information that becomes available after the printing of this manual will be contained in a README file on the Access Point disk.

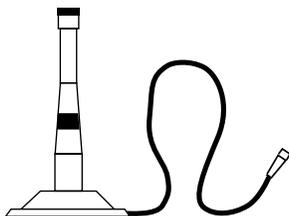
Access Point Package Components



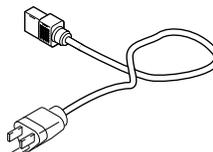
*0100 Access Point
Configuration Software*



0100 Access Point



*0100 Access Point
Antenna*



Power Cord

AP-01

System Requirements

To begin using your Access Point, you need the following minimum system requirements:

- An Ethernet cable drop: 10BASE2 (Thin Coax BNC) or 10BASET (Twisted Pair)
- A DOS-based PC either on the network or with a free serial port to run the configuration program

Or,

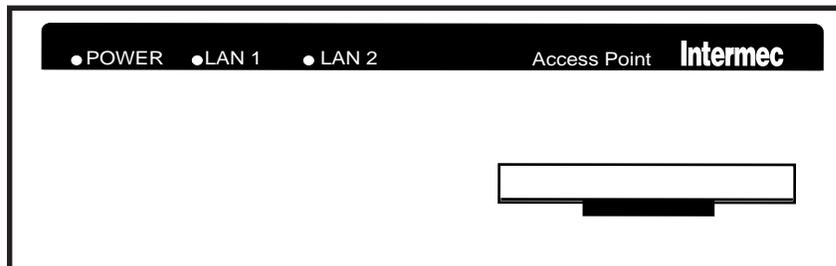
An SNMP management station

Access Point LEDs

There are three LEDs on the front panel of the Access Point.

- The green Power LED is on whenever the Access Point is powered on.
- The yellow LAN1 LED flashes to indicate RF transmissions on the network.
- The red LAN2 LED flashes to indicate Ethernet transmissions on the network.

Front Panel LEDs

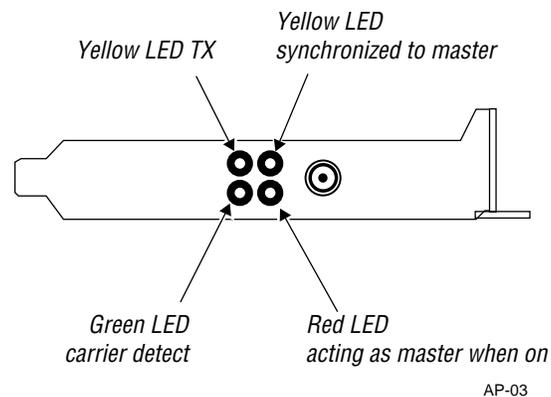


AP-02

There are four lights on the ISA card that are visible on the back of the Access Point.

- The yellow LED in the upper left indicates the ISA card is trying to transmit.
- The yellow LED in the upper right lights when the ISA card is synchronized to a master.
- The green LED in the bottom left lights whenever the card detects another station is transmitting.
- The red LED in the bottom right lights when the Access Point is acting as the master. There should be only one ISA card on the subnetwork with this light on at any time.

ISA Card LEDs



Access Point Reset Button

There is a reset button on the front panel of the Access Point. Press this button to reboot the Access Point.

Making a Backup Copy of the Boot Disk

Make a backup copy of your original Access Point boot disk and place the original disk in a safe place. Run the Access Point from the backup copy.

To make a backup copy

1. Insert the Access Point boot disk in the 3.5 inch drive of your host PC. You may have to remove it from the Access Point drive.
2. From a DOS prompt on your host PC, type

```
XCOPY A: A: /S
```

Note: If your 3.5 inch drive is the drive B of your PC, substitute B for A in the command line.

3. Follow the instructions on your host PC screen to copy the disk.
4. Remove the copied disk and place it in the Access Point drive. Place the original disk in a safe place.
5. Install the faceplate covering the 3.5 inch drive on the front panel of the Access Point.

The Access Point boot disk is copied.

Performing a Quick Installation



Caution

ETSI and FCC regulations mandate that the Access Point antenna not be alterable. Therefore, Access Point uses a custom antenna connector. Do not attempt to use a different antenna or you may damage the connector and the bridge.

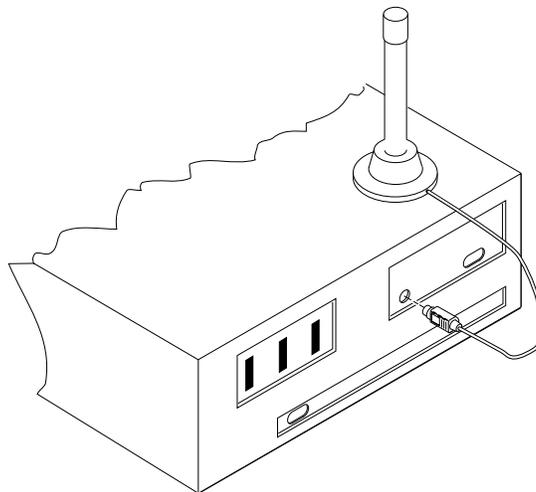
Conseil

La réglementation ETSI et FCC exige que l'antenne Access Point ne soit pas modifiable. Par conséquent, l'antenne Access Point utilise un connecteur d'antenne personnalisé. Ne tentez pas d'utiliser une antenne différente car vous risquez d'endommager le connecteur et le pont.

To install the Access Point

1. Locate the antenna connector at the back of the Access Point.
2. Firmly screw in the end of the antenna cable to the connector. Refer to the figure below.
3. Attach your Ethernet cable to the Ethernet port on the back of the Access Point.
4. Plug the power cable into the back of the Access Point and into an AC power outlet. The Access Point runs on any voltage from 100 to 240 VAC at 50 Hz or 60 Hz.
5. Insert the copy of the Access Point boot disk into the drive on the front of the Access Point.
6. Attach the faceplate over the Access Point drive.
7. Turn on the Access Point. The power switch is on the back. The Access Point emits a series of beeps as it is booting and initializing.

Attaching the Access Point Antenna



AP-04

0100 Access Point User's Manual

You have finished installing the Access Point if all of the following conditions are true:

- There will only be one Access Point on this network.

If you have more Access Points, refer to your site survey to place and configure them.

- You will use all the Access Point default values.

If you need to change any of the default values, refer to Chapter 3, "Configuring the Access Point."

- You will not be setting security IDs on your network.

If you want to set security IDs, refer to Chapter 3, "Configuring the Access Point."

- All other RF products are configured as stations or alternate masters.

If you have other masters on your network, you may need to configure the Access Point. Refer to Chapter 3, "Configuring the Access Point."

Configuring the Access Point

This chapter explains how to configure the Access Point locally and remotely using the Access Point configuration software.

Navigating Through the Configuration Application

When running the configuration application software, you can use either a mouse or keyboard to make selections. When using a keyboard:

- To make a selection, press the **Alt** key followed by the highlighted letter.
- To cycle through the buttons displayed, press the **Tab** key.
- To find out more information about the dialog box, choose the **Help** button.

Before You Run the Configuration Application

Before you run the configuration software, you need to install it on your host PC. Then, you need to decide if you want to configure the Access Point by hooking it up to your PC (locally), or if you are going to configure it across the network (remotely).

To install the configuration software on your PC

1. Insert the configuration software disk into your host PC. Create a new directory on your host PC for the configuration software and copy the software into this directory. For example:

```
C:\>MD AP
C:\>CD AP
C:\AP>COPY A:*.*
```

Note: If your 3.5 inch drive is the B drive of your PC, substitute B for A in the command line.

2. Choose one:
 - If you want to configure the Access Point locally, use the instructions in the next section.
 - If you want to configure the Access Point remotely, use the instructions in the section, "Configuring the Access Point Remotely," later in this chapter.

Configuring the Access Point Locally

To configure the Access Point locally, you need to connect your PC serial port to the RS-232 serial port on the back of the Access Point. You need:

- A null modem RS-232 cable.
- A DOS-based PC with an available serial port.

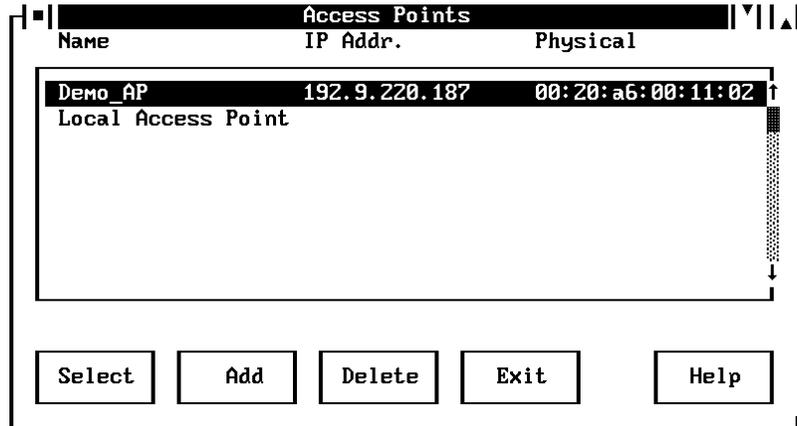
To configure the Access Point

1. Make sure to plug the power cable into the Access Point and into an AC power outlet.
2. Insert the copy of the Access Point boot disk into the Access Point drive and attach the faceplate over the drive.
3. Connect the Access Point to a serial port on your PC using the null modem RS-232 cable.
4. Turn on the Access Point. You will hear a series of beeps as the Access Point boots and initializes.
5. If the serial port that is connected to the Access Point is not COM2, change the SLIP.BAT file to reflect the correct port. Refer to the section, "Editing the SLIP.BAT File," later in this chapter.
6. Move to the directory where you copied the configuration application, type SLIP, and then type CFG. For example:

```
C:\>CD AP
C:\AP>SLIP
C:\AP>CFG
```

The following dialog box appears. Follow the instructions in the section, "Using the Configuration Dialog Box," later in this chapter.

Note: You may not run IP protocol stacks while the CFG program is loaded. You may run non-IP protocol stacks while the CFG program is loaded. You will need to create entries for those stacks in the NET.CFG file and bind them to the proper frame type.

Configuration Application Main Menu**Editing the SLIP.BAT File**

The SLIP.BAT file tells the configuration application which port on the PC you are using to communicate with the Access Point. Edit SLIP.BAT using a text editor (MS-DOS Edlin or Edit). It is formatted as follows:

```
SLIP8250 0x60 SLIP {INT} {I/O} {BAUD}
```

where {INT} and {I/O} refer to the interrupt and I/O address of the COM port. Refer to the following table.

	INT	I/O
COM1	4	0x3F8
COM2	3	0x2F8
COM3	4	0x3E8
COM4	3	0x2E8

An example of the SLIP.BAT file if the Access Point is connected to COM2 and communicating at 9600 baud is:

```
SLIP8250 0x60 SLIP 3 0x2F8 9600
```

Configuring the Access Point Remotely

To configure the Access Point remotely, you need:

- a DOS-based PC with an Ethernet card

To configure the Access Point

1. Load a packet driver for your Ethernet card on your PC. If you wish to use the Ethernet card's ODI driver rather than a packet driver, follow Step 2 through Step 5. Otherwise, go to Step 6.
2. Copy the ODI driver for this card into the same directory on your PC as the configuration application.
3. Edit the NET.CFG file (using a text editor like MS-DOS Edlin or Edit) and add the following information:

```
LINK SUPPORT  
BUFFERS 6 1600
```

For an example of the NET.CFG file, refer to Appendix A.

4. In the NET.CFG file, under the Link Driver section for your Ethernet card, make sure that the following line is listed as the **first** frame type:

```
FRAME ETHERNET_II
```

For an example of the NET.CFG file, refer to Appendix A.

5. Edit your AUTOEXEC.BAT file to load LSL, the ODI driver, and ODIPKT (using a text editor like MS-DOS Edlin or Edit).

For an example of the AUTOEXEC.BAT file, refer to Appendix A.

6. Edit the CFG.CFG file to add the IP address for the PC that is running the configuration application (using a text editor like MS-DOS Edlin or Edit).

If your network does not carry IP traffic, use the default setting of 192.0.1.1. The network portion of the PC's IP address must match that of the IP address of the Access Point.

An example of the CFG.CFG file is as follows:

```
# Configuration Tool configuration file  
ip_address 192.9.200.24
```

7. Reboot your PC.
8. Move to the directory on your PC where you copied the configuration application. Start the software by typing CFG. For example:

```
C:\>CD AP
C:\AP>CFG
```

The configuration application main menu dialog box appears. Follow the instructions in the section, "Using the Configuration Dialog Box" later in this chapter.

Note: You may not run IP protocol stacks while the CFG program is loaded. You may run non-IP protocol stacks while the CFG program is loaded. You will need to create entries for those stacks in the NET.CFG file and bind them to the proper frame type.

Configuring the Access Point Using SNMP Management Packages

You can manage the Access Point using any SNMP management package. The Access Point supports the following managed objects:

- MIB-II (RFC 1213)
- IEEE 802.1d Bridge MIB (RFC 1493)
- Enterprise MIB - The Enterprise MIB is supplied in ASN.1 format on the Access Point diskette. Follow the instructions in your SNMP management package for incorporating enterprise-specific MIBs.

0100 Access Point User's Manual

The following table contains a list of user-configurable SNMP objects:

Reset Access Point	prAPReset
IP Address	prAPIPAddress
RF Channel	prRlCfgChannel
RF Subchannel	prRlCfgSubchannel
RF Domain	prRlCfgDomain
RF Security ID	prRlCfgSecurityID
RF Station Type	prRlCfgStationType
RF Master Name	prRlCfgMasterName
Spanning Tree Priority	dot1dStpPriority
Bridge Max Age	dot1dStpBridgeMaxAge
Bridge Hello Timer	dot1dStpBridgeHelloTime
Bridge Forward Delay	dot1dStpBridgeForwardDelay
RF Port Priority	dot1dStpPortPriority
RF Port Enabled	dot1dStpPortEnable
RF Port Path Cost	dot1dStpPortPathCost
Ethernet Port Priority	dot1dStpPortPriority
Ethernet Port Enabled	dot1dStpPortEnable
Ethernet Port Path Cost	dot1dStpPortPathCost
Aging Time	dot1dTpAgingTime

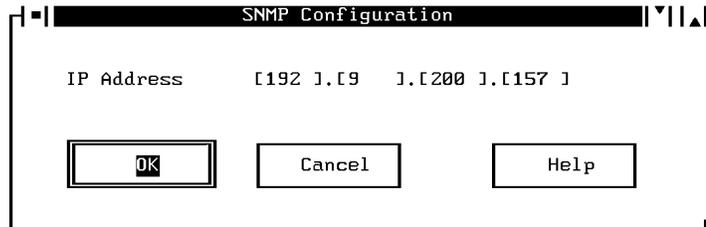
The Access Point currently supports two SNMP community strings: "Public," which has read-only permission, and "Private," which has full read-write permission.

To use SNMP management

1. Move to the directory on your PC where you copied the configuration application. Start the software by typing CFG. For example:

```
C:\>CD AP
C:\AP>CFG
```

The configuration application main menu dialog box appears.



2. Use the down arrow key to select the Access Point you want to manage.
3. Choose Select. The configuration dialog box appears.
4. Choose Configure SNMP. The SNMP Configuration dialog box appears.
5. Assign an IP Address to the Access Point you want to manage.
6. Choose OK to exit this dialog box and return to the configuration dialog box.
7. Cycle power on the Access Point, or press the reset button on the front panel of the Access Point for your changes to take effect.

Note: You may not run IP protocol stacks while the CFG program is loaded. You may run non-IP protocol stacks while the CFG program is loaded. You will need to create entries for those stacks in the NET.CFG file and bind them to the proper frame type.

Starting the Configuration Application

From the main menu of the configuration application, you can:

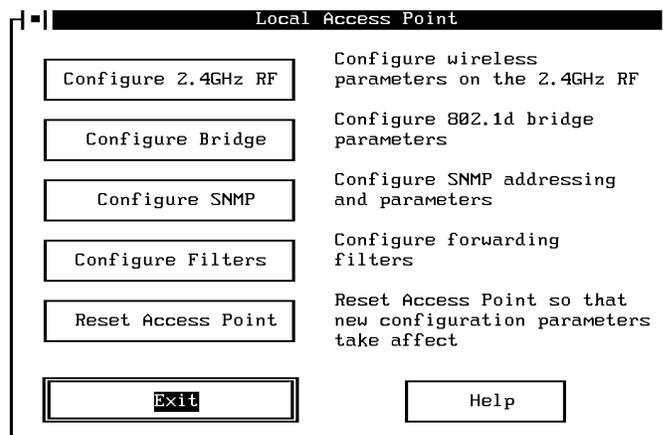
- **Select** an Access Point to configure. Choose this button if you want to configure a local Access Point or edit an existing remote Access Point.
- **Add** a new Access Point and configure it. Choose this button if you want to add a remote Access Point.
- **Delete** an Access Point.

Configuring a Local Access Point

1. From the main menu, use the down arrow key to select the Local Access Point.
2. Choose Select. The configuration dialog box appears.

The name of the Access Point, you are configuring is in the title bar of this dialog box. Follow the instructions in the section, "Using the Configuration Dialog Box," later in this chapter.

Configuration Dialog Box



Adding a New Remote Access Point

1. From the main menu, choose Add.

The Add Access Point dialog box appears.



The screenshot shows a dialog box titled "Add Access Point". It contains three input fields: "Access Point Name", "IP Address", and "Physical Address". Each field has a small cursor icon. Below the fields are three buttons: "OK", "Cancel", and "Help".

2. Enter a name for the Access Point.
3. Assign an IP Address to the new Access Point.
If your network does not carry IP traffic and you do not have another Access Point, use the default setting of 192.0.1.1.
If you do not want to assign an IP address or if you do not know the IP address, you can use a BOOTP server. Enter the Internet address into the BOOTP server.
4. Enter the Physical Address for the new Access Point. The physical address is written on a label that is on the rear panel of the Access Point.
5. Choose OK.
6. Cycle power on the Access Point, or press the reset button on the front panel of the Access Point for your changes to take effect.
7. If you need to configure the new Access Point, follow the instructions in the next section, "Editing a Remote Access Point."

Editing a Remote Access Point

1. From the main menu, use the down arrow key to select name, IP address, and physical address of the Access Point you want to edit.
2. Choose Select.

The configuration dialog box appears. The name of the Access Point you are configuring is in the title bar of this dialog box. Follow the instructions in the section "Using the Configuration Dialog Box" later in this chapter.

Deleting an Access Point

1. From the main menu, use the down arrow key to select the Access Point you want to delete.
2. Choose Delete.
3. Choose Yes when you are asked if you are sure you want to delete this Access Point.
Otherwise, choose No.

The configuration application removes the Access Point from the list in the main menu.

Using the Configuration Dialog Box

From the configuration dialog box, you can:

Configure 2.4 GHz RF This dialog box allows you to set the radio parameters.

Configure Bridge This dialog box allows you to set the spanning tree protocol parameters.

Configure SNMP This dialog box allows you to configure SNMP address and parameters.

Configure Filters This dialog box allows you to configure the filters.

Reset Access Point This dialog box allows you to reset the Access Point you are configuring so the new parameters take effect.

Configuring the Radio Parameters

For more information on radio parameters, refer to Appendix B, “Understanding the Radio Parameters.”

To fill in the 2.4 GHz RF Configuration dialog box

1. From the configuration dialog box, choose **Configure 2.4 GHz RF**. The 2.4 GHz RF Configuration dialog box appears.

2.4GHz RF Configuration		
Station Type	[Master]↓
Channel	[13]↓
Subchannel	[5]↓
Domain	[13]↓
Master Name	[TEST_AP]

Buttons: Set Security ID, Use Defaults, OK, Cancel, Help

2. Click the down arrow in the right side of the Station Type field. A dropdown list box appears.
3. From the list box, select the Station Type: Master, Alternate Master, Station. If you selected Station, skip to Step 6.
4. In the Channel field, enter the channel through which the master communicates with its stations.
5. If you have more than 15 masters in the Subchannel field, enter the subchannel through which the master communicates with its stations.
6. In the Domain field, enter the domain of the subnetwork through which all masters and stations in the network will communicate.
7. In the Master Name field, if you selected the station type to be Master or Alternate Master, enter an alias name.
8. Choose OK to exit this dialog box and return to the configuration dialog box.
9. Cycle power on the Access Point, or press the reset button on the front panel of the Access Point for your changes to take effect.

Configuring the Spanning Tree Protocol Parameters

For more information on the spanning tree protocol parameters, refer to Appendix B, "Understanding the Spanning Tree Protocol Parameters."

To fill in the Bridge Configuration dialog box

1. From the configuration dialog box, choose **Configure Bridge**. The Bridge Configuration dialog box appears.

Parameter	Value	Unit
Spanning Tree Priority	[32768]	
Bridge Max Age	[20]	seconds
Bridge Hello Time	[2]	seconds
Bridge Forward Delay	[15]	seconds
Aging Time	[300]	seconds
2.4GHz RF Port Priority	[128]	
2.4GHz RF Port Enabled	[Enabled]↓	
2.4GHz RF Port Path Cost	[625]	
Ethernet Port Priority	[128]	
Ethernet Port Enabled	[Enabled]↓	
Ethernet Port Path Cost	[100]	

2. Enter the appropriate information for your network for spanning tree protocol support, or you can choose the **Use Defaults** button.
3. Choose **OK** to exit this dialog box and return to the configuration dialog box.
4. Cycle power on the Access Point, or press the reset button on the front panel of the Access Point for your changes to take effect.

Configuring Filters

Access Point filters allow you to configure the Access Point to filter different kinds of packets.

To configure a filter

1. From the configuration dialog box, choose **Configure Filters**. The Access Point Filters dialog box appears.

```

Access Point Filters

[ X ] NON-2.4GHz RF ADDRESS FILTER

NOVELL IPX BROADCAST FILTERS          PROTOCOL TYPE FILTERS

[ X ] RIP                             [ ] IP/ARP (TCP/IP)
[ X ] SAP                             [ ] IPX (Novell)
[ X ] LSP                             [ ] Netbeui (Lan Manager, WFW)
                                       [ X ] AppleTalk
                                       [ ] Other

ARP FILTER

[ ] ARP Filter
Network IP Address                    [ 0 ] .1.0 .1.0 ]
Network Subnet Mask                   [ 0 ] .1.0 .1.0 ]

[ OK ] [ Cancel ] [ Use Defaults ] [ Help ]

```

2. Select all the traffic that you want to filter out and not forward to the RF network.
3. Choose OK to exit this dialog box and return to the configuration dialog box.
4. Cycle power on the Access Point, or press the reset button on the front panel of the Access Point for your changes to take effect.

More About the Access Point Filters

The filter configuration allows you to customize the type of traffic that is forwarded from the Ethernet network to the RF network. If one of the boxes contains a check, this indicates that traffic that meets the corresponding filter characteristic such as the Protocol Type will be filtered out and will not be forwarded.

Non-2.4 GHz RF Address Filter This filter prevents traffic that is destined to a non-broadcast, non-multicast, non-RF address from being forwarded from Ethernet to wireless.

Do not use this filter when using the node address overwrite feature on RF stations.

Novell IPX Broadcast Filters These filters prevent IPX broadcasts of the specified types from being forwarded from Ethernet to RF. Since RIP, SAP, and LSP broadcasts are of interest to routers and not end stations, these filters can typically be turned on.

Protocol Type Filters These filters prevent traffic of a particular protocol type from being forwarded from Ethernet to RF. When "Other Types" is checked, all types other than those listed will be filtered out.

Do not filter out the types of packets you know RF nodes will need to receive.

If you use TCP/IP as a protocol on your network, do not filter IP/ARP traffic.

If you have Macintosh computers on your Ethernet network that send AppleTalk traffic only to each other, you may want to filter those packets from RF stations.

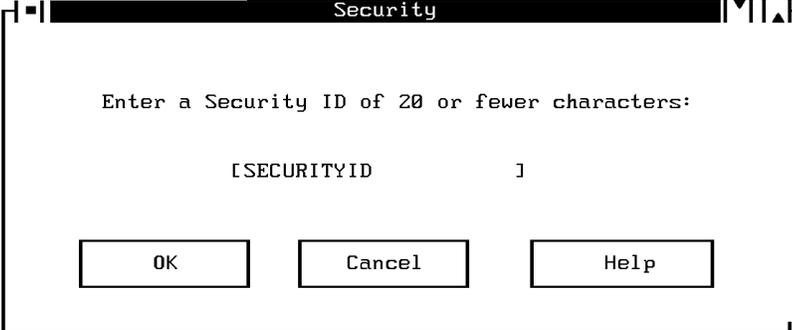
ARP Filter This filter enables IP ARP broadcast filtering. When this filter is enabled, ARP broadcasts will be forwarded from Ethernet to RF only if the destination IP address is on the IP network defined by the IP Network Address and Subnet Mask fields.

Setting the Security ID

As an added security measure, the Access Point allows you to set a security ID for each RF product installed on a network. All RF products must have matching security IDs in order to communicate.

To set the security ID

1. From the main menu, use the down arrow key to select the Access Point you want to assign a security ID.
2. Choose **Select**. The configuration dialog box appears.
3. Choose **Configure 2.4 GHz RF**. The 2.4 GHz RF Configuration dialog box appears.
4. Choose **Set Security ID**. The Security ID dialog box appears.



Security

Enter a Security ID of 20 or fewer characters:

[SECURITYID]

OK Cancel Help

5. Enter a security ID for the Access Point.
6. Choose OK to exit this dialog box and return to the 2.4 GHz RF Configuration Dialog box.
7. Choose OK to return to the configuration dialog box.

Resetting the Access Point

Each time you change one of the parameters in the Access Point, you need to reset it for the changes to take effect. There are three ways to reset the Access Point.

- From the configuration dialog box, choose **Reset Access Point**.
- Press the reset button on the front panel of the Access Point.
- Turn the Access Point off and then on using the switch on the back of the Access Point.

Helpful Hints and Troubleshooting

This chapter gives you some ideas on how to increase performance on a wireless network. It also provides solutions to some of the more common problems.

Helpful Hints

The following sections provide some helpful hints that may make your Access Point or your network run more efficiently.

Running Large Executable Files Efficiently

Some executable files, like Novell's LOGIN program, can take a long time to start up. You may be able to reduce this time if you copy the file to your local hard disk. This way the server is only accessed to read data files, which will allow for better performance.

Novell's VLM Technology

The ISA and PCMCIA ODI drivers support Novell's new VLM technology. It is the new standard interface for NetWare 2.x, 3.x, 4.x, and Personal NetWare clients. If you choose to use VLM.EXE instead of NETX.EXE when attaching a NetWare 2.x, 3.x, 4.x, or Personal NetWare client, you will achieve greater performance by up to 82% according to Novell's Systems Research Department tests. On a NetWare 3.11 server, you must load PBURST.NLM for the VLM technology's performance enhancements to take effect.

Determining Master Stations and Alternate Master Stations

The 2.4 GHz RF network uses a spread spectrum frequency hopping technique. This technique means that the radio signal is constantly moving from one frequency to another in a predefined sequence. In order for several radios to communicate, they must be at the same frequency at the same time.

The master station sets the pace for the other radios. All stations look to the master station to determine where and when to hop. If no master station is present, a station configured as an alternate master station will become the master for that session.

This configuration leaves the system administrator for the network with the task of configuring each wireless station on the network as a master station, alternate master station, or a station. In most cases, using the default configurations for each of the drivers will work fine. There may be times, however, when an administrator wants to change the configuration for performance or for other reasons.

Here are several factors to consider:

1. In every wireless network, at most one station must act as the master station. If you need to set up additional master stations, they should be configured as alternate master stations so that there is only one true master station on the network.
2. The master station must be within range of the other wireless stations on the network.
3. The master station should not be a station that will be moved or turned off like a notebook computer or a user's personal machine.
4. On a client-server based network, it usually makes sense for the server to be the master station.
5. On a peer-to-peer based network, it is probably a good idea to designate at least one computer as an alternate master station in the event that the master station is unavailable.
6. On a network with all notebook or pen-based computers, it may be advisable for all machines to be alternate master stations.
7. You will achieve better performance by configuring the fewest number of machines possible as masters or alternate masters.

Microwave Ovens

Microwave ovens operate in the same frequency band as the 0100 Access Point. Therefore, if you use a microwave within range of the 0100 you may notice network performance degradation. However, both your microwave and your 0100 network will continue to function.

Antenna Placement

Proper antenna placement can help improve Access Point performance. Use the following guidelines:

- Place the antenna as high as possible in an office environment above cubicle walls.
- Do not place a sheet of metal between two antennas.
- Make sure that the two antennas that are communicating are in the same plane. For example, do not lie one antenna on its side and have its partner standing upright.
- If the Access Point is mounted towards the ceiling, do not put the antenna on top of it.

Troubleshooting

The Access Point is very easy to install and operate. If you do experience difficulties however, use the information in this section to help diagnose and solve the problem. If you cannot resolve the problem, contact your Intermec service representative.

- Problem:** No response from the Access Point when configuring remotely.
- Solutions:**
1. Verify that the IP address for the configuration tool PC is set properly in the CFG.CFG file.
 2. Using local management, verify that the IP address for the Access Point is set correctly.
 3. Verify that you are not duplicating IP addresses on your network.
 4. Verify that no IP protocol stacks are loaded.

0100 Access Point User's Manual

- Problem:** No response from the Access Point when configuring locally.
- Solutions:**
1. Verify that SLIP.BAT is configured for the correct I/O port address and IRQ interrupt of the configuration PC's COM port.
 2. Verify that there are no IRQ conflicts between the configuration PC's COM port and other cards in the computer.
 3. Verify that you are using a null modem serial cable when attaching a configuration PC to the Access Point.
- Problem:** You are unable to establish communication with another machine on the network.
- Solution:** You may not have the same domain and security ID as on the other machine.
- Problem:** The SNMP management system is unable to write parameters.
- Solution:** Verify that you are using "Private" for the community string.



Appendix

Specifications

Network Interfaces	Ethernet 10BASE2 (Thin Coax BNC) Ethernet 10BASET (Twisted Pair)
Data Frame Types	Ethernet_802.2 Ethernet_802.3 Ethernet_II
Data Rate	1.6 Mbps (uncompressed) — RF 10 Mbps — Ethernet
Media Access Protocol	CSMA/CA
Ethernet Compatibility	Ethernet packet types and Ethernet Addressing
Frequency Band	2.4-2.483 GHz (spread spectrum frequency hopping)
Independent Channels	15
Output Power	100 mW
Range	240 ft radius (80 m)

How the 2.4 GHz RF Network Fits in the OSI Model

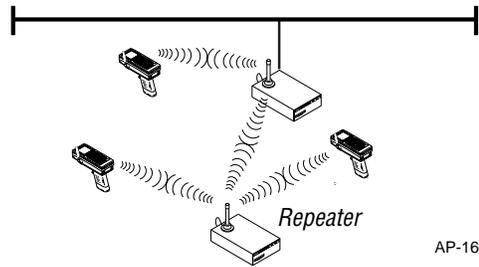
In 1977, a joint international working group, ISO/CCITT (International Standards Organization/Comité Consultatif Internationale de Telegrafique et Telefonique) developed the OSI reference model as a basic framework to deal with the complexity of communicating systems and the required protocol standards.

The OSI model divides a network into seven layers, each with clear tasks or functions. It also provides specific input to adjacent layers. Both hardware and software functions are accounted for in the model.

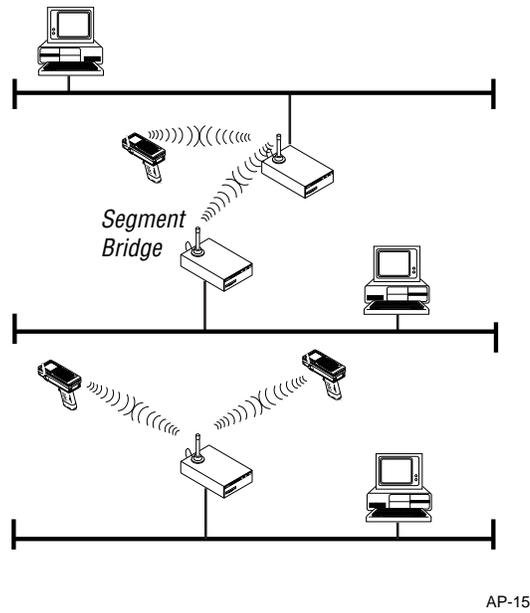
The following picture shows where the 2.4 GHz RF Network fits into the OSI model.

Layer	Name	2.4 GHz RF Network
7	Application	
6	Presentation	
5	Session	NetBIOS
4	Transport	Novell's IPX/SPX and TCP/IP
3	Network	Novell's ODI
2	Data Link	0100 Access Point MAC Layer S/W Novell's LSL
1	Physical	Access Point/JANUS 2020

Access Point as a One-Hop Repeater



Access Point as an Ethernet Segment Bridge



The AUTOEXEC.BAT File for the Access Point

The following printout is the AUTOEXEC.BAT file that the Access Point uses.

```
call slip
rem if not errorlevel 1 beep
lsl
rem if not errorlevel 1 beep
rl2isa
rem if not errorlevel 1 beep
ni6510
rem if not errorlevel 1 beep
ap
```

The NET.CFG File for the Access Point

The following printout is the NET.CFG file that the Access Point uses.

```
protocol stack 8021d
    StpPriority           32768
    StpMaxAge            364
    StpHelloTime        36
    StpForwardDelay     273
#StpPort 1 is ethernet
    StpPort #1 priority  128
    StpPort #1 enabled   1
    StpPort #1 pathCost 100
#StpPort 2 is RangeLAN
    StpPort #2 priority  128
    StpPort #2 enabled   1
    StpPort #2 pathCost  625
    TpAgingTime          300
    resets               117
    assert None
```

NET.CFG (continued)

```
link driver RL2ISA
    int            15
    port           270
    channel        13
    subchannel     13
    domain         7
    station_type   2
    master_name    Test_AP
    hop_period     1
    b_freq         2
    s_freq         7
    radio_mode     3
    bus_mode       2
    no_roaming
    no_repeating
    bridge
;    debug_color
    frame ethernet_II
    frame ethernet_802.2
    protocol ip 800 ethernet_II
    protocol arp 806 ethernet_II
    protocol span 42 ethernet_802.2

LINK DRIVER NI6510
    INT 5
    PORT 300
    DMA 5
    frame ethernet_II
    frame ethernet_802.2
    protocol ip 800 ethernet_II
    protocol arp 806 ethernet_II
    protocol span 42 ethernet_802.2

PROTOCOL TCPIP
    ip_address     192.9.200.157
    ip_router      192.9.200.1
    ip_subnetbits  24
```

The CFG.CFG File for the Access Point

The following printout is the CFG.CFG file that the Access Point uses.

```
ip_address 192.9.200.24
```



Appendix

Understanding the Radio Parameters

Access Points easily integrate into your existing network operating system. Each client on your network operates the same as any wired client PC except that wireless units share the same media or airspace. The following RF parameters allow the wireless adapters to share the same airspace effectively.

Note: Do not assign two Access Points or ISA cards to the same domain, channel, and subchannel unless you are purposely doing this in a spanning tree. If two wireless adapters have these parameters the same, you will create a loop in the network.

Station Type

Master	Alternate	Station
2	1	0

You need to configure each wireless adapter as a master, alternate master, or station. In each subnetwork, one master coordinates communication between various stations. This acting master can be either a master or an alternate master. An alternate master acts as either a master or a station. If an alternate master locates a master, then it acts as a station. If an alternate master cannot locate any other master within range, it acts as a master. For most network operating systems, define the ISA card in the server or Access Point as the master and all clients such as JANUS readers as stations.

A setting of 0 indicates the unit is a station; 1 indicates alternate master; 2 indicates master. The Access Point defaults to a station type of 2.

For performance considerations regarding the setting of this parameter, refer to Chapter 4, "Helpful Hints and Troubleshooting."

Master Name

Master	Alternate	Station
Optional	Optional	N/A

You can use this optional parameter to specify an alphanumeric name of up to 11 characters to simplify the identification of each master in your network.

Channel

Master	Alternate	Station
X	X	N/A

Each master can select one of 15 channels to establish communications with stations. The channels are designated 1 through 15, with 1 being the default setting. Wireless products use the surrounding air as the medium to transmit information. Each channel separates communications for each subnetwork to allow for higher data rate transmission capability in the same airspace. Each channel provides the 1.6 Mbps for a maximum total bandwidth of 24 Mbps in a particular area.

For networks with multiple masters, set each master to a different channel for optimum performance.

Subchannel

Master	Alternate	Station
X	X	N/A

If you need more than 15 masters in the same area, you can change the subchannel to a different value to separate the various networks. The subchannels are designated 1 through 15, with 1 being the default setting.

Domain

Master	Alternate	Station
X	X	X

To establish communications, all station types must have the same domain number. The domain is a number between 0 and 15, with 0 being the default setting.

For larger wireless networks, use the domain to establish roaming subnetworks throughout your building. Only clients with the same domain will roam from one Access Point to another.

Security ID

Master	Alternate	Station
X	X	X

To further improve the security of a wireless subnetwork, each RF product requires the same security ID to establish communication.

Understanding the Spanning Tree Protocol Parameters

The 0100 Access Point meets the IEEE 802.1d Spanning Tree Protocol specification. This protocol handles a complex bridged network (multiple bridges) where loops are created either unintentionally or to provide redundancy in the network. The bridges configure themselves into a spanning tree topology, removing any loops within the network. If you administer a network with more than one bridge, you will probably need to have some understanding of this protocol so that you can configure your bridges for optimum performance.

One of the bridges will become the root of the spanning tree. This root is determined by the bridge with the lowest spanning tree priority on the network. This bridge determines when all the bridges will broadcast their priorities, physical addresses, activity states, and other parameters. This communication is sent in "hello packets," and the root bridge determines the interval between these packets called the "hello time."

Once a root to the tree is established, all other bridges on the network must become branches. The order of the branches is determined by the spanning tree priority, path cost (number of jumps away from the root), and port priority for each bridge and each port on each bridge.

Where redundant bridges cause loops in the network, these loops are resolved by one of the bridges becoming inactive. This means the bridge will no longer forward packets of data that are sent to it. If the loops were not resolved, the same packet of data could travel around the network forever.

The network's bridges determine which bridge should become inactive based on several parameters. You can configure these parameters on an Access Point using the configuration program CFG.EXE, or on a network management station that supports the IEEE 802.1d Bridge MIB (RFC 1493).

Spanning Tree Priority

This parameter sets the priority of an Access Point in the spanning tree created on the network. Use it to determine the root node and the branches of the tree and to resolve conflicts over which bridge on a network will become inactive when there is a loop. In the event that two bridges have the same priority, the unique physical address breaks the tie. The lower value has the higher priority.

For this parameter, you may choose a value of 0 to 65,535, with a default value of 32,768.

Bridge Max Age

When the Access Point acts as the root, it uses this parameter to determine the maximum amount of time before discarding hello packet data for all bridges on the network.

This parameter is specified in seconds between 6 and 40, with a default value of 20.

Bridge Hello Timer

When the Access Point acts as the root, it uses this parameter to determine the interval of time between hello packets. If this parameter is set too high, the network will not quickly resolve contention problems. However, if the parameter is set too low, the network will be crowded with hello packet traffic.

This parameter is specified in seconds between 1 and 10, with a default value of 2.

Bridge Forward Delay

This parameter specifies the amount of time it takes to transition between port states after reset of the Access Point. The state transitions are as follows:

- disabled
- blocking incoming packets
- listening for other bridges
- learning the addresses of other bridges
- forwarding data

This parameter is specified in seconds between 4 and 30, with a default value of 15.

Aging Time

This parameter specifies the time after which the learned physical address of the network node is discarded. This data is dynamically acquired by the Access Point so that it can forward packets properly.

This parameter is specified in seconds between 10 and 1,000,000, with a default value of 300.

RF Port Priority and Ethernet Port Priority

These parameters are used in the spanning tree algorithm to determine the place of the port in the tree as well as to resolve loop contention problems. The lower value has the higher priority. You can set this parameter for both the RF port and the Ethernet port.

These parameters range from 0 to 255, with default values of 128.

RF Port Enabled and Ethernet Port Enabled

If either port is disabled, the Access Point will not forward data packets to the network through this port. Since there are only two ports on the Access Point, disabling either port would make the entire bridge inactive.

RF Port Path Cost and Ethernet Port Path Cost

These parameters specify the cost that is added to the spanning tree for this port of the Access Point. This cost applies only when the Access Point is not the root of the tree and when the port you are setting is the root port of the two Access Point ports.

The parameter range is 1 to 65535, with a default value of 100 for the Ethernet port and 625 for the RF port.



Glossary

This glossary contains definitions for terms specific to this manual and the Novell software network user environment.

0100 Access Point

Intermec's wireless bridge that allows RF packets to go from the RF network to the Ethernet network.

alphanumeric

Character set containing letters, numbers, and other characters, such as punctuation marks.

API (Application Programming Interface)

A well-defined interface to routines that an application can use to request and perform system-level tasks.

bandwidth

The size in hertz of the frequency range that a signal transmission occupies. Typical narrow band signals occupy a 25 KHz bandwidth. The 2.4 GHz radio frequency signal occupies a 1 MHz bandwidth.

bindery emulation

NetWare 4.0 feature that lets you emulate the bindery database system that was available in all previous versions.

BOOTP (Bootstrap Protocol) Server

A device that assigns an IP address in response to a query from an IP node. In this query, the IP node supplies its physical address. The BOOTP server then checks its tables to determine the corresponding IP address.

bridge

An internetworking device that incorporates the first two layers of the OSI model and allows connection of networks or subnetworks with similar architectures.

broadcast

A type of transmission in which a message sent from the host is received by many devices on the system.

BRU (Base Radio Unit)

A device that receives messages from the controller and broadcasts them to the data collection devices over radio frequency waves. The BRU also receives messages sent from devices over the radio waves and uploads them to the controller.

buffer

An area of storage used to hold data being transferred from one device to another.

channel

The path for transmitting data from a device to the host computer. In RF networks, it is the frequency hopping sequence the card follows. The 2.4 GHz bandwidth can be divided into 15 different channels.

CMOS (Complementary Metal-Oxide Semiconductor)

A type of integrated circuit noted for its extremely low power consumption.

controller

An electronic device that interfaces between the data collection devices and the system computer.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

CSMA is a protocol in which each node senses whether or not a channel is in use before attempting to transmit information. CA is an algorithm by which channel time is reserved to avoid collisions.

data collection device

A device used with a scanner to collect data from scanned bar codes and send it to a host computer.

data transmission

An event in which a block of data is transmitted from one device to another.

default router

An internal TCP/IP protocol stack variable.

device

Any physical item that is attached to a computer. A terminal, a printer, a reader, and a controller are all devices.

device address

A type of address that is used by the host to identify a particular data collection device.

direct sequencing

A spread spectrum technique by which the transmitted signal is spread over a particular frequency range.

domain

The area within a LAN that defines a region administered by a controller or server. The domain is also called a subnetwork.

downline

A device that is at the terminal end of a connection to the computer is referred to as being downline. When devices are connected to a computer, they are connected in a "line." Downline is a direction relative to the computer. Contrast with "upline."

If more than one computer is connected in a line, the upline computers usually handle data processing and the downline computers usually handle data collection and sometimes some data "preprocessing."

driver

A software module that controls an input/output port or external device.

Ethernet

A type of LAN that allows the transmission of computer data, audio data, and video data. Ethernet uses the access method known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD). See IEEE 802.3 standard for the specifications.

frequency hopping

A spread spectrum technique by which the band is divided into a number of channels and the transmissions hop from channel to channel in a prespecified sequence.

hand-held scanner

A scanner held and operated by a human. The scanner is moved to the object to be scanned, instead of moving the object close to the scanner.

host computer

If several computers are connected together on a network, the controlling computer is the host computer. A host computer can be a desktop, laptop, or notebook PC.

HOSTS file

A database that contains a list of remote hosts' IP addresses and their logical names (aliases) that any device on the network can reach.

inteference

A situation that occurs when an unwanted RF signal occupies the same frequency band as a desired signal.

IP (Internet Protocol)

This protocol provides a method for transmitting blocks of data (IP datagrams) between hosts.

IP address

An internal TCP/IP protocol stack variable. This address is a network level address assigned to each device in a TCP/IP network.

IPX (Internet Packet eXchange)

This protocol provides a means for message packets to be exchanged on an internetwork.

IRL (Interactive Reader Language)

A high level programming language developed by Intermec for their bar code readers.

LAN (Local Area Network)

A group of intelligent workstations that are hooked together to allow them to share of data, printers, and other devices. LANs are usually used over a small geographic area.

LSL (Link Support Layer)

This layer serves as an intermediary between the ODI and the link driver that supplies an interface between the network board and the rest of the operating system.

network

A collection of devices that can store and manipulate electronic data, interconnected in such a way that their users can store, retrieve, and share information with each other.

network ID

A number used by a device during channel search to locate the controller's RFNC address.

network node

An end point in a network to which or from which data can be routed. Usually this is a workstation or host computer.

Novell user name

This parameter identifies the user to the Novell software running on a remote host.

operating system

Refers to the code that operates a computer by managing its file systems, handling user input and output, and running programs. DOS, Windows, and UNIX are all operating systems.

OSI model

Open Systems Interconnection reference model. A framework developed by the International Standards Organization (ISO) to provide worldwide standards for computer communications.

packet

The unit of information by which the network communicates. A single network message with its associated header, addressing information, data, and optional trailer. A packet can also be called a frame or datagram.

port

The physical place where devices connect to each other for communication purposes.

protocol stack

A group of drivers that work together to span the layers in the network protocol hierarchy.

preferred tree

The tree you specify that you first want to connect to in a NetWare 4.X network if you have multiple trees. If this tree has a server with a free connection, the NetWare DOS Requester attaches to it.

RAM (Random Access Memory)

A memory that can be written into, or read, by locating any data address. A device that permits individual interrogation of any memory cell in a completely random sequence.

RARP (Reverse Address Resolution Protocol) Server

A device that assigns a physical address in response to a query from an IP node. In this query, the IP node supplies its IP address. The RARP server then checks its tables to determine the corresponding physical address.

repeater

The repeater extends coverage of the RFDC system by functioning as a message store-and-forward device.

RFDC (Radio Frequency Data Collection) system

The RFDC system refers to a data collection system in which the individual components communicate with each other by radio signals.

RFNC (Radio Frequency Network Controller) address

The radio frequency network controller's address that is used by the devices to communicate with the BRUs attached to the controller.

router

A software and hardware connection between two or more networks that permits traffic to be routed from one network to another on the basis of the intended destinations of that traffic.

scratch drive

The physical hard drive that you use to build the JANUS reader's drive images.

serial

A communication scheme in which the bits of a byte are transferred one at a time. Often serial transmission is used to link host computers to terminals and PCs to printers.

server

A computer that is configured to provide services to the network.

shell out feature

This feature allows you to go to the DOS command line without exiting the installation utility.

spread spectrum

A radio data transmission modulation technique by which the transmitted signal is spread over a bandwidth wider than the information bandwidth.

SNMP (Simple Network Management Protocol)

A protocol used to manage network activity.

SPX (Sequenced Packet eXchange)

This protocol provides a method for two workstations or applications to communicate across the network. SPX works with IPX to deliver the messages. However, SPX guarantees the delivery of the messages and maintains the order of messages on the packet stream.

standard upgrade

The process that allows you to make sure your JANUS reader has the most current version of firmware and that it has the default configuration.

subnet mask

An internal TCP/IP protocol stack variable.

subnetwork

A section of a large network that functions as an independent network, but does not appear separate to remote networks.

TCP (Transmission Control Protocol)

This protocol provides a method for creating a connection-oriented, reliable, error-free, full-duplex, byte-stream communication between two processes.

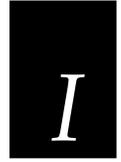
UNIX user name

This parameter is a variable in the DOS environment. The UNIX user name identifies the user to the Novell software running on a remote host.

upline

A device that is at the computer end of a connection between a computer and a device is referred to as being upline. When devices are connected to a computer, they are connected in a "line." Upline is a direction relative to the device, in contrast to "downline."

If more than one computer is connected in a line, the upline computers usually handle data processing and the downline computers usually handle data collection and sometimes some data "preprocessing."



Index

Symbols

- 10BASE2, 2-4
- 10BASET, 2-4
- 2.4 GHz RF Configuration dialog box. *See also* radio
 - parameters
 - channel, 3-13
 - domain, 3-13
 - master name, 3-13
 - Set Security ID, 3-17
 - station type, 3-13
 - subchannel, 3-13

A

- Access Point
 - 110V power cable, 2-3
 - adding a remote, 3-11
 - antenna, 2-3
 - antenna placement, 4-5
 - as a one-hop repeater, A-5
 - as an Ethernet segment bridge, A-5
 - AUTOEXEC.BAT, A-6
 - CFG.CFG, A-8
 - configuration application, 2-3
 - configuring a local, 3-10
 - deleting, 3-12
 - editing a remote, 3-12
 - features, 1-6
 - filters, 3-15
 - front panel LEDs, 2-4
 - how used, 1-11
 - in the OSI model, 1-3, A-4
 - installing, 2-6
 - NET.CFG, A-6
 - placement, 4-4
 - radio parameters, B-3
 - reset button, 2-5
 - resetting, 3-18
 - roaming, 1-7
 - security ID, 3-17
 - spanning tree protocol parameters, B-6
 - specifications, A-3
 - system requirements, 2-4

- troubleshooting, 4-5
 - unpacking, 2-3
 - Access Point Filters dialog box, 3-15
 - Add Access Point dialog box, 3-11
 - IP address, 3-11
 - name, 3-11
 - physical address, 3-11
 - adding a remote Access Point, 3-11
 - aging time, B-7
 - alphanumeric
 - definition, G-3
 - Alt key
 - and the configuration application, 3-3
 - alternate master, B-3
 - help determining, 4-3
 - antenna, 2-3
 - caution, 2-6
 - installing, 2-7
 - antenna placement, 4-5
 - API
 - definition, G-3
 - application programming interface. *See* API
 - ARP filter, 3-16
 - AUTOEXEC.BAT, A-6
 - loading LSL, 3-6
 - loading ODIPKT, 3-6
 - loading the ODI driver, 3-6
- B**
- bandwidth
 - definition, G-3
 - base radio unit. *See* BRU
 - bindery emulation
 - definition, G-3
 - BOOTP server, 3-11
 - definition, G-3
 - bootstrap protocol server. *See* BOOTP server
 - bridge, 1-3
 - definition, G-3
 - Bridge Configuration dialog box, 3-14. *See also*
 - spanning tree protocol parameters
 - Use Defaults button, 3-14
 - bridge forward delay, B-7

0100 Access Point User's Manual

bridge hello timer, B-7

bridge max age, B-7

broadcast

definition, G-3

BRU

definition, G-4

buffer

definition, G-4

buffers, 3-6

button

reset, 2-5

C

carrier sense multiple access/collision avoidance. *See* CSMA/CA

caution, viii

CFG.CFG, A-8

adding the IP address for the PC, 3-6

channel, 1-7, 3-13, B-4

definition, G-4

client, 1-4, 1-9

CMOS

definition, G-4

COM port

setting, 3-5

commands, ix

complementary metal-oxide semiconductor. *See* CMOS

configuration application

and IP protocol stacks, 3-7

configuring locally, 3-3

configuring remotely, 3-3, 3-6

installing, 3-3

main menu, 3-5

making a backup copy, 2-6

navigating, 3-3

starting, 3-7, 3-10

configuration dialog box, 3-10

Configure 2.4 GHz RF button, 3-12

Configure Bridge button, 3-12

Configure Filters button, 3-12

Configure SNMP button, 3-12

Reset Access Point button, 3-12, 3-18

Configure 2.4 GHz RF button, 3-12

Configure Bridge button, 3-12

Configure Filters button, 3-12

Configure SNMP button, 3-12

configuring

local Access Point, 3-10

local requirements, 3-4

remote requirements, 3-6

using SNMP management packages, 3-7

configuring filters, 3-15

configuring SNMP, 3-9

controller

definition, G-4

CSMA/CA

definition, G-4

D

data collection device

definition, G-4

data transmission

definition, G-4

default router

definition, G-4

deleting an Access Point, 3-12

device

definition, G-5

device address

definition, G-5

direct sequencing

definition, G-5

disk

making a backup copy, 2-6

domain, 1-7, 3-13, B-3, B-5

definition, G-5

DOS-based PC, 3-4, 3-6

downline

definition, G-5

driver

definition, G-5

E

editing a remote Access Point, 3-12

Ethernet

definition, G-5

Ethernet cable drop, 2-4

installing, 2-7

Ethernet card
 ODI driver, 3-6
 packet driver, 3-6
 Ethernet port enabled, B-8
 Ethernet port path cost, B-8
 Ethernet port priority, B-8
 Ethernet segment bridge, A-5
 executable files
 running efficiently, 4-3

F

filters
 ARP, 3-16
 configuring, 3-15
 non-2.4 GHz RF address, 3-16
 Novell IPX broadcast, 3-16
 protocol type, 3-16
 frequency hopping
 definition, G-5
 front panel
 LEDs, 2-4

G

green LED, 2-4, 2-5

H

hand-held scanner
 definition, G-6
 help
 for the configuration application, 3-3
 Help button, 3-3
 helpful hints, 4-3
 determining station types, 4-3, 4-4
 microwave ovens, 4-4
 Novell's VLM technology, 4-3
 running large executable files efficiently, 4-3
 host computer
 definition, G-6
 HOSTS file
 definition, G-6

I

IEEE 802.1d, 1-6
 IEEE 802.3, 1-3
 installing the Access Point, 2-6
 inteference
 definition, G-6
 interactive reader language. *See* IRL
 Internet packet exchange. *See* IPX
 Internet protocol. *See* IP
 IP
 definition, G-6
 IP address
 assigning, 3-9, 3-11
 definition, G-6
 editing CFG.CFG, 3-6
 using a BOOTP server, 3-11
 using default, 3-11
 IP protocol stacks
 and the configuration application, 3-4, 3-7, 3-9
 IPX
 definition, G-6
 IRL
 definition, G-6
 ISA card LEDs, 2-5

K

keypad input, viii

L

LAN
 definition, G-6
 LAN1 LED, 2-4
 LAN2 LED, 2-4
 LEDs
 front panel, 2-4
 ISA card, 2-5
 light emitting diodes. *See* LEDs
 link driver, 3-6
 link support, 3-6
 link support layer. *See* LSL: definition
 local Access Point
 configuring, 3-10

0100 Access Point User's Manual

local area network. *See* LAN: definition

LOGIN program

 running efficiently, 4-3

LSL

 adding to AUTOEXEC.BAT, 3-6

 definition, G-7

M

main menu

 adding an Access Point, 3-10

 deleting an Access Point, 3-10

 editing an Access Point, 3-10

manual

 audience, viii

 conventions used in, viii

 Installation Utility, ix

 JANUS 2020, ix

 JANUS addendum, ix

 JANUS roadmap, ix

 mounting bracket, ix

 NetWare Administrator's Guide, ix

 related, ix

 terms used in, viii

master, B-3

 assigning a name, B-4

 help determining, 4-3

master name, 3-13, B-4

microwave ovens, 4-4

N

NET.CFG, A-6

 buffers, 3-6

 editing for configuring remotely, 3-6

 editing for IP protocol stacks, 3-4, 3-7, 3-9

 link driver, 3-6

 link support, 3-6

network

 definition, G-7

network applications, 1-4

network ID

 definition, G-7

network node

 definition, G-7

network operating systems

 about, 1-3

 and the RF network, 1-5

 applications, 1-4

 client, 1-4

 functions, 1-4

 moderately complex example, 1-4

 moderately complex wireless example, 1-6

 peer-to-peer, 1-9

 roaming example, 1-8

 server, 1-4

 simple wireless example, 1-5

 wireless peer-to-peer example, 1-10

networks

 simple example, 1-3

non-2.4 GHz RF address filter, 3-16

note, viii

Novell IPX broadcast filter, 3-16

Novell user name

 definition, G-7

null modem cable, 3-4

O

ODI driver, 3-6

 adding to AUTOEXEC.BAT, 3-6

ODIPKT

 adding to AUTOEXEC.BAT, 3-6

one-hop repeater, A-5

operating system

 definition, G-7

OSI model, 1-3

 definition, G-7

P

packet

 definition, G-7

packet driver, 3-6

peer-to-peer network

 about, 1-9

 and the RF network, 1-10

 client, 1-9

 example, 1-9

 server, 1-9

 wireless example, 1-10

 wireless to wired example, 1-11

- physical address, 3-11
- port
 - definition, G-8
- power cable, 2-3, 3-4
 - installing, 2-7
- Power LED, 2-4
- power switch, 2-7
- preferred tree
 - definition, G-8
- protocol stack
 - definition, G-8
- protocol type filters, 3-16
- R**
- radio frequency data collection system. *See* RFDC system: definition
- radio frequency network controller address. *See* RFNC address: definition
- radio parameters
 - channel, 3-13, B-4
 - configuring, 3-13
 - domain, 3-13, B-3, B-5
 - master name, 3-13, B-4
 - security ID, B-5
 - spanning tree, B-3
 - station type, 3-13, B-3
 - subchannel, 3-13, B-4
 - understanding, B-3
- RAM
 - definition, G-8
- random access memory. *See* RAM: definition
- RARP server
 - definition, G-8
- README file, 2-3
- red LED, 2-4, 2-5
- remote Access Point, 3-11
 - adding, 3-11
 - deleting, 3-12
 - editing, 3-12
- repeater
 - definition, G-8
- requirements
 - to connect the Access Point, 2-4
- Reset Access Point button, 3-12, 3-18
- reset button, 2-5, 3-18
- resetting the Access Point, 3-18
- reverse address resolution protocol server. *See* RARP server: definition
- RF network, 1-5
 - and the peer-to-peer network, 1-10
 - moderately complex wireless example, 1-6
 - peer-to-peer example, 1-11
 - setting security IDs, 3-17
 - simple wireless example, 1-5
 - wireless peer-to-peer example, 1-10
- RF port enabled, B-8
- RF port path cost, B-8
- RF port priority, B-8
- RFDC system
 - definition, G-8
- RFNC address
 - definition, G-8
- roaming, B-5
 - between Access Points, 1-7
 - example, 1-8
 - with JANUS readers, 1-7
- router, G-4. *See also* default router
- S**
- safety, vii
 - caution, viii
 - note, viii
- security ID, 1-7, B-5
 - setting, 3-17
- Security ID dialog box, 3-17
- server, 1-9
- Set Security ID, 3-17
- setting the security ID, 3-17
- simple network management protocol. *See* SNMP capability
- SLIP.BAT
 - changing the COM port, 3-5
- SLIP.BAT file
 - editing, 3-5
- SNMP, 2-4
 - assigning an IP address, 3-9
 - capability, 1-6
 - user-configurable objects, 3-8
 - using management packages, 3-7
- SNMP Configuration dialog box, 3-9

0100 Access Point User's Manual

- spanning tree, B-3
- spanning tree priority, B-6
- spanning tree protocol parameters, 1-6
 - aging time, B-7
 - bridge forward delay, B-7
 - bridge hello timer, B-7
 - bridge max age, B-7
 - configuring, 3-14
 - Ethernet port enabled, B-8
 - Ethernet port path cost, B-8
 - Ethernet port priority, B-8
 - RF port enabled, B-8
 - RF port path cost, B-8
 - RF port priority, B-8
 - spanning tree priority, B-6
 - understanding, B-6
- specifications
 - data frame types, A-3
 - data rate, A-3
 - Ethernet compatibility, A-3
 - frequency band, A-3
 - independent channels, A-3
 - media access protocol, A-3
 - network interfaces, A-3
 - output power, A-3
 - range, A-3
- station, B-3
- station type, B-3
 - alternate master, 3-13, B-3
 - master, 3-13, B-3
 - station, 3-13, B-3
- station types
 - help determining, 4-4
- subchannel, 1-7, 3-13, B-4
- subnet mask
 - definition, G-10
- subnetwork, 1-5. *See also* domain
 - bridging, 1-11
 - definition, G-10
- system requirements, 2-4
 - DOS-based PC, 2-4
 - Ethernet cable drop, 2-4
 - SNMP management station, 2-4

T

- Tab key
 - and the configuration application, 3-3
- TCP
 - definition, G-10
- thin Coax BNC cable, 2-4
- transmission control protocol. *See* TCP: definition
- transparent bridging, 1-6
- troubleshooting, 4-5
- twisted pair cable, 2-4

U

- UNIX user name
 - definition, G-10
- upline
 - definition, G-10

V

- VLM
 - helpful hints, 4-3

W

- warranty, ii, vii
- workstation. *See* client

Y

- yellow LED, 2-4, 2-5