Technical Reference Manual

P/N 067150-005

21XX Universal Access Point™

Intermec
A UNOVA Company

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

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

Canadian service and technical 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.

Manual Change Record

This page records the changes to this manual. The manual was originally released as version 001.

Version	Date	Description of Change
002	11/98	Revised to add information about the 900 MHz UAP and WAP, and the OpenAir WAP.
003	6/99	Revised to add information about the IEEE 802.11 Direct Sequence radio and firmware upgrade features.
004	10/99	Revised to add information about the UHF radio and the 2101 Universal Office Access Point. This revision also reflects the discontinuance of the 2110 Wireless Access Point and the name change for this manual from a user's manual to a technical reference manual.
005	12/99	Revised IEEE 802.11 DS radio menus and parameters.

Contents

2

Installing and Configuring the UAP

3

Installing and Configuring a Wireless Access Point

4

Configuring the Ports

5

Configuring the Bridging Parameters

C

Positioning Antennas

D

Upgrading the UAP

G

Glossary

I

Index

Before You Begin

This section introduces you to standard warranty provisions, safety precautions, cautions and notes, document formatting conventions, and sources of additional product information. A documentation roadmap is also provided to guide you in finding the appropriate 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. you can call 1-800-755-5505, and in Canada call 1-800-688-7043. Otherwise, refer to the Worldwide Sales & Service list that ships with this manual for the address and telephone number of your Intermec Technologies sales organization.

Note: Opening this product may void the warranty. The internal workings of this product can only be accessed by Intermec service personnel. Radio replacements and upgrades require Intermec service personnel.

Safety Summary

Your safety is extremely important. Read and follow all warnings and cautions in this book 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.

Note: 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 *21XX Universal Access Point Technical Reference Manual* provides you with information about the features of this product, and how to install, configure, and troubleshoot it. You must be familiar with your host PC, your other Intermec equipment, and your network.

What You Will Find in This Manual

This table summarizes the information in each chapter of this manual:

For Information On	Refer To
Understanding the access point and its features	Chapter 1, "Learning About the 21XX Universal Access Point," explains the features of the access point and how it works in an RF network.
Installing and configuring the 21XX Universal Access Point	Chapter 2, "Installing and Configuring the UAP," explains how to install and configure the 21XX Universal Access Point.
Installing and configuring a wireless access point	Chapter 3, "Installing and Configuring a Wireless Access Point," explains how to install and configure a wireless access point.
Configuring the ports	Chapter 4, "Configuring the Ports," explains how to configure your wired and wireless ports.
Configuring the bridging parameters	Chapter 5, "Configuring the Bridging Parameters," explains how to set bridge parameters, create filters, and set global radio parameters.

For Information On	Refer To
Using Telnet or a Web browser to access the access point	Chapter 6, “Managing the UAP Remotely,” provides information on accessing the UAP remotely.
Performing maintenance and troubleshooting	Chapter 7, “Maintenance and Troubleshooting,” provides information on using the Maintenance menu and resolving frequently asked questions.
Using advanced features	Chapter 8, “Advanced Features,” explains how to use console command mode, script files, and the UAP command monitor.
Specifications and default values	Appendix A, “Specifications,” provides specifications and default values for the universal access point.
INCA/IP	Appendix B, “Understanding INCA/IP” provides an overview of INCA/IP.
Positioning antennas	Appendix C, “Positioning Antennas” provides specific information about positioning antennas for the UAP.
Upgrading the access point	Appendix D, “Upgrading the UAP” provides procedures for upgrading the access point firmware.

Terminology

You should be aware of how these terms are being used in this manual:

Term	Description
UAP or 21XX Universal Access Point	These terms are used to describe any of the 21XX Universal Access Point devices, including the 2100 Universal Access Point and the 2101 Universal Office Access Point, unless specifically stated otherwise.
WAP	This term refers specifically to a 21XX Universal Access Point that is configured as a wireless repeater.
end device	Any wireless device used to collect and transmit data to a 21XX Universal Access Point.

Format Conventions for Input From a Keyboard or Keypad

This table describes the formatting conventions for input from host PC keyboards:

Convention	How to Interpret the Convention
`Special text`	Shows the command as you should enter it into the device.
Italic text	Indicates a variable that you must replace with a value.
Bold text	Indicates the keys you must press on a PC keyboard. For example, “press **Enter**” means you press the key labeled “Enter” on the PC keyboard.
where	This word introduces a list of parameters and explains the values you can specify for them.

Patent Information

Product is covered by one or more of the following patents: 4,910,794; 5,070,536; 5,295,154; 5,349,678; 5,394,436; 5,425,051; 5,428,636; 5,483,676; 5,504,746; 5,546,397; 5,574,979; 5,592,512; 5,680,633; 5,682,299.

Other Related Manuals

You may need additional information when working with the 21XX Universal Access Point. Please visit our Web site at www.intermec.com to download many of our current manuals in PDF format. To order printed versions of the Intermec manuals, contact your local Intermec representative or distributor.

1

Learning About the 21XX Universal Access Point

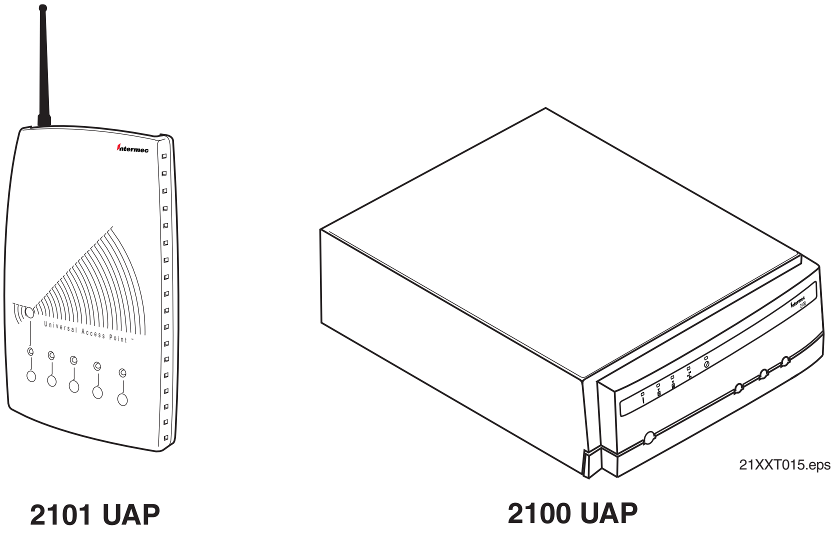
This chapter provides an overview of the 21XX Universal Access Point.

What Is the Intermec 21XX Universal Access Point?

The Intermec 21XX Universal Access Point™ (UAP) is an extended-range, high-performance, wireless local area network (LAN) device. UAPs extend the range of your wired network by providing network communications between the wired network and wireless end devices. You can use the system defaults or configure the device to meet your particular network needs.

The UAP has been designed to be powerful yet easy to use. The UAP can be configured as an access point or as a point-to-point bridge. An access point attaches to a wired network and provides wireless network access for end devices. A point-to-point bridge connects two wired LANs. A point-to-point bridge is often used to provide wireless communications in locations where it is difficult to run cable, such as across roads or between buildings.

You can also configure a UAP as a repeater or wireless access point (WAP). A WAP requires no Ethernet connection; it receives data from an end device and forwards it to an access point. A WAP is useful in areas that do not support a wired network connection.



The 2101 Universal Office Access Point is a high-performance access point that features a streamlined case designed for the office environment.

The 2100 Universal Access Point features a sealed case that meets IP 54 standards. It is designed for industrial environments and for placement outdoors. Options include an integrated heater for use in environments that experience temperature fluctuations that drop below freezing. A heater/insulated bag option is also available for use in environments that maintain constant cold temperatures, such as cold storage facilities.

Note: The model 2110 WAP has been discontinued. The WAP functionality is now available in the 2100 and 2101 UAPs.

Features of the UAP

The 21XX Universal Access Point supports a variety of wireless technologies and allows easy software and hardware upgrades. Some of the features of the UAP are described here.

High Performance The UAP includes a state-of-the-art RISC processor that meets current data requirements and will support future high-speed wired and wireless LAN technologies. The UAP filters traffic at full Ethernet wire speeds and forwards traffic at full radio speeds. You can use flooding and filtering options to keep unnecessary traffic off the airwaves and optimize performance on busy networks. You can configure a variety of protocol and broadcast filters to further eliminate traffic.

Radio Independent The UAP's Radio Independent™ architecture supports a variety of radios and allows you to upgrade your radios as technology changes. Radios can be added or replaced without replacing the entire access point infrastructure. Additionally, future releases of the UAP will offer dual radio support so the UAP can support mixed wireless radios for different range and throughput requirements.

Enterprise Roaming INCA/IP is an advanced feature that allows enterprise roaming. Using INCA/IP in networks with standard IP routers allows end devices to roam across network subnets. INCA/IP uses Generic Routing Encapsulation (GRE), a registered protocol from the TCP/IP suite. GRE allows frames destined for end devices on a different IP subnet to be encapsulated with an IP address that passes transparently through the routers. This encapsulation is referred to as tunneling. Encapsulated frames may be sent, or tunneled, through any of the physical ports. Additionally, you can restrict tunneling to only end devices or selected frame types. For detailed information about INCA/IP, see Appendix B, "Understanding INCA/IP."

Advanced Network Management If you intend to manage your UAP remotely, you must first configure the UAP using a direct serial link. You can then use Telnet, SNMP, or a Web browser to remotely monitor traffic, set additional configuration parameters, and upgrade the firmware.

You can use any SNMP network management platform to manage the UAP by using variables defined in the UAP's Management Information Base (MIB). Contact your local Intermec representative for information about obtaining the MIB, which is SNMP Version 1 compliant.

Advanced Filtering The UAP has an advanced wireless LAN feature called Wireless ARP (WARP) Server. An ARP (Address Resolution Protocol) is a multicast message that is used to determine the physical MAC address of an end device when the IP address is known. The ARP server enables the UAP to convert multicast ARP requests to unicast ARP requests. These unicast requests reduce wireless broadcast traffic, thereby increasing network performance and extending battery life in end devices.

Additionally, you can set both Ethernet and INCA/IP filters on the UAP. Ethernet filters help reduce the amount of traffic forwarded into the radio network. INCA/IP filters limit the protocol types that can pass through an INCA/IP tunnel.

IGMP The UAP supports IP multicasting and the Internet Group Management Protocol (IGMP). IGMP is a protocol that allows you to have more than 8 INCA/IP tunnels. Using IGMP, an IP host notifies IP routers that it wants to participate in an IP multicast group. In an INCA network that includes INCA/IP tunnels, the multicast group consists of the root UAP and UAPs on remote IP subnets. An IP router forwards IP packets with a Class D multicast destination address to those IP subnets that have at least one host participating in the multicast group.

You can establish multiple INCA/IP tunnels with a single multicast IP address. (You can only create one tunnel for each unicast or directed-broadcast IP address.) IGMP allows a UAP to participate in an IP multicast group without requiring any special router configuration.

Electronic Software Distribution You can upgrade the firmware on your UAP using a Web browser. After you upgrade the root UAP, you can distribute the firmware upgrade to all UAPs on your network. The UAP supports Trivial File Transfer Protocol (TFTP) so you can perform a TFTP transfer using the UAP as either a TFTP client or server. The UAP also supports scripting via Telnet and SNMP. For more information about the electronic software distribution capabilities of the UAP, see Appendix D, “Upgrading the UAP.” Contact your local Intermec representative for information about obtaining firmware upgrades.

DHCP Support The UAP supports the client Dynamic Host Configuration Protocol (DHCP). You can have a DHCP or BOOTP server assign a permanent lease to the UAP and then automatically assign an IP address, default router, and subnet mask to it.

Security Security for the UAP is provided on both the network connection and the serial connection. You must enter a valid password before you can access the Configuration menu. You can change the default password from the Maintenance screen. See “Understanding the Maintenance Menu” in Chapter 7 for more information.

Bridging Features

The UAP is a translating bridge, forwarding frames that have unique physical and MAC protocol implementations between the Ethernet network and wireless media. The UAP implements the basic learning and forwarding functions of a simple wired LAN bridge and includes additional functionality to address unique problems in wireless LANs.

End devices operate similarly to Ethernet products; therefore, all of your existing Ethernet applications will work with the wireless network without any special networking software. Some of the significant functions supported at the bridging layer are described in this section.

Network Organization UAPs automatically configure into a self-organized network using a spanning tree topology. As devices are added to or removed from the network, the UAPs automatically reconfigure to maintain reliable operation. The spanning tree provides efficient, loop-free forwarding of frames through the network and allows rapid roaming of end devices.

The root UAP initiates the spanning tree. The root UAP is a UAP that coordinates the network and distributes common system parameters to other UAPs and end devices. The root is elected from a group of UAPs that are designated as root candidates at the time of installation. The election process also occurs in the event of a root failure. You can configure your network with overlapping coverage so that the network automatically recovers from any single point of failure. For more information about the root, see Chapter 5, “Configuring the Bridging Parameters.”

End devices can optionally participate in the INCA spanning tree protocol by explicitly attaching to the network. As a result, operational parameters are easily distributed, unicast flooding is reduced or eliminated, and roaming hand-off logic is more robust.

Forwarding The UAP maintains a forwarding database of all physical station addresses, and it knows the correct port for each address. The UAP updates this database by monitoring source addresses on each port (backward learning), by receiving explicit INCA attachment messages, and by examining messages exchanged between UAPs when end devices roam. The database also includes the power management status of each end device, which allows the UAP to support the pending message feature of the network. The forwarding database allows the bridging software to make efficient forwarding decisions.

Switch Support Ethernet switches that do not comply with the 802.1d standard have difficulty handling end devices that roam between different switched segments. The UAP provides data link tunneling for switches that do not handle roaming. Using data link tunneling, frames for a given end device always appear on the root UAP’s switched segment, regardless of roaming, and the switch’s routing tables remain stable.

Flooding Configurations When the destination address is unknown, standard LAN bridges flood frames on all ports. Most end devices supported by the UAP operate at lower speeds than Ethernet; therefore, indiscriminate flooding from a busy Ethernet backbone to an end device can consume a substantial portion of the available wireless bandwidth and reduce system performance. The UAP allows you to set flooding control options for both unicast and multicast frames to free up bandwidth and improve system performance.

Pending Messages End devices may use power management to maintain battery life. These devices wake up periodically to receive frames that arrived while their radio was powered down. The bridging software in the UAP provides a pending message delivery service that allows frames to be held until the end device is ready to receive them.

Filtering Options The UAP incorporates extensive filtering capabilities. Basic filters allow you to filter on DIX type, protocol port, socket, or SAP. Advanced filters let you create and group filters based on data patterns that you define.

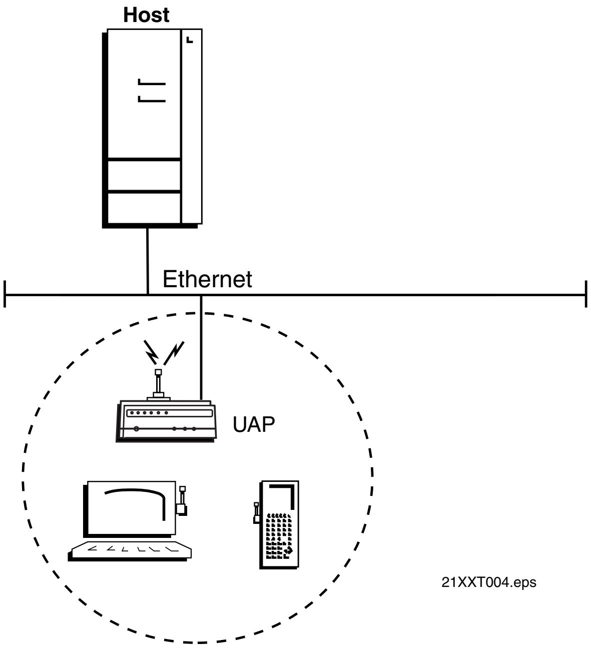
Using the UAP in a Wireless Network

In general, the 21XX Universal Access Point forwards data between end devices and the wired network. Note that the 2100 and the 2101 offer the same access point functionality and are interchangeable in your network. You should install the 2100 where certain environmental factors are a concern, and you should install the 2101 where environmental packaging is not required. The UAP supports a variety of network configurations.

Using a UAP in a Simple Wireless Network

You can use the UAP to extend your existing Ethernet network to include wireless nodes. The UAP connects directly to your wired network, and the end devices form an INCA network that functions as a wireless extension of the wired LAN.

In a simple wireless network, a single UAP on the wired network serves as a transparent bridge between the wired network and end devices. The end devices communicate exclusively with devices on the wired network and do not communicate with other end devices. For information about configuring the UAP for your network, see Chapter 2, “Installing and Configuring the UAP.”



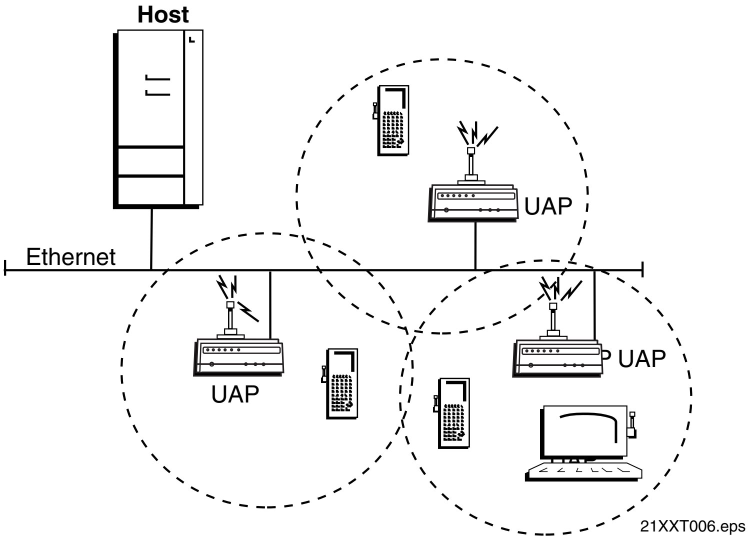
21XXT004.eps

Using Multiple UAPs and Roaming End Devices

For larger or more complex environments, you can install multiple UAPs so that end devices can roam from one UAP to another. When you use multiple UAPs, they establish coverage areas or cells similar to those of a cellular phone network. End devices can connect with any UAP that is within range and that belongs to the same INCA network.

With the UAP multichannel architecture, you can have more than one UAP within the same cell area to increase throughput. In addition, overlapping radio coverage cells offer redundancy for critical applications so that coverage is not lost if a single UAP or radio fails.

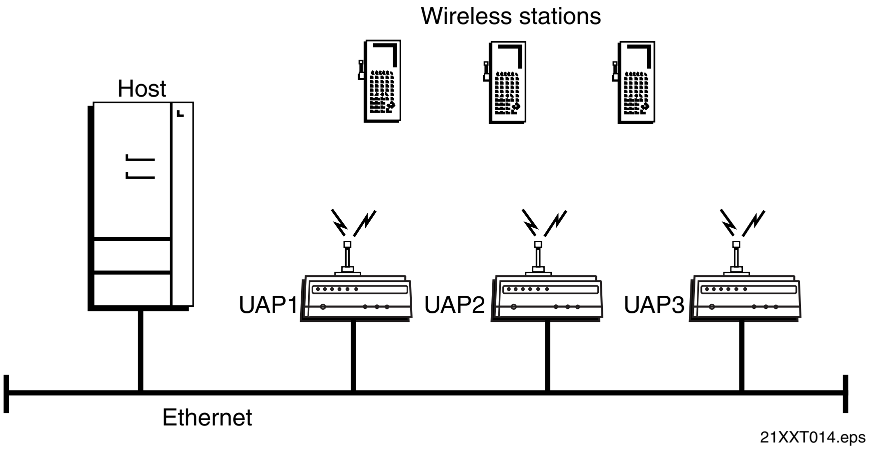
You initially configure the UAP using the serial port. You can then use SNMP, Telnet, or a Web browser to manage them remotely. For information about configuring your UAPs, see “Performing a Standard Installation” in Chapter 2.



Using UAPs with Dual OpenAir Radios for Redundancy

To provide redundancy for your network, you can use UAPs that have two 2.4 GHz OpenAir radios installed. You configure one OpenAir radio as a master to communicate with end devices configured as stations. The second OpenAir radio, configured as a station, provides backup transmission if the Ethernet network goes down.

During normal operations, frames received from end devices are transmitted to the master OpenAir radio in the UAP, which then bridges the frames to the Ethernet network. However, if the Ethernet connection is broken, the master OpenAir radio receives the transmissions from the end devices, and then the station OpenAir radio in the UAP transmits the data to a master OpenAir radio in another UAP.

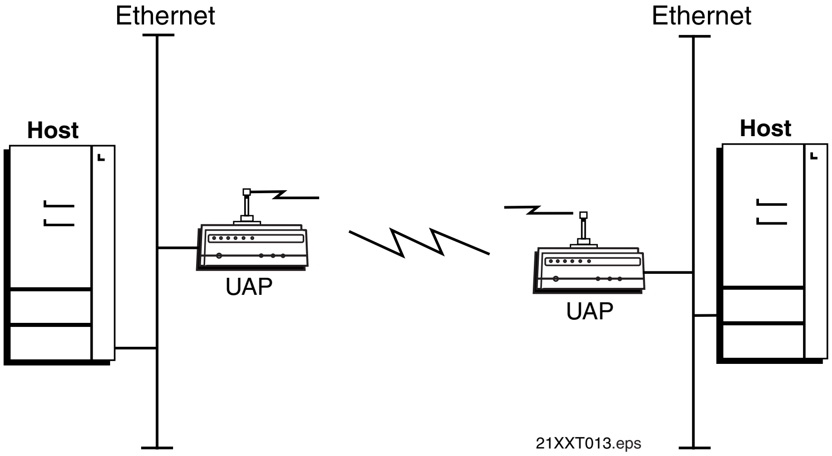


In the above example, UAP3 might be located on a loading dock or other remote location. It has dual OpenAir radios for redundancy. During normal operations, UAP3 functions as a wired bridge, transmitting to and from the host on the Ethernet network. However, if the Ethernet connection is disrupted, UAP3 functions as a wireless access point or repeater, continuing operations using a wireless link to a master OpenAir radio in UAP2.

Note: In the above example, UAP2 must have the Wireless Hops parameter enabled and UAP3 must be within range of UAP2.

Using UAPs as a Point-To-Point Bridge

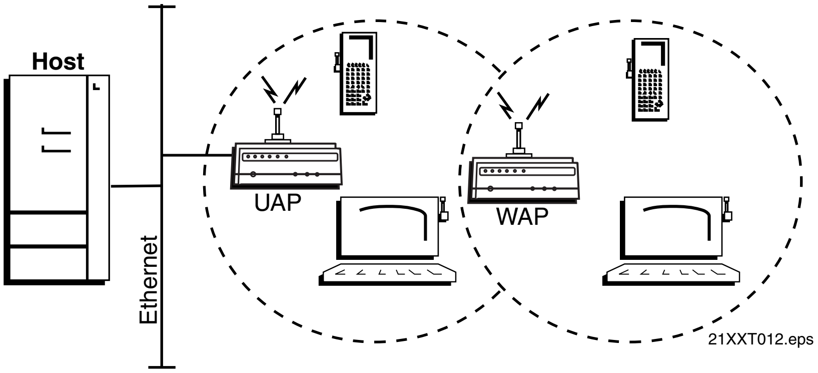
You can use UAPs to create a wireless or point-to-point bridge between two LANs. You can have a UAP wired to a network in one building and have a second UAP wired to a network in another building. Wired and wireless clients in both buildings can then communicate with each other over the wireless bridge created by the UAPs. This configuration is useful in areas where pavement or other obstacles prevent installation of a wired link. For information about configuring UAPs for point-to-point bridging, see “Configuring UAPs for Point-to-Point Bridging” in Chapter 2.



Note: You can configure UAPs for point-to-point bridging if the UAPs that form the bridge each have two 2.4 GHz OpenAir radios or one 900 MHz Falcon radio. Intermec does not support point-to-point functionality using other radio configurations at this time.

Using a UAP as a Repeater

When distance or physical layout impedes radio reception and transmission, you can extend the range of your network by configuring a UAP as a wireless access point or repeater. You can position the WAP in a strategic location so that it receives data from end devices and then forwards the data toward the wired network. No more than two wireless repeaters are allowed for each UAP wired to your network. For information about configuring the UAP as a WAP, see Chapter 3, “Installing and Configuring a Wireless Access Point.”



Note: You can configure the UAP as a repeater if it has two 2.4 GHz OpenAir radios or one 900 MHz radio. Intermec does not support repeater functionality using other radio configurations at this time.

Optimizing Wireless Network Performance

How and where you install your UAP can affect your network performance. This section provides some recommendations for positioning your UAPs and optimizing your network.

General Installation Guidelines

Intermec recommends that you have Intermec or other certified providers conduct a site survey to determine the ideal locations for all of your network components. A proper site survey requires special equipment and training.

The following general practices should be followed in any installation:

- Locate UAPs centrally within areas requiring coverage.
- Overlap UAP coverage areas to avoid coverage holes.
- Try to position the UAP so its LEDs are visible. The LEDs are useful for troubleshooting.
- Install wired LAN cabling within node limit and cable length limitations.
- An uninterruptable power supply is recommended when the AC power system is not reliable.

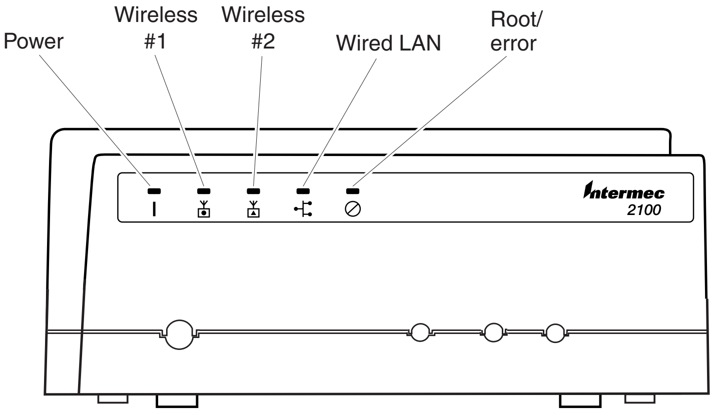
Decreasing Interference

Microwave ovens operate in the same frequency band as a UAP with a 2.4 GHz OpenAir radio. Therefore, if you use a microwave within range of your Intermec RF network, you may notice network performance degradation. However, both your microwave and your RF network will continue to function. For optimal performance, consider locating your microwave oven out of range of your UAP.

If you have a 900 MHz Falcon radio in your UAP, you need to be aware that the 900 MHz radio may experience interference from 900 MHz cordless telephones. For optimal performance, consider operating 900 MHz cordless telephones out of range of your UAP.

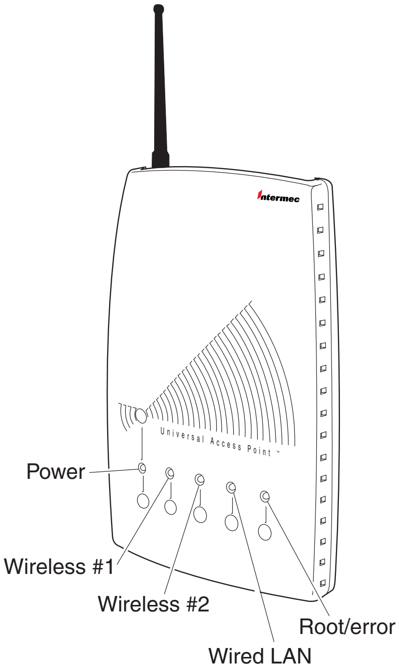
Understanding the LEDs

The UAP has five LEDs. The following illustration identifies the LEDs on the 2100.



21XXT003.eps

The following illustration identifies the LEDs on the 2101.



21XXT018.eps

When you first apply power to the UAP, all LEDs light as the UAP performs a self-test. When the self-test is complete, only the Power LED remains on. If the UAP is configured as the root, the Root/error light flashes. If any other LED remains on after the self-test, an error has occurred. For troubleshooting information, see Chapter 7, “Maintenance and Troubleshooting.”

During normal operation, the LEDs flash on and off as the UAP transmits data. The following table describes each LED.

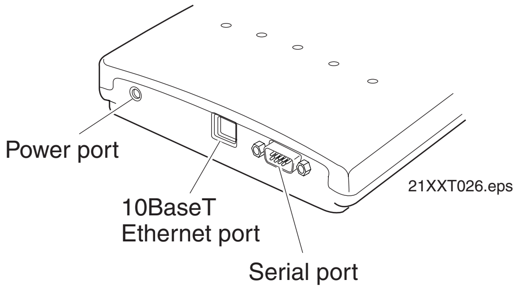
Function	Description
Power	Remains on when power is applied.
Wireless #1	Flashes when a frame is transmitted or received on the radio port for the radio installed in slot 1.
Wireless #2	If the UAP has a second radio installed, this LED flashes when a frame is transmitted or received on the radio port for the radio installed in slot 2.
Wired LAN	Flashes when a frame is transmitted or received on the Ethernet port.
Root/error	Flashes if this device is configured as the root.

Understanding the Connectors

The following table describes the connectors that are on both the 2100 and 2101 UAPs.

Function	Description
Power port	Use the Power port and an appropriate power cable to connect your UAP to an AC power source.
Serial port	Use the Serial port and a null-modem cable to connect the UAP to a terminal or PC to perform the initial configuration.
10BaseT Ethernet port	You can use this port to connect the UAP to your Ethernet network.

The following illustration identifies the connectors on the 2101.



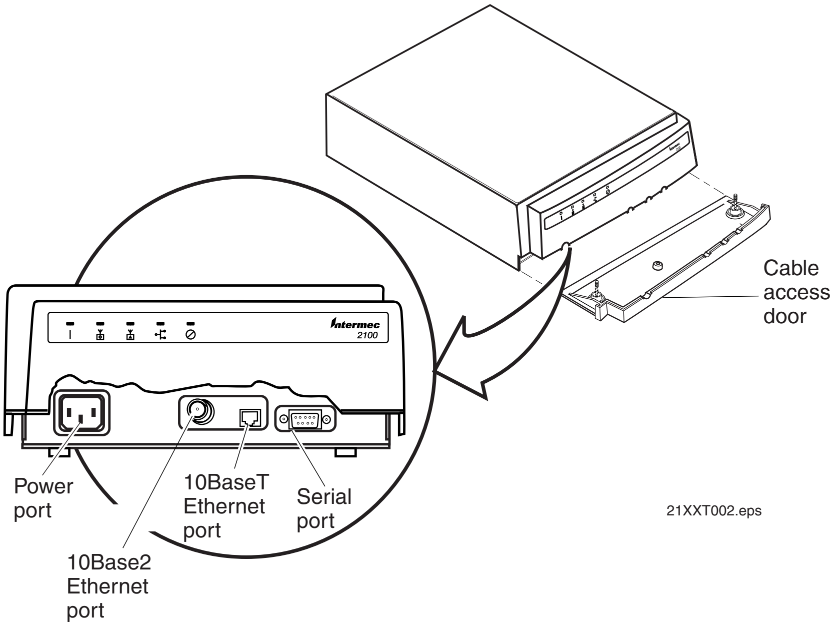
The 2100 also has a 10Base2 Ethernet port connector. You can use either this port or the 10BaseT Ethernet port to connect the 2100 to your Ethernet network.

To access the connectors on the 2100, you must remove the cable access door.

To remove the 2100 cable access door

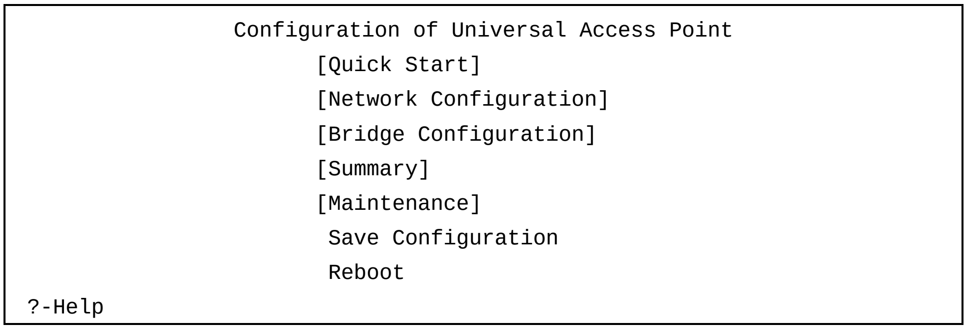
1. Unscrew the two thumbscrews on the cable access door.
2. Slide off the door.

The following illustration identifies the connectors on the 2100.



Navigating Through the Configuration Menus

The UAP features a system of configuration menus that appear on your terminal or PC after you successfully log on. The main menu is shown here. This section explains how to navigate through the configuration menus.



```
                  Configuration of Universal Access Point
                         [Quick Start]
                         [Network Configuration]
                         [Bridge Configuration]
                         [Summary]
                         [Maintenance]
                          Save Configuration
                          Reboot
?-Help
```

Basic Keystrokes

Use these keystrokes to move through the configuration menus.

Key	Action
↑, –	Scroll up through items in a list.
↓, +, =, **Tab**	Scroll down through items in a list.
→, **Enter**, **Spacebar**	Display options or prompt. Also use these keys to select the desired setting.
←, **Esc**	Exit a menu or prompt.
?	Display help.
Esc	Cancel editing or online help.
Enter	Complete editing.

Selecting Menu Options

To select a menu option, position the cursor on the option and press **Enter.** If the option is surrounded by square brackets, you go to another menu. For example, if you select `[Quick Start]` on the main menu and press **Enter,** you go to the Quick Start menu.

Entering a Value in a Dialog Box

If an option has a wide range of possible values, a dialog box appears when you press **Enter.** The dialog box displays the range of values for that option. For instance, the example below displays the range for the IP address field. Type the desired address in the dialog box by entering 4 numbers that range from 0 to 255 and then press **Enter**.

```
Range is:
4 nums 0..255
```

Selecting a Predefined Value

If an option can have one of several predefined values, when you press **Enter** a menu appears listing the predefined values. For instance, when you select IP frame type and press **Enter**, a new menu appears listing DIX and SNAP. Select the frame type you want and press **Enter**.

```
                  [Network Configuration.IP Frame Type]
                        DIX
                        SNAP
?-Help
```

Using Online Help

The 21XX Universal Access Point features online help.

To activate online help

- Hold down the **Shift** key and press the **?** key.

Use the arrow keys to page through online help for each menu item.

To exit online help

- Press **Esc**.

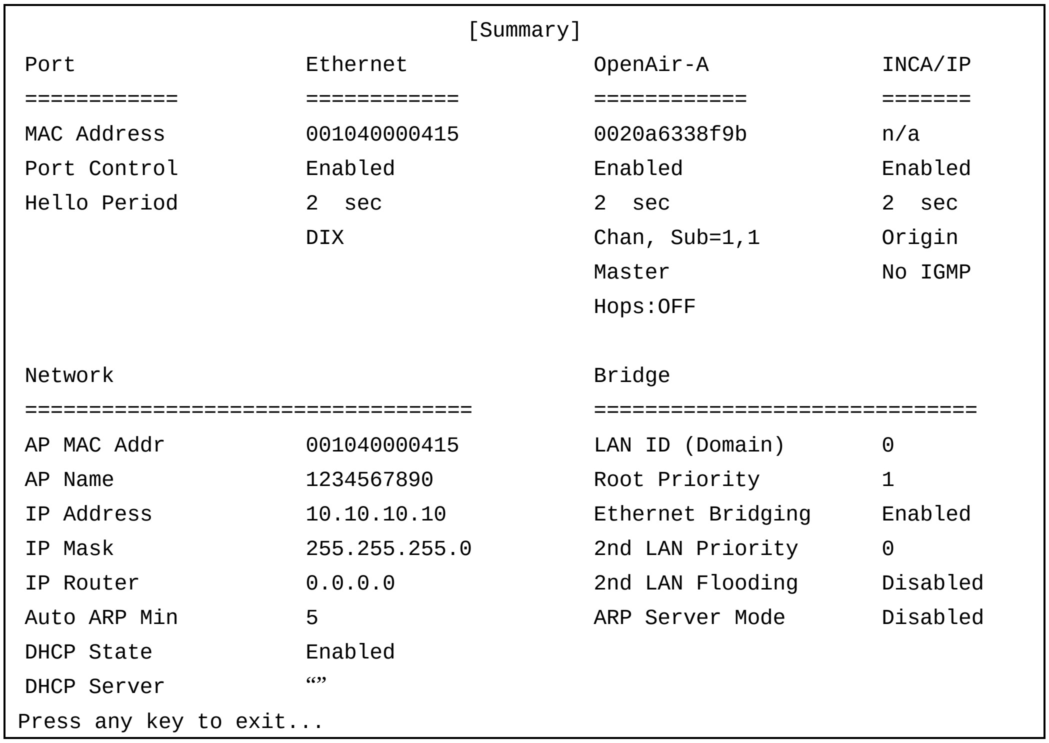
Understanding the Summary Screen

The read-only Summary screen displays the major settings for your UAP. Information on the screen is organized into three main areas:

- Port information is displayed at the top of the screen.
- Network information is displayed on the lower left.
- Bridge information is displayed on the lower right.

Some address strings may be truncated to fit the screen. Your screen will reflect your installed hardware and your UAP settings; therefore, your screen may look different from the example shown here.

Note: If you use DHCP to assign an IP address, the IP address will not appear on the Summary screen. You must refer to the DHCP server to determine the IP address of the UAP.



```
                                   [Summary]
 Port                  Ethernet               OpenAir-A             INCA/IP
 ============          ============           ============          =======
 MAC Address           001040000415           0020a6338f9b          n/a
 Port Control          Enabled                Enabled               Enabled
 Hello Period          2  sec                 2  sec                2  sec
                       DIX                    Chan, Sub=1,1         Origin
                                              Master                No IGMP
                                              Hops:OFF

 Network                                      Bridge
 ===================================          ==============================
 AP MAC Addr           001040000415           LAN ID (Domain)       0
 AP Name               1234567890             Root Priority         1
 IP Address            10.10.10.10            Ethernet Bridging     Enabled
 IP Mask               255.255.255.0          2nd LAN Priority      0
 IP Router             0.0.0.0                2nd LAN Flooding      Disabled
 Auto ARP Min          5                      ARP Server Mode       Disabled
 DHCP State            Enabled
 DHCP Server           “”
Press any key to exit...
```

2

Installing and Configuring the UAP

Installing and Configuring the UAP

2

This chapter describes the system requirements for the UAP. It also provides procedures for performing a quick installation and a standard installation, and it provides an explanation of when you can perform a quick installation. This chapter also includes specific information about configuring UAPs for point-to-point bridging.

System Requirements

You need to provide certain items to install the UAP in your wired network. Additionally, you may need to configure the UAP before you install it. This section describes the items you need to install the UAP, and it provides information to help you determine if you need to configure the UAP before installing it. This section also lists the items you need to perform the configuration.

Installation Requirements

To install a 2100 in your network, you need to provide these items:

- 10BaseT or 10Base2 Ethernet cable
- Power cable
- Antenna or antenna cable

Intermec sells a variety of antennas and power cables. Contact your Intermec representative for information about the power cable or antenna appropriate for your installation.

To install a 2101 in your network, you need to provide:

- 10BaseT Ethernet cable. The 2101 ships with a power cable and an antenna.

Configuration Requirements

You may need to configure the UAP before you install it in your network. If ALL the following conditions are true, you can perform a quick installation and you do not need to configure the UAP before you install it. You can follow the quick installation procedures in the next section if all these conditions are true:

- You have only one UAP on this network.
- You use the default settings. The default values are listed in the section “Default Settings” in Appendix A.
- You do not need to set any filters.
- You do not want to manage the UAP remotely using SNMP, Telnet, or a Web browser.

If the above conditions do not apply to your installation, you need to configure the UAP through the serial port before you install it. To configure and install the UAP, see “Performing a Standard Installation” later in this chapter.

To configure the UAP for your network using the serial port, you need:

- ASCII terminal or PC that is running a terminal emulation program with Y-modem capability
- RS-232 null-modem cable. The cable must have a 9-pin socket connector to connect to the serial port on the UAP. Intermec offers a 9-socket to 9-socket null-modem cable (Part No. 059167) that may be appropriate for your installation.

Performing a Quick Installation

This section describes how to install the UAP in your network when you do not need to configure any network or radio parameters.

CAUTION

Caution
Government regulatory agencies mandate that the antenna not be alterable. Therefore, the access point uses a custom antenna connector. Do not attempt to use a different antenna or you may damage the connector and the access point.

Conseil
Les agences responsables de la réglementation gouvernementale exigent que l'antenne ne soit pas modifiable. Par conséquent, le point d'accès est doté d'un connecteur d'antenne personnalisé. Ne pas essayer d'utiliser une antenne différente au risque d'endommager le connecteur et le point d'accès.

To perform a quick installation

1. Use a clockwise motion to firmly attach an antenna or antenna cable onto the antenna connector on the UAP.
2. If you have a 2100, unscrew the thumbscrews on the cable access door and remove the door.
3. Attach an Ethernet cable to the appropriate Ethernet port.
4. If you have a 2100, plug one end of the power cable into the power port on the 2100.

   If you have a 2101, plug the power cable into the power supply. Plug the power supply into the 2101.
5. If you have a 2100, reinstall the cable access door and tighten the thumbscrews.
6. Mount the UAP, if needed. The 2101 ships with a wall bracket and mounting instructions. Additional mounting brackets are available as accessories for both the 2100 and the 2101. For mounting instructions, see the instruction sheet that shipped with the bracket.
7. Plug the power cable into an AC power outlet. There is no On/Off switch—the UAP turns on as soon as power is applied.

You are ready to begin using your UAP to send packets from your end devices to your wired network. The UAP will use the default parameters listed in the “Default Settings” section in Appendix A.

Performing a Standard Installation

The steps for a standard installation are summarized below. Read this entire section before you configure and install the UAP. Each step is described in detail in the rest of this section. After you configure the UAP, you can manage it using SNMP, Telnet, or a Web browser.

To perform a standard installation

1. Attach the antenna.
2. Connect to the serial port.
3. Apply power.
4. Configure the communications parameters.
5. Log onto the UAP.
6. Configure the network parameters.
7. Mount the UAP.
8. Attach the Ethernet cable.

Attaching an Antenna

The 2101 ships with a dipole antenna. If you are configuring a 2100, or you want to use a different antenna with the 2101, contact your local Intermec representative for information about antenna options. Intermec sells several different antennas, including higher gain and directional antennas. Each of these antennas ships with installation and mounting instructions.

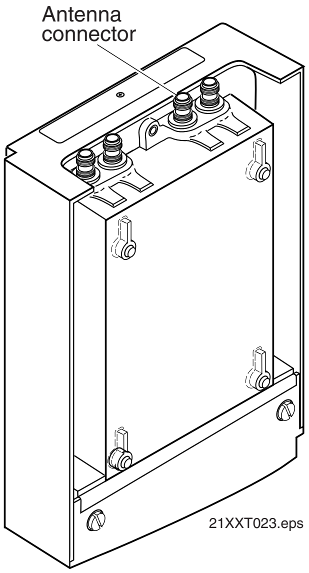
CAUTION

Caution
Government regulatory agencies mandate that the antenna not be alterable. Therefore, the access point uses a custom antenna connector. Do not attempt to use a different antenna or you may damage the connector and the access point.

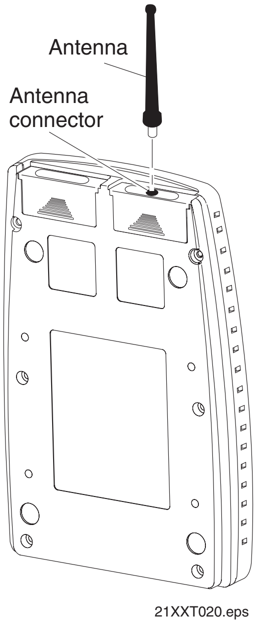
Conseil
Les agences responsables de la réglementation gouvernementale exigent que l’antenne ne soit pas modifiable. Par conséquent, le point d’accès est doté d’un connecteur d’antenne personnalisé. Ne pas essayer d’utiliser une antenne différente au risque d’endommager le connecteur et le point d’accès.

To install the antenna

- Using a clockwise motion, firmly screw the antenna or antenna cable onto the antenna connector on the UAP. The following illustration shows the antenna connector on the 2100.



The following illustration identifies the antenna connector on the 2101.



Connecting to the Serial Port

Use an RS-232 null-modem cable to connect the serial port on the UAP to your ASCII terminal or PC so that you can manually configure the network parameters.

Note: If you use a terminal application that has the option to check for the CD signal before establishing a connection, configure the software to ignore CD.

To connect to the serial port

1. If you have a 2100, unscrew the thumbscrews on the cable access door and then remove the door.
2. Attach one end of a null-modem cable to the serial port on the UAP.
3. Attach the other end of the null-modem cable to the serial port on a PC or a terminal that is powered off.

Applying Power

1. If you have a 2100, plug one end of a power cable into the power port on the UAP.

   If you have a 2101, plug the power cable into the power supply, and then plug the power supply into the 2101.
2. Plug the other end of the power cable into an AC power outlet. The UAP has no On/Off switch, so it boots as soon as you apply power.

The following screen appears on your PC or terminal after the UAP has loaded the UAP Monitor boot code and UAP Program code:

```
UAP Monitor V3.05 March 5, 1999
<Press any key within 5 seconds to enter the UAP monitor>

Executing file UAP.PRG from segment 1.

UAP V3.77 September 1, 1999
<Press any key within 5 seconds to configure the UAP before starting
system>
```

Configuring Communications Parameters

1. Set the serial port terminal communications parameters on your PC to the following values:

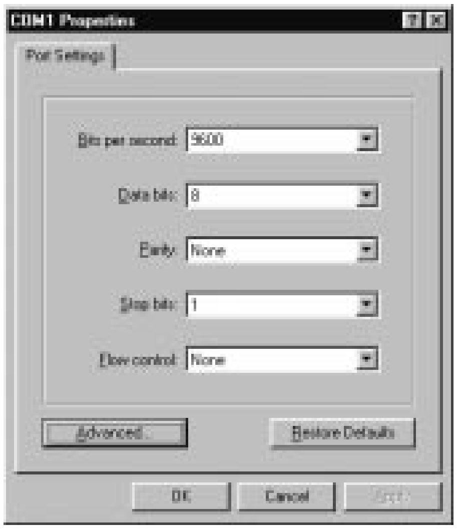
Parameter	Setting
Baud	9600
Data bits	8
Parity	none
Stop bit	1
Flow control	none

2. If you are using a terminal emulation program, choose VT100 as the terminal type.

For information about changing the baud rate of the UAP, see "Using UAP Monitor Commands" in Chapter 8.

To configure the communications parameters using HyperTerminal

1. Open HyperTerminal.
2. From the File menu, choose Properties.
3. From the Phone Number tab, choose Configure. The COM1 Properties dialog box appears.
4. Set the parameters to the values shown here.



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

5. Click OK.

Logging Onto the UAP

There are two ways you can log onto the UAP to configure it:

- You can interrupt the boot process and configure the UAP before it loads the current (default) configuration.
- You can allow the UAP to complete the boot process using the current (default) configuration and then reconfigure it.

To interrupt the boot process and log on

1. When you see the following message on the screen, quickly press any key on the keyboard:

   ```
   Press any key within 5 seconds to configure the UAP before
   starting system
   ```

   The following message appears on the screen:

   ```
   Opening configuration session - please wait...
   ```

   The logon screen appears.

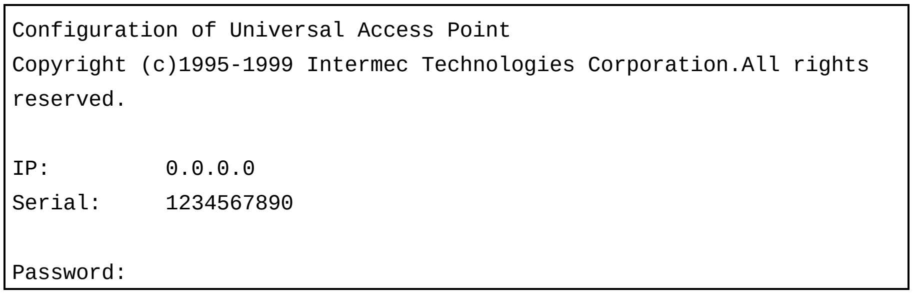
2. Type a password and press **Enter**. The factory default password is `Intermec.`

To log on after the boot process is complete

1. Press **Enter** when the following message appears on the screen:

   ```
   Starting system
   ```

   The logon screen appears.

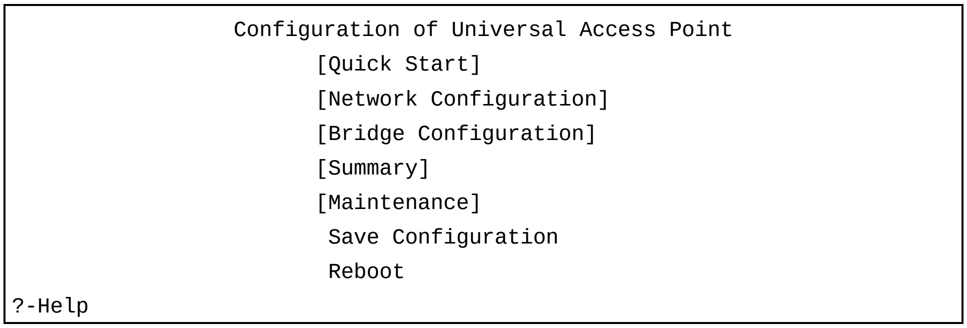


```
Configuration of Universal Access Point
Copyright (c)1995-1999 Intermec Technologies Corporation.All rights
reserved.

IP:         0.0.0.0
Serial:     1234567890

Password:
```

2. Type a password and press **Enter**. The factory default password is `Intermec.`

Configuring Network Parameters

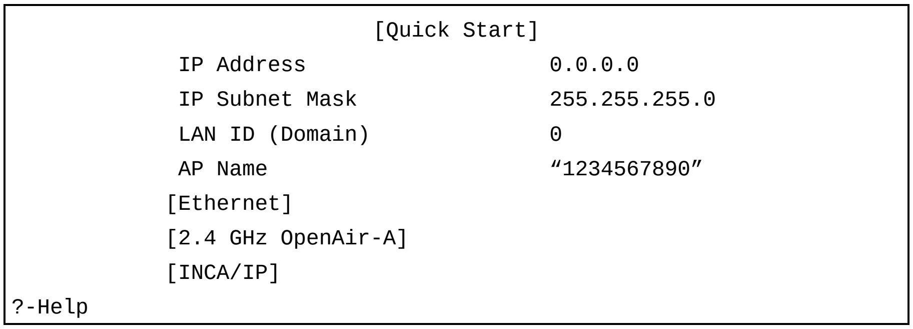
You need to configure the UAP for your network. After you type a valid password and press **Enter**, the Configuration menu appears.



```
                 Configuration of Universal Access Point
                        [Quick Start]
                        [Network Configuration]
                        [Bridge Configuration]
                        [Summary]
                        [Maintenance]
                         Save Configuration
                         Reboot
?-Help
```

To configure network parameters

1. Use the arrow keys or **Tab** key to position on Quick Start and press **Enter**. The Quick Start menu appears.



```
                            [Quick Start]
             IP Address                    0.0.0.0
             IP Subnet Mask                255.255.255.0
             LAN ID (Domain)               0
             AP Name                       “1234567890”
            [Ethernet]
            [2.4 GHz OpenAir-A]
            [INCA/IP]
?-Help
```

2. Configure these parameters using the Quick Start menu:
   - IP Address
   - IP Subnet Mask
   - LAN ID (Domain)

   See “Using the Quick Start Menu” later in this chapter for more information.

3. To configure the radio parameters, choose the radio port from the Quick Start menu and then configure the parameters.

   - If you are using 2.4 GHz OpenAir radios, configure these parameters:

     Channel
     Subchannel
     Node Type
     Security ID

     Additionally, if you are configuring one UAP as a master and a second UAP as a station, you must enable wireless hops in the master UAP. For more information, see “Configuring the 2.4 GHz OpenAir Port” in Chapter 4.

   - If you have a 2100 with a 900 MHz Falcon radio, configure the Mode-Channel parameter. For more information, see “Configuring the 900 MHz Falcon Port” in Chapter 4.

   - If you are using IEEE 802.11 DS radios, configure these parameters:

     Frequency
     Network Name

     For more information, see “Configuring the IEEE 802.11 Direct Sequence Port” in Chapter 4.

4. If you are configuring the UAP as a point-to-point bridge, see “Configuring UAPs for Point-to-Point Bridging” later in this chapter.

5. If the UAP will communicate with devices on the other side of a router, set IP router to the address of the router that will forward frames to another subnet. For more information, see “Using the Network Configuration Menu” later in this chapter.

6. To save your configuration, choose Save Configuration from the Configuration menu and press **Enter**.

You can now mount your UAP and connect it to your Ethernet network.

Mounting the UAP

The 2100 is designed to be placed horizontally on a desk or counter. You can also mount it vertically to a wall or beam using the Intermec mounting bracket kit (Part No. 068918) or the Intermec rotating mounting bracket kit (Part No. 068751). You must mount the UAP in either the horizontal or vertical position to maintain the IP 54 environmental rating.

The 2101 ships with a wall bracket and instructions for mounting the UAP to a wall. Contact your Intermec representative for information about the availability of additional 2101 mounting bracket kits.

To mount the UAP

1. Disconnect the serial and power cables.
2. Mount the UAP. If you are using an Intermec mounting bracket, follow the instructions that came with the bracket.
3. Reconnect the UAP to a power supply.

Connecting to the Ethernet Network

You can connect a 2100 to your Ethernet network using either a 10BaseT or 10Base2 connection. You must use a 10BaseT connection to connect the 2101 to the Ethernet network.

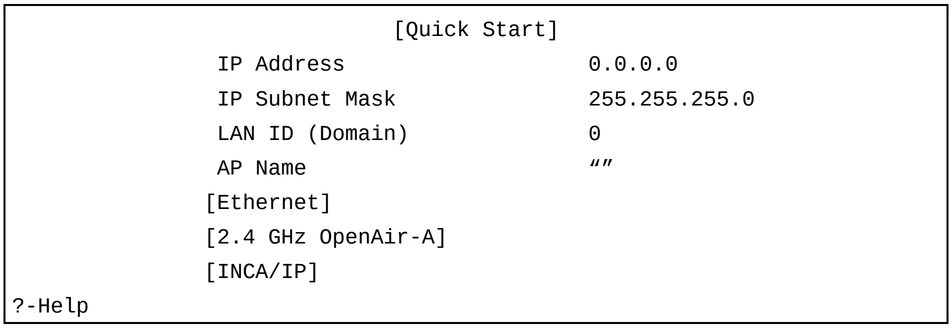
To connect the UAP to an Ethernet network

- If you are using a 10BaseT cable, attach one end of the cable to the 10BaseT port on the UAP and attach the other end to your Ethernet network.

  Or, if you have a 2100, you can attach one end of a 10Base2 cable to the 10Base2 port on the 2100 and attach the other end to your Ethernet network.

Using the Quick Start Menu

You use the Quick Start menu to set basic network parameters. The UAP automatically detects the ports and radio cards installed in it and displays each port on the Quick Start menu. Your Quick Start menu may display different radio options than the example shown here because of the variety of hardware configurations available.



```
                              [Quick Start]
                IP Address                    0.0.0.0
                IP Subnet Mask                255.255.255.0
                LAN ID (Domain)               0
                AP Name                       “”
               [Ethernet]
               [2.4 GHz OpenAir-A]
               [INCA/IP]
?-Help
```

IP Address Each node that communicates with the Ethernet network must have a unique IP address. The IP address is a network level address assigned to each device in a TCP/IP network. The default IP address is 0.0.0.0. The range is 0 to 255. The first number cannot be zero unless all remaining numbers are zero. The first node also cannot be 127 or greater than 223. If the IP address is 0.0.0.0 and DHCP is enabled on the Network Configuration menu, the IP address is obtained via DHCP. If the IP address is 0.0.0.0 and DHCP is disabled, TCP/IP access to this UAP is disabled.

If you are installing this UAP on an existing Ethernet segment, you should allocate the IP address from the same pool as the existing computers on the segment.

If you are installing this UAP as the first device on a new Ethernet segment that is not going to connect to the Internet, try using this Class C address: 192.168.h.h. This Class C network address is reserved by the numbering authority for a company’s internal use. If the Class C address appears on the Internet, routers drop the data. For each UAP in your network, replace the h’s with unique numbers between 0 and 254.

IP Subnet Mask The subnet mask is used in the IP protocol to separate the subnet address from the local IP address. The IP protocol performs a bit-wise AND on the IP address and the subnet mask. For example, if the IP address is 192.168.150.184 and the subnet mask is 255.255.255.0, the subnet address is 192.168.150. The default IP subnet mask is 255.255.255.0.

If this UAP is installed on an existing Ethernet segment, the subnet mask should match the other computers on the segment. If you are using DHCP to obtain an IP address, then the subnet mask that is obtained from DHCP will supersede this one.

If you are using the suggested 192.168.h.h IP address, you should use the subnet mask of 255.255.0.0. This mask provides network 192.168 with space for thousands of devices.

LAN ID (Domain) The LAN ID or domain identifies the INCA spanning tree. All devices in a wireless network must have the same LAN ID. The range is 0 to 254. The default value is 0.

Note: If you assign a LAN ID greater than 15 for an OpenAir radio, the value the UAP uses is the remainder after dividing the LAN ID by 16. For example, the domain is 5 if the LAN ID is 5, 21, or 37.

AP Name You can assign a unique name to identify this UAP in the network. AP name can be from 1 to 16 characters long. The default AP name is the serial number of the UAP.

The AP Name parameter is also used by the OpenAir master to distinguish the radios in this UAP from other radios in the network. Only the first 11 characters are used for the OpenAir master name.

[Ethernet] Choose this menu command to access the Ethernet port configuration menu. See Chapter 4, “Configuring the Ports,” for more information about configuring the Ethernet port.

[2.4 GHz OpenAir-A] This menu command appears if a 2.4 GHz OpenAir radio is installed in the first radio slot in the UAP. Choose this menu command to access the OpenAir port configuration menu. For information about configuring this port, see “Configuring the 2.4 GHz OpenAir Port” in Chapter 4.

[2.4 GHz OpenAir-B] This menu command appears if a 2.4 GHz OpenAir radio is installed in the second radio slot in the UAP. Choose this menu command to access the OpenAir port configuration menu. For information about configuring this port, see “Configuring the 2.4 GHz OpenAir Port” in Chapter 4.

[900 MHz] This menu command appears if a 900 MHz Falcon radio is installed in the UAP. Choose this menu command to access the 900 MHz Falcon port configuration menu. For information about configuring this port, see “Configuring the 900 MHz Falcon Port” in Chapter 4.

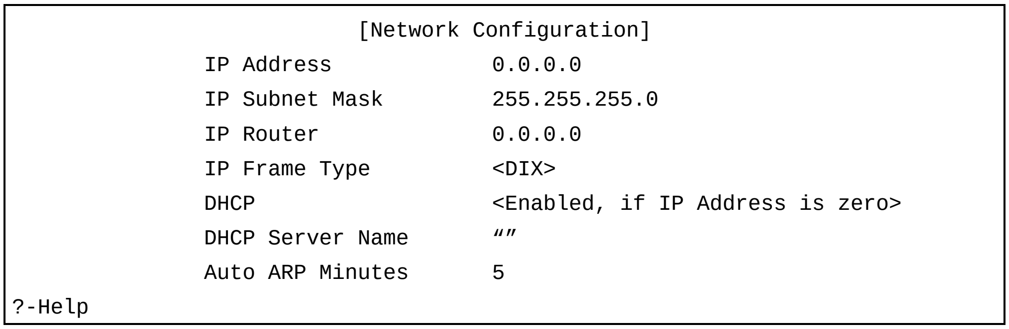
[UHF-A] This menu command appears if a UHF radio is installed in the UAP. Choose this menu command to access the UHF port configuration menu. For information about configuring this port, see “Configuring the UHF Port” in Chapter 4.

[IEEE 802.11 DS-A] This menu command appears if an IEEE 802.11 DS radio is installed in your UAP. Choose this menu command to access the IEEE 802.11 DS port configuration menu. For information about configuring this port, see “Configuring the IEEE 802.11 Direct Sequence Port” in Chapter 4.

[INCA/IP] Choose this menu command to access the INCA/IP port configuration menu. For information about configuring this port, see “Configuring the INCA/IP Port” in Chapter 4.

Using the Network Configuration Menu

You use the Network Configuration menu to configure the UAP for your network. If you have more than one UAP on your network, each UAP must have a unique address configuration.



```
                            [Network Configuration]
               IP Address            0.0.0.0
               IP Subnet Mask        255.255.255.0
               IP Router             0.0.0.0
               IP Frame Type         <DIX>
               DHCP                  <Enabled, if IP Address is zero>
               DHCP Server Name      “”
               Auto ARP Minutes      5
?-Help
```

IP Address Each node that communicates with the Ethernet network must have a unique IP address. The IP address is a network level address assigned to each device in a TCP/IP network. The default IP address is 0.0.0.0. The range is 0 to 255. The first number cannot be zero unless all remaining numbers are zero. The first node also cannot be 127 or greater than 223. If the IP address is 0.0.0.0 and DHCP is enabled, the IP address is obtained via DHCP. If the IP address is 0.0.0.0 and DHCP is disabled, TCP/IP access to this UAP is disabled.

If you are installing this UAP on an existing Ethernet segment, you should allocate the IP address from the same pool as the existing computers on the segment.

If you are installing this UAP as the first device on a new Ethernet segment that is not going to connect to the Internet, try using this Class C address: 192.168.h.h. This Class C network address is reserved by the numbering authority for a company’s internal use. If the Class C address appears on the Internet, routers drop the data. For each UAP in your network, replace the h’s with unique numbers between 0 and 254.

IP Subnet Mask The subnet mask is used in the IP protocol to separate the subnet address from the local IP address. The IP protocol performs a bit-wise AND on the IP address and the subnet mask. For example, if the IP address is 192.168.150.184 and the subnet mask is 255.255.255.0, the subnet address is 192.168.150. The default IP subnet mask is 255.255.255.0.

If this UAP is installed on an existing Ethernet segment, the subnet mask should match the other computers on the segment. If you are using DHCP to obtain an IP address, then the subnet mask that is obtained from DHCP will supersede this one.

If you are using the suggested 192.168.h.h IP address, you should use the subnet mask of 255.255.0.0. This mask provides network 192.168 with space for thousands of devices.

IP Router This parameter identifies the address of the default router that the UAP uses to route packets to other subnets or networks. The range is 4 numbers from 0 to 255. The first number cannot be zero unless all remaining numbers are zero. The first node also cannot be 127 or greater than 223. The default is 0.0.0.0, which disables the ability of this subnet to exchange TCP/IP traffic with another subnet or network. If you are using DHCP to obtain an IP address, and a DHCP server specifies a default IP router, then the DHCP specification will supersede the value you set in this field.

IP routers are typically configured so that the UAP only needs to know the address of one router even if there are several routers on the segment connecting to several other segments. If the subnet mask is 255.255.0.0, for example, a router that connects subnet 1 to subnet 2 might have the address 172.16.8.1 on subnet 1 and 172.16.16.1 on subnet 2. A host with IP address 172.16.16.5 would specify an IP router address of 172.16.16.1 to reach host 172.16.8.10.

The UAP dynamically creates a new IP route table entry whenever it receives an Internet Control Message Protocol (ICMP) redirect packet. For example, a default router may return an ICMP redirect packet to a UAP when it receives an IP packet from the UAP and there is a preferred router for the target destination.

IP Frame Type This parameter indicates the type of frame that contains IP traffic. The type can be either DIX or SNAP. DIX frames are also known as Ethernet v2.0 frames. You typically use DIX frames for TCP/IP over an Ethernet network. If other computers on your network use RFC1042 SNAP encapsulation for IP frames, then select SNAP frame type. The default is DIX.

DHCP The UAP has DHCP client support so that it can automatically accept IP addresses from a DHCP or BOOTP server on the network. Preference is given to DHCP servers. If a BOOTP reply arrives at the UAP before any DHCP offers are received, the UAP waits an additional 4 seconds for a DHCP offer before responding. If a DHCP offer is received within the 4-second period, the BOOTP reply is ignored and the DHCP offer is accepted.

The DHCP settings are:

Enabled	This setting allows you to enable DHCP without setting the IP address to 0.0.0.0. If DHCP is enabled, the UAP will accept addresses from the DHCP server. You may find this setting helpful when troubleshooting your network.
Enabled, if IP address is zero	You must set IP address to 0.0.0.0 to enable DHCP. DHCP will then assign the IP address, subnet mask, and default router.
Disabled	DHCP not used.

DHCP Server Name This parameter identifies the network server that the UAP accesses for automatic address assignment for IP address, IP subnet mask, and IP router values. The UAP only responds to address offer messages from the DHCP or BOOTP server specified. If no DHCP server name is specified, the client responds to offers from any server.

DHCP server name can be 0 to 31 characters. The name prevents the UAP from inadvertently obtaining an IP configuration from other servers on the network. The class identifier string for the UAP is “ ” (blank). Servers use this string to identify the UAP.

When the UAP responds to a DHCP or BOOTP server, it broadcasts a single ARP request to the address offered. If no ARP response is received within 3 seconds, the UAP assumes the IP address is unique and completes the negotiation for that address. If an ARP reply is received before the timeout, the UAP assumes the address is a duplicate and declines the offer.

An address offer from a BOOTP server is treated as if it were an infinite lease from a DHCP server. See “Leases” later in this section for more information.

Auto ARP Minutes The UAP periodically sends an unsolicited ARP request so that routers can update their routing tables. The request enables a network management platform to learn about the UAP on the network by querying routers. The auto ARP period controls the time interval between ARP broadcasts. The range is from 1 to 120 minutes. The default is 5 minutes. A setting of 0 disables this parameter.

If the address of the default router is 0.0.0.0, the UAP sends an ARP request to its own IP address; otherwise, it sends an ARP request to the default router. Without this option, a UAP might not use its IP address for extended periods of time and the IP address expires from the router ARP table. If the IP address expires, the network management program needs to ping all potential addresses on a subnet to locate active IP addresses, or require the user to enter a list. You should not allow the IP address for the UAP to expire.

Leases

A DHCP server may issue a finite or renewable lease to an IP address. If the lease expires and is not renewed, the client must stop using the IP address.

A DHCP server may also be configured to grant an infinite lease or permanent address assignment to the UAP. The UAP recognizes an infinite lease as a special case. The UAP stores the IP address, subnet mask, and default router in non-volatile memory and then disables DHCP. These settings are maintained if the UAP is powered off or rebooted. To force the UAP to use DHCP the next time it boots, reset IP address to 0.0.0.0 or set DHCP to enabled.

If you are using INCA/IP tunneling and you are using DHCP to allocate IP addresses to root candidates or designated bridges, you must obtain a permanent lease and you must reboot the UAP after obtaining an address.

Configuring UAPs for Point-to-Point Bridging

A point-to-point or wireless bridge connects two wired Ethernet segments. A wireless bridge is an ideal way to connect two networks when pavement or other physical features present an obstacle to running cable. You configure a UAP in each wired network so that the UAPs create a wireless bridge that allows devices in both networks to communicate across the bridge.

You can create a wireless bridge using UAPs configured with these radios:

- 2.4 GHz OpenAir
- 900 MHz Falcon

Note: UAPs with IEEE 802.11 DS radios or UHF radios do not support point-to-point bridging.

Regardless of the type of radio you are using, both UAPs in a wireless bridge configuration must have the same LAN ID. The UAPs use LAN ID to form the INCA spanning tree.

You may need to adjust the Global Flooding parameters for wireless bridging. Here are some considerations for configuring the Global Flooding parameters for a point-to-point bridge:

- If all gateways and servers are on the primary LAN, use the Multicast Flood Mode default parameter of hierarchical.
- If end devices must communicate with gateways or servers on a secondary LAN, set the Multicast Flood Mode parameter to universal.
- If end devices on a secondary LAN communicate with end devices on another secondary LAN, set the Multicast Flood Mode parameter to universal.

You configure the Global Flooding parameters from the Bridge Configuration menu. For more information, see Chapter 5, “Configuring the Bridging Parameters.”

Configuring 2.4 GHz OpenAir UAPs for Point-to-Point Bridging

If you are using 2.4 GHz OpenAir radios for wireless bridging, you need to configure one UAP as a master, and configure the second UAP as a station.

For wireless bridging, both 2.4 GHz OpenAir radios must have the same:

- LAN ID
- Security ID
- Channel
- Subchannel

The following table provides an example of how to configure 2.4 GHz OpenAir UAPs for a point-to-point or wireless bridge.

Parameter	UAP on Primary LAN	UAP on Secondary LAN
LAN ID	1	1
Root Priority	5	0
Secondary LAN Bridge Priority	0	5
Secondary LAN Flooding	Disabled	Disabled
Node Type	Master	Station
Channel	1	1
Subchannel	1	1
Wireless Hops	Enabled	(does not apply)

Note: Make sure the root priority of the 2.4 GHz OpenAir master is greater than the root priority of the 2.4 GHz OpenAir station. The devices will not form the desired wireless bridge if the master has a lower root priority than the station.

Configuring 900 MHz Falcon UAPs for Point-to-Point Bridging

To configure the 900 MHz Falcon UAPs as a wireless bridge, you need to configure the radios in each UAP with the same LAN ID. You also need to set parameters that determine bridge priority.

The following table provides an example of how to configure 900 MHz Falcon UAPs for a point-to-point or wireless bridge.

Parameter	UAP on Primary LAN	UAP on Secondary LAN
LAN ID	1	1
Root Priority	5	0
Secondary LAN Bridge Priority	0	5
Secondary LAN Flooding	Disabled	Disabled

Note: You can position your 900 MHz Falcon UAPs at least 15.24 meters (50 feet) apart. Positioning your UAPs closer than 15.24 meters will not increase throughput, but may provide redundancy.

3

Installing and Configuring a Wireless Access Point

This chapter describes how to install and configure the 21XX Universal Access Point as a repeater or Wireless Access Point (WAP).

Installation Requirements

You need these items to install and configure a WAP in your network:

- ASCII terminal or PC that is running a terminal emulation program with Y-modem capability
- RS-232 null-modem cable that has a 9-pin socket connector on one end

If you are configuring a 2100, you also need to provide these items:

- Power cable
- Antenna or antenna cable

Intermec offers a variety of cables and antennas, including a 9-socket to 9-socket null-modem cable (Part No. 059167) that may be appropriate for your installation. Contact your Intermec representative for additional information.

Note: You can configure any 21XX Universal Access Point as a wireless access point if it has either two 2.4 GHz OpenAir radios or one 900 MHz Falcon radio. Intermec does not support an IEEE 802.11 DS or UHF wireless access point at this time. The 2110 Wireless Access Point is no longer available.

Intermec recommends that you install no more than two WAPs for each UAP.

Installing the WAP

You must configure the WAP before you install it. You can then manage it using SNMP, Telnet, or a Web browser. You should read this entire section before you install the WAP. The steps for installing the WAP are summarized here. Each step is described in detail in the rest of this section.

To install the WAP

1. Attach the antenna.
2. Connect to the serial port.
3. Apply power.
4. Configure the communications parameters.
5. Log onto the WAP.
6. Configure the WAP.
7. Mount the WAP.

Attaching an Antenna

The 2101 ships with a dipole antenna. If you are configuring a 2100, or you want to use a different antenna with the 2101, contact your local Intermec representative for information about antenna options. Intermec sells several different antennas, including higher gain and directional antennas. Each of these antennas ships with installation and mounting instructions.

Caution
Government regulatory agencies mandate that the antenna not be alterable. Therefore, the access point uses a custom antenna connector. Do not attempt to use a different antenna or you may damage the connector and the access point.

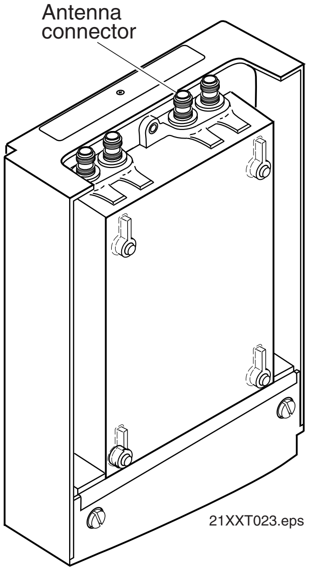
Conseil
Les agences responsables de la réglementation gouvernementale exigent que l'antenne ne soit pas modifiable. Par conséquent, le point d'accès est doté d'un connecteur d'antenne personnalisé. Ne pas essayer d'utiliser une antenne différente au risque d'endommager le connecteur et le point d'accès.

To install the antenna

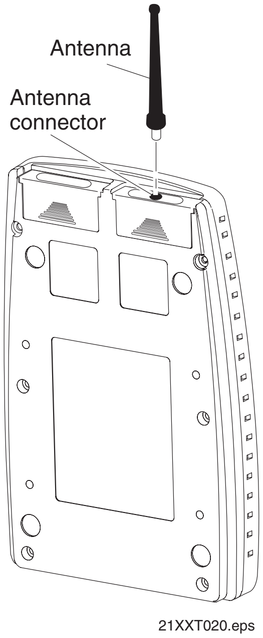
- Using a clockwise motion, firmly screw the antenna or antenna cable onto the antenna connector on the WAP.

  If you have a WAP with 2.4 GHz OpenAir radios, you need to attach one antenna cable for each radio. For specific information about antenna placement, see "Positioning the Antennas for a 2.4 GHz OpenAir WAP" in Appendix C.

The following illustration identifies the antenna connector on the 2100.



The following illustration identifies the antenna connector on the 2101.



Connecting to the Serial Port

Use an RS-232 null-modem cable to connect the serial port on the WAP to your ASCII terminal or PC so that you can manually configure the network parameters.

Note: If you use a terminal application that has the option to check for the CD signal before establishing a connection, configure the software to ignore CD.

To connect to the serial port

1. If you have a 2100, unscrew the thumbscrews on the cable access door, and then remove the door.
2. Attach one end of a null-modem cable to the serial port on the WAP.
3. Attach the other end of the null-modem cable to the serial port on a PC or a terminal that is powered off.

Applying Power

1. If you have a 2100, plug one end of a power cable into the power port on the 2100.

   If you have a 2101, plug the power cable into the power supply, and then plug the power supply into the power port on the 2101.
2. Plug the other end of the power cable into an AC power source. The WAP has no On/Off switch, so it boots as soon as you apply power.

The following screen appears on your PC or terminal after the WAP has loaded the UAP Monitor boot code and the UAP Program code:

```
UAP Monitor V3.05 March 5, 1999
<Press any key within 5 seconds to enter the UAP monitor>

Executing file UAP.PRG from segment 1.

UAP V3.77 September 1, 1999
<Press any key within 5 seconds to configure the UAP before starting
system>
```

Configuring Communications Parameters

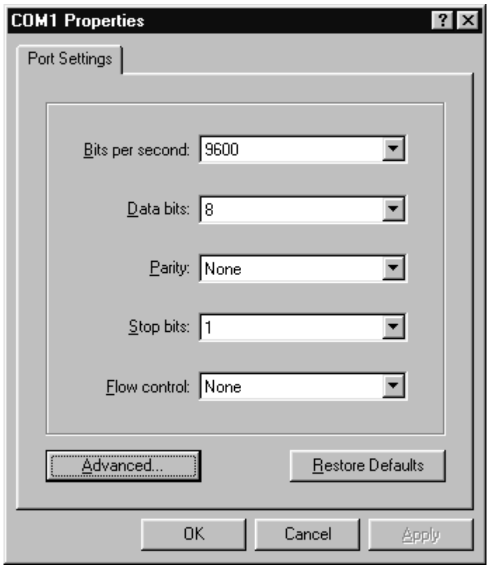
1. Set the serial port terminal communications parameters on your PC to the following values:

Parameter	Setting
Baud	9600
Data bits	8
Parity	none
Stop bit	1
Flow control	none

2. If you are using a terminal emulation program, choose VT100 as the terminal type.

To configure the communications parameters using HyperTerminal

1. Open HyperTerminal.
2. From the File menu, choose Properties.
3. Choose Configure. The COM1 Properties dialog box appears.
4. Set the parameters to the values shown here.



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

5. Click OK.

Logging Onto the WAP

There are two ways you can log onto the WAP to configure it:

- You can interrupt the boot process and configure the WAP before it loads the current (default) configuration.
- You can allow the WAP to complete the boot process using the current (default) configuration and then reconfigure it.

To interrupt the boot process and log on

1. When you see the following message on the screen, quickly press any key on the keyboard:

   ```
   Press any key within 5 seconds to configure the UAP before
   starting system
   ```

   The following message appears on the screen:

   ```
   Opening configuration session - please wait...
   ```

   The logon screen appears.

2. Type a password and press **Enter**. The factory default password is `Intermec.`

To log on after the boot process is complete

1. Press **Enter** when the following message appears on the screen:

   ```
   Starting system
   ```

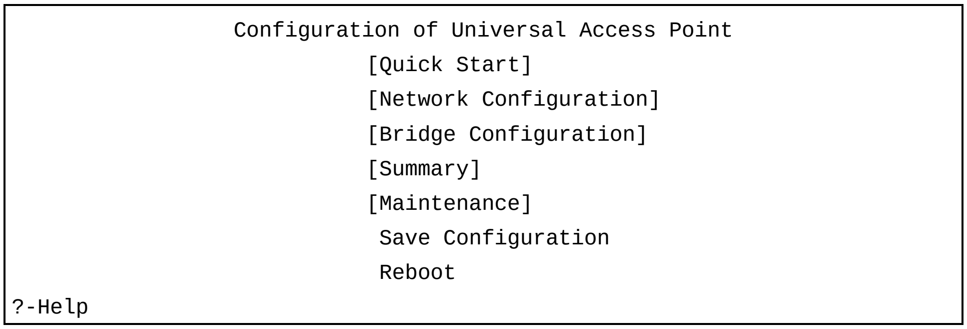
   The logon screen appears.

```
Configuration of Universal Access Point
Copyright (c)1995-1999 Intermec Technologies Corporation.All rights
reserved.

IP:         0.0.0.0
Serial:     1234567890

Password:
```

2. Type a password and press **Enter**. The factory default password is `Intermec.`

Configuring the WAP

The Configuration menu appears after you successfully log onto the WAP.



```
                  Configuration of Universal Access Point
                             [Quick Start]
                             [Network Configuration]
                             [Bridge Configuration]
                             [Summary]
                             [Maintenance]
                              Save Configuration
                              Reboot
?-Help
```

To configure the WAP

1. Configure the parameters for your network.
   - If you have a 2.4 GHz WAP, see “Configuring the 2.4 GHz OpenAir WAP” later in this chapter.
   - If you have a 900 MHz Falcon WAP, see “Configuring the 900 MHz Falcon WAP” later in the chapter.
2. On the Bridge Configuration menu, set the Root Priority parameter to 0 so the WAP will not become the root. For more information, see Chapter 5, “Configuring the Bridging Parameters.”
3. To save your configuration, choose Save Configuration from the Configuration menu and press **Enter.**
4. To reboot the WAP using the new configuration, choose Reboot from the Configuration menu and press **Enter**.

Mounting the WAP

The 2100 is designed to be placed horizontally on a desk or counter. You can also mount it vertically to a wall or beam using the Intermec mounting bracket kit (Part No. 068918) or the Intermec rotating mounting bracket kit (Part No. 068751). To maintain the IP 54 environmental rating, you must mount the 2100 in either the horizontal or vertical position.

The 2101 ships with a wall bracket and instructions for mounting the 2101 to a wall. Contact your Intermec representative for information about the availability of additional 2101 mounting bracket kits.

To mount the WAP

1. Disconnect the serial and power cables.
2. Mount the WAP. If you are using an Intermec mounting bracket, follow the instructions that came with the bracket.
3. Reconnect the WAP to a power source.

Configuring the 2.4 GHz OpenAir WAP

If you are using a 2.4 GHz OpenAir WAP, you configure one radio in the WAP as a station and the other radio as a master. The master radio communicates with end devices that are configured as stations, and the station radio communicates with a 2.4 GHz radio in a UAP that is configured as a master and wired to the Ethernet network.

For a station to communicate with a master, the station and master must have the same:

- LAN ID (Domain)
- Security ID
- Channel
- Subchannel

Here is an example of how you might configure the radio in the UAP on the Ethernet network and the two radios in the WAP. In this example, the OpenAir-B radio in the WAP is configured as a station and has the same channel and subchannel as the OpenAir-A radio in the UAP on the Ethernet network, so the radios can communicate. You need to configure your end devices to communicate with the OpenAir-A master radio in the WAP.

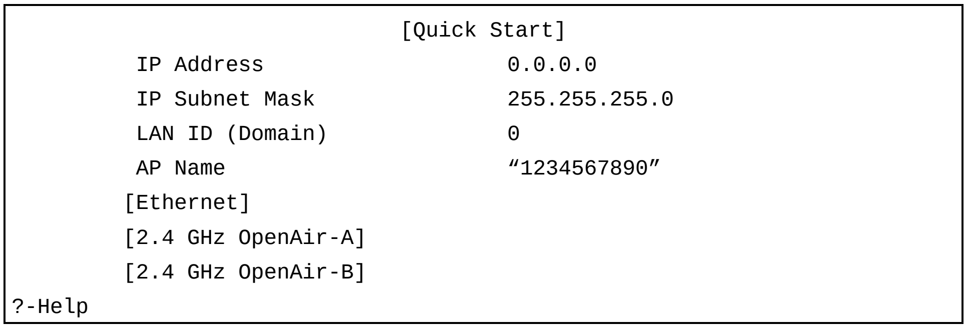
Parameter	UAP OpenAir-A	WAP OpenAir-A (WAP)	WAP OpenAir-B (WAP)
LAN ID	0	0	0
Security ID	(null)	(null)	(null)
Node Type	Master	Master	Station
Channel	1	2	1
Subchannel	1	2	1
Wireless Hops	Enabled	Disabled	(does not apply)

You use the Quick Start menu to set basic network parameters, including LAN ID. Use the 2.4 GHz OpenAir menu for a specific radio to configure security ID, node type, channel, subchannel, and wireless hops.

Note: If you are installing an OpenAir WAP in a network that has existing UAPs with Release 1.0 firmware, you must upgrade the boot and program code in the existing UAPs. Contact your Intermec representative for information on obtaining the latest firmware. For information on upgrading UAPs, see Appendix D, "Upgrading the UAP."

Using the Quick Start Menu

You use the Quick Start menu to set basic network parameters. The Quick Start menu for an OpenAir WAP is shown here.



```
                              [Quick Start]
          IP Address                    0.0.0.0
          IP Subnet Mask                255.255.255.0
          LAN ID (Domain)               0
          AP Name                       “1234567890”
         [Ethernet]
         [2.4 GHz OpenAir-A]
         [2.4 GHz OpenAir-B]
?-Help
```

You need to configure these parameters using the Quick Start menu:

- IP Address
- IP Subnet Mask
- LAN ID (Domain)

The Quick Start parameters are described below.

IP Address Each node that communicates with the Ethernet network must have a unique IP address. The IP address is a network level address assigned to each device in a TCP/IP network. The default IP address is 0.0.0.0. The range is 0 to 255. The first number cannot be zero unless all remaining numbers are zero. The first node also cannot be 127 or greater than 223. If the IP address is 0.0.0.0 and DHCP is enabled on the Network Configuration menu, the IP address is obtained via DHCP. If the IP address is 0.0.0.0 and DHCP is disabled, TCP/IP access to this UAP is disabled.

IP Subnet Mask The subnet mask is used in the IP protocol to separate the subnet address from the local IP address. The IP protocol performs a bit-wise AND on the IP address and the subnet mask. For example, if the IP address is 192.168.150.184 and the subnet mask is 255.255.255.0, the subnet address is 192.168.150. The default IP subnet mask is 255.255.255.0.

If this WAP is installed on an existing segment, the subnet mask should match the other computers on the segment. If you are using DHCP to obtain an IP address, then the subnet mask that is obtained from DHCP will supersede this one.

If you are using the suggested 192.168.h.h IP address, you should use the subnet mask of 255.255.0.0. This mask provides network 192.168 with space for thousands of devices.

LAN ID (Domain) The LAN ID or domain identifies the INCA spanning tree. All devices in a wireless network must have the same LAN ID. The range is 0 to 254. The default value is 0.

Note: If you assign a LAN ID greater than 15 for an OpenAir radio, the value the WAP uses is the remainder after dividing the LAN ID by 16. For example, the domain is 5 if the LAN ID is 5, 21, or 37.

AP Name You can assign a unique name to identify this WAP in the network. AP name can be from 1 to 16 characters long. The default AP name is the serial number of the WAP.

AP name is also used by the OpenAir master to distinguish the radios in this unit from other radios in the network. Only the first 11 characters are used for the OpenAir master name.

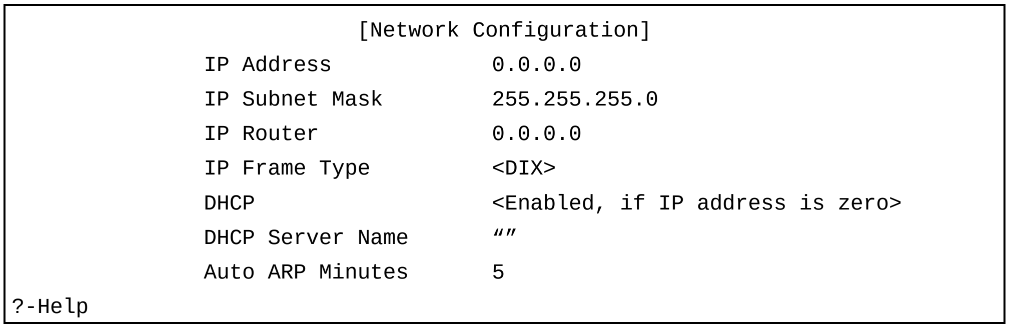
[Ethernet] You need to select this command and then disable port control so your UAP functions as a wireless device.

[2.4 GHz OpenAir-A] Select this command to configure OpenAir radio A in your WAP.

[2.4 GHz OpenAir-B] Select this command to configure OpenAir radio B in your WAP.

Using the Network Configuration Menu

If your WAP will communicate with devices on the other side of a router, you must set the IP address of the router that will forward data frames to addresses on another subnet. Use the Network Configuration menu to configure the IP router.



```
                            [Network Configuration]
               IP Address             0.0.0.0
               IP Subnet Mask         255.255.255.0
               IP Router              0.0.0.0
               IP Frame Type          <DIX>
               DHCP                   <Enabled, if IP address is zero>
               DHCP Server Name       “”
               Auto ARP Minutes       5
?-Help
```

IP Address Each node that communicates with the Ethernet network must have a unique IP address. The IP address is a network level address assigned to each device in a TCP/IP network. The default IP address is 0.0.0.0. The range is 0 to 255. The first number cannot be zero unless all remaining numbers are zero. The first node also cannot be 127 or greater than 223. If the IP address is 0.0.0.0 and DHCP is enabled, the IP address is obtained via DHCP. If the IP address is 0.0.0.0 and DHCP is disabled, TCP/IP access to this UAP is disabled.

IP Subnet Mask The subnet mask is used in the IP protocol to separate the subnet address from the local IP address. The IP protocol performs a bit-wise AND on the IP address and the subnet mask. For example, if the IP address is 192.168.150.184 and the subnet mask is 255.255.255.0, the subnet address is 192.168.150. The default IP subnet mask is 255.255.255.0.

If this WAP is installed on an existing segment, the subnet mask should match the other computers on the segment. If you are using DHCP to obtain an IP address, then the subnet mask that is obtained from DHCP will supersede this one.

If you are using the suggested 192.168.h.h IP address, you should use the subnet mask of 255.255.0.0. This mask provides network 192.168 with space for thousands of devices.

IP Router This parameter identifies the address of the default router that the WAP uses to route packets to other subnets or networks. The range is 4 numbers from 0 to 255. The first number cannot be zero unless all remaining numbers are zero. The first node also cannot be 127 or greater than 223. The default is 0.0.0.0, which disables the ability of this subnet to exchange TCP/IP traffic with another subnet or network. If you are using DHCP to obtain an IP address for this WAP, and a DHCP server specifies a default IP router, then the DHCP specification will supersede the value you set in this field.

IP routers are typically configured so that the WAP only needs to know the address of one router even if there are several routers on the segment connecting to several other segments. If the subnet mask is 255.255.255.0, for example, a router that connects subnet 1 to subnet 2 might have the address 172.16.8.1 on subnet 1 and 172.16.16.1 on subnet 2. A host with IP address 172.16.16.5 would specify an IP router address of 172.16.16.1 to reach host 172.16.8.10.

The WAP dynamically creates a new IP route table entry whenever it receives an Internet Control Message Protocol (ICMP) redirect packet. For example, a default router may return an ICMP redirect packet to a WAP when it receives an IP packet from the WAP and there is a preferred router for the target destination.

IP Frame Type This parameter indicates the type of frame that contains IP traffic. The type can be either DIX or SNAP. DIX frames are also known as Ethernet v2.0 frames. You typically use DIX frames for TCP/IP over an Ethernet network. If other computers on your network use RFC1042 SNAP encapsulation for IP frames, then select SNAP frame type. The default is DIX.

DHCP The WAP has DHCP client support so that it can automatically accept IP addresses from a DHCP or BOOTP server on the network. Using DHCP simplifies installation of IP devices because it eliminates the manual entry of the IP address, IP subnet mask, and IP router addresses on every device.

The WAP responds to both DHCP and BOOTP servers; however, preference is given to DHCP servers. If a BOOTP reply arrives at the WAP before any DHCP offers are received, the WAP waits an additional 4 seconds for a DHCP offer before responding. If a DHCP offer is received within the 4-second period, the BOOTP reply is ignored and the DHCP offer is accepted.

The DHCP settings are:

Enabled	This setting allows you to enable DHCP without setting IP address to 0.0.0.0. If DHCP is enabled, the UAP will accept addresses from the DHCP server. You may find this setting helpful when troubleshooting your network.
Enabled, if IP address is zero	You must set IP address to 0.0.0.0 to enable DHCP. DHCP will then assign IP address, IP subnet mask, and IP router addresses.
Disabled	DHCP not used.

DHCP Server Name The DHCP server name identifies the network server that the WAP accesses for automatic assignment of IP address, IP subnet mask, and IP router addresses. The WAP only responds to address offer messages from the DHCP or BOOTP server specified. If no DHCP server name is specified, the client will respond to offers from any server.

DHCP server name can be 0 to 31 characters. The name prevents the WAP from inadvertently obtaining an IP configuration from other servers on the network. The class identifier string for the WAP is “ ” (blank). Servers use this string to identify the WAP.

When the WAP responds to a DHCP or BOOTP server, it broadcasts a single ARP request to the address offered. If no ARP response is received within 3 seconds, the WAP assumes the IP address is unique and completes the negotiation for that address. If an ARP reply is received before the timeout, the WAP assumes the address is a duplicate and declines the offer.

An address offer from a BOOTP server is treated as if it were an infinite lease from a DHCP server. For more information, see “Leases” in Chapter 2.

Auto ARP Minutes The WAP periodically sends an unsolicited ARP request so that routers can update their routing tables. The request enables a network management platform to learn about the WAP on the network by querying routers. The auto ARP period controls the time interval between ARP broadcasts. The range is from 1 to 120 minutes. The default is 5 minutes. A setting of 0 disables this parameter.

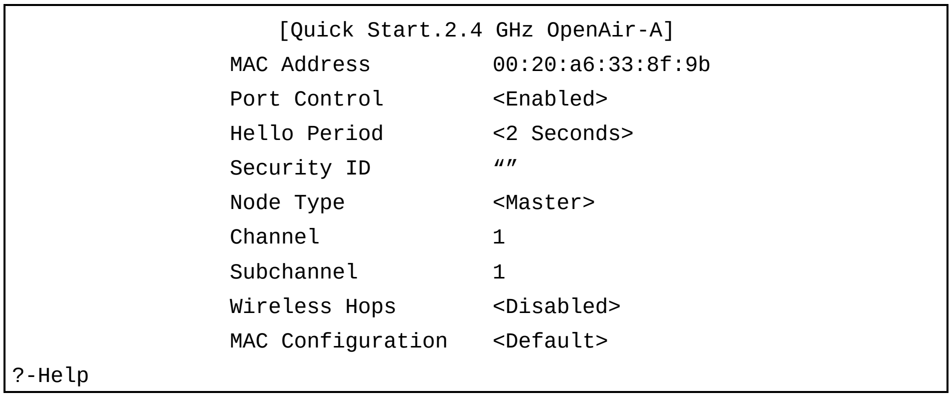
If the address of the default router is 0.0.0.0, the WAP sends an ARP request to its own IP address; otherwise, it sends an ARP request to the default router. Without this option, a WAP might not use its IP address for extended periods of time and the IP address expires from the router ARP table. If the IP address expires, the network management program needs to ping all potential addresses on a subnet to locate active IP addresses, or require the user to enter a list. You should not allow the IP address for the WAP to expire.

Configuring the 2.4 GHz OpenAir Radios

You must configure both 2.4 GHz OpenAir radios in the WAP. The default radio values in your WAP are:

Parameter	2.4 GHz OpenAir-A	2.4 GHz OpenAir-B
Node Type	Master	Station
Channel	1	9
Subchannel	1	9
Wireless Hops	Disabled	(does not apply)

The 2.4 GHz OpenAir-A menu is shown here. You must also configure the 2.4 GHz OpenAir-B radio.



```
                        [Quick Start.2.4 GHz OpenAir-A]
                    MAC Address         00:20:a6:33:8f:9b
                    Port Control        <Enabled>
                    Hello Period        <2 Seconds>
                    Security ID         “”
                    Node Type           <Master>
                    Channel             1
                    Subchannel          1
                    Wireless Hops       <Disabled>
                    MAC Configuration   <Default>
?-Help
```

MAC Address This read-only parameter displays the MAC address of this port.

Port Control This parameter allows you to enable or disable this OpenAir port. The default is Enabled.

Hello Period This parameter controls how frequently the WAP broadcasts hello packets on the OpenAir port if the OpenAir radio is configured as a master and wireless hops is enabled. Hello packets are used to maintain the spanning tree. Hello packets also serve as beacon messages to synchronize communications with power-managed stations. You can specify hello packets to be broadcast every 1, 2, or 3 seconds. The default is 2 seconds.

Security ID All 2.4 GHz OpenAir devices in the same network must have the same security ID to communicate with each other. Security ID can be from 0 to 20 characters in length. The default is no security ID.

Note: If you are using RT1100, RT1700, or RT5900 devices with 2.4 GHz OpenAir radios, you must limit the security ID to a maximum length of 16 characters.

Node Type You must configure one OpenAir radio in a WAP as a master and the other as a station.

Channel This parameter sets the hopping sequence for the radio. You can set the channel to a value from 1 to 15. The default channel for a master is 1; the default channel for a station is 9.

Subchannel This parameter enables WAPs to share the same channel but have a unique subchannel so a WAP does not receive frames intended for another WAP. The subchannel can be set to a value from 1 to 15. The default subchannel for a master is 1. The default subchannel for a station is 9.

Wireless Hops This parameter only appears if node type is set to master. You can enable a wireless hop between this WAP and another WAP by setting wireless hops to enabled. If you set wireless hops to enabled, this WAP honors a connection from a 2.4 GHz OpenAir WAP configured as a station. The station WAP must have the same LAN ID, security ID, channel, and subchannel settings as the master. The default value is disabled.

MAC Configuration You may be able to enhance the performance of your OpenAir radio by adjusting the MAC Configuration parameter. MAC configuration settings are:

Default (default) Uses the factory settings for the radio protocol. You should use this setting for normal operation.

Interference Optimizes the settings for the radio protocol for better performance in environments with high interference or multipath.

Throughput Optimizes the settings for the radio protocol for better performance of file transfer operations in open or uncongested environments, such as office areas.

Manual Allows you to adjust OpenAir MAC parameters individually using the MAC Configuration option.

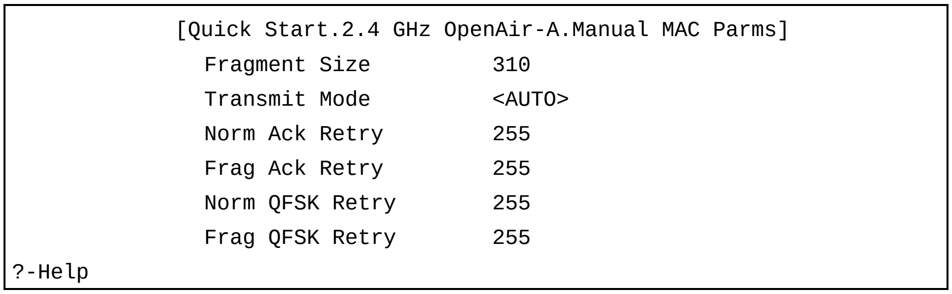
Note: An inefficient MAC configuration setting can adversely affect the performance of your wireless LAN. You should change the MAC configuration setting only under the direction of Intermec Technical Support.

[Manual MAC Parms] This command only appears on the menu if you set the MAC Configuration parameter to the manual setting. When you choose this command, you go to a menu where you can set specific MAC parameters.

Setting Manual MAC Configurations on the WAP

You can configure MAC settings manually by using the Manual MAC Parms menu. To access this menu, you must set the MAC Configuration parameter to manual and then select Manual MAC Parms from the 2.4 GHz OpenAir configuration menu.

Note: Adjusting the manual MAC parameters is not advised unless instructed to do so by Intermec Technical Support.



```
             [Quick Start.2.4 GHz OpenAir-A.Manual MAC Parms]
               Fragment Size          310
               Transmit Mode          <AUTO>
               Norm Ack Retry         255
               Frag Ack Retry         255
               Norm QFSK Retry        255
               Frag QFSK Retry        255
?-Help
```

Fragment Size This parameter specifies the maximum fragment size that can be sent over this radio during interference. Fragments are created when errors occur in transmission. You can set fragment size to a value from 1 to 1540. The default is 310. You may want to set a smaller fragment size if your environment has a high level of interference.

Transmit Mode This parameter modulates the transmit signal and sets the bits per second. You can set transmit mode to BFSK, QFSK, or AUTO. The default is AUTO. Transmit mode settings are:

BFSK (Binary Frequency Shift Keying)	Transmits at 0.8 Mbps. Data is transmitted by shifting between 2 frequencies to represent 1 bit of 0 or 1. BFSK has extended range over QFSK at the expense of throughput.
QFSK (Quadrature Frequency Shift Keying)	Transmits at 1.6 Mbps. Data is transmitted by shifting among four frequencies to represent 2 bits of 0 or 1. QFSK has better throughput than BFSK at the expense of range.
AUTO (default)	Automatically adapts the bit rate to the error conditions. The transmit mode is automatically selected for the best range and throughput.

Norm Ack Retry This parameter controls the number of times an unfragmented frame is resent unsuccessfully before fragmenting. You can set norm ack retry to a value from 1 to 255. The default is 255, which allows the radio to choose an optimal value.

The norm ack retry count includes the norm QFSK retry count; therefore, norm ack retry should be greater than norm QFSK retry.

Frag Ack Retry This parameter controls the number of times any fragmented QFSK or BFSK frame is resent unsuccessfully before failing. You can set frag ack retry to a value from 1 to 255. The default is 255, which allows the radio to choose an optimal value.

The frag ack retry count includes the frag QFSK retry count; therefore, frag ack retry should be greater than frag QFSK retry.

Norm QFSK Retry This parameter controls the number of times that an unfragmented QFSK frame is resent unsuccessfully before switching to BFSK. This parameter is only in effect when transmit mode is set to AUTO. You can set norm QFSK retry to a value from 1 to 255. The default value is 255.

Frag QFSK Retry Fragmented QFSK retry controls the number of times a fragmented QFSK frame is resent unsuccessfully before switching to BFSK. This parameter is only in effect when transmit mode is set to AUTO. You can set frag QFSK retry to a value from 1 to 255. The default is 255.

Configuring the 900 MHz Falcon WAP

The 900 MHz Falcon WAP has only one radio. The 900 MHz Falcon WAP will communicate with other 900 MHz Falcon radios that have the same:

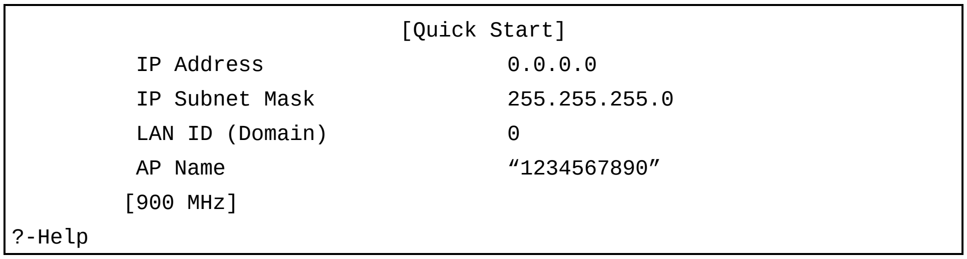
- LAN ID (Domain)
- Mode-Channel

You use the Quick Start menu to set basic network parameters, including LAN ID. Use the Network Configuration menu if you need to set a default IP router. Use the 900 MHz Falcon port menu to set the radio parameters, including the Mode-Channel parameter.

Using the Quick Start Menu

You need to configure these basic network parameters using the Quick Start menu:

- IP Address
- IP Subnet Mask
- LAN ID (Domain)



```
                              [Quick Start]
          IP Address                   0.0.0.0
          IP Subnet Mask               255.255.255.0
          LAN ID (Domain)              0
          AP Name                      “1234567890”
         [900 MHz]
?-Help
```

IP Address Each node that communicates with the Ethernet network must have a unique IP address. The IP address is a network level address assigned to each device in a TCP/IP network. The default IP address is 0.0.0.0. The range is 0 to 255. The first number cannot be zero unless all remaining numbers are zero. The first node also cannot be 127 or greater than 223. If the IP address is 0.0.0.0 and DHCP is enabled on the Network Configuration menu, the IP address is obtained via DHCP. If the IP address is 0.0.0.0 and DHCP is disabled, TCP/IP access to this UAP is disabled.

IP Subnet Mask The subnet mask is used in the IP protocol to separate the subnet address from the local IP address. The IP protocol performs a bit-wise AND on the IP address and the subnet mask. For example, if the IP address is 192.168.150.184 and the subnet mask is 255.255.255.0, the subnet address is 192.168.150. The default IP subnet mask is 255.255.255.0.

If this WAP is installed on an existing segment, the subnet mask should match the other computers on the segment. If you are using DHCP to obtain an IP address, then the subnet mask that is obtained from DHCP will supersede this one.

If you are using the suggested 192.168.h.h IP address, you should use the subnet mask of 255.255.0.0. This mask provides network 192.168 with space for thousands of devices.

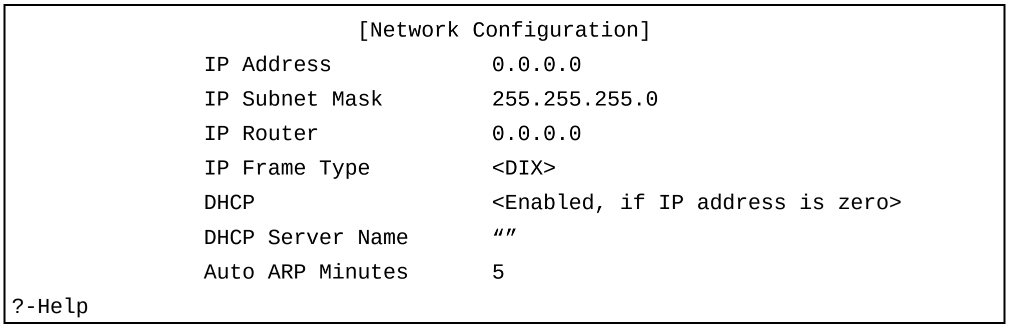
LAN ID (Domain) The LAN ID or domain identifies the INCA spanning tree. All wireless devices in a wireless network must have the same LAN ID. The range for 900 MHz Falcon devices is 0 to 254. The default value is 0.

AP Name You can assign a unique name to identify this WAP in the network. AP name can be from 1 to 16 characters long. The default is the serial number of the WAP.

[900 MHz] Select this command to configure the 900 MHz Falcon radio in your WAP.

Using the Network Configuration Menu

If your WAP will communicate with devices on the other side of a router, you must set the IP address of the router that will forward data frames to addresses on another subnet. Use the Network Configuration menu to configure the IP router.



```
                        [Network Configuration]
               IP Address            0.0.0.0
               IP Subnet Mask        255.255.255.0
               IP Router             0.0.0.0
               IP Frame Type         <DIX>
               DHCP                  <Enabled, if IP address is zero>
               DHCP Server Name      “”
               Auto ARP Minutes      5
?-Help
```

IP Address Each node that communicates with the Ethernet network must have a unique IP address. The IP address is a network level address assigned to each device in a TCP/IP network. The default IP address is 0.0.0.0. The range is 0 to 255. The first number cannot be zero unless all remaining numbers are zero. The first node also cannot be 127 or greater than 223. If the IP address is 0.0.0.0 and DHCP is enabled, the IP address is obtained via DHCP. If the IP address is 0.0.0.0 and DHCP is disabled, TCP/IP access to this UAP is disabled.

IP Subnet Mask The subnet mask is used in the IP protocol to separate the subnet address from the local IP address. The IP protocol performs a bit-wise AND on the IP address and the subnet mask. For example, if the IP address is 192.168.150.184 and the subnet mask is 255.255.255.0, the subnet address is 192.168.150. The default IP subnet mask is 255.255.255.0.

If this WAP is installed on an existing segment, the subnet mask should match the other computers on the segment. If you are using DHCP to obtain an IP address, then the subnet mask that is obtained from DHCP will supersede this one.

If you are using the suggested 192.168.h.h IP address, you should use the subnet mask of 255.255.0.0. This mask provides network 192.168 with space for thousands of devices.

IP Router This parameter identifies the address of the default router that the WAP uses to route packets to other subnets or networks. The range is 4 numbers from 0 to 255. The first number cannot be zero unless all remaining numbers are zero. The first node also cannot be 127 or greater than 223. The default is 0.0.0.0, which disables the ability of this subnet to exchange TCP/IP traffic with another subnet or network. If you are using DHCP to obtain an IP address for this WAP, and a DHCP server specifies a default IP router, then the DHCP specification will supersede the value you set in this IP router field.

IP routers are typically configured so that the WAP only needs to know the address of one router even if there are several routers on the segment connecting to several other segments. If the subnet mask is 255.255.255.0, for example, a router that connects subnet 1 to subnet 2 might have the address 172.16.8.1 on subnet 1 and 172.16.16.1 on subnet 2. A host with IP address 172.16.16.5 would specify an IP router address of 172.16.16.1 to reach host 172.16.8.10.

The WAP dynamically creates a new IP route table entry whenever it receives an Internet Control Message Protocol (ICMP) redirect packet. For example, a default router may return an ICMP redirect packet to a WAP when it receives an IP packet from the WAP and there is a preferred router for the target destination.

IP Frame Type This parameter indicates the type of frame that contains IP traffic. The type can be either DIX or SNAP. DIX frames are also known as Ethernet v2.0 frames. You typically use DIX frames for TCP/IP over an Ethernet network. If other computers on your network use RFC1042 SNAP encapsulation for IP frames, then select SNAP frame type. The default is DIX.

DHCP The WAP has DHCP client support so that it can automatically accept IP addresses from a DHCP or BOOTP server on the network. Using DHCP simplifies installation of IP devices because it eliminates the manual entry of IP addresses, subnet masks, and default router IP addresses on every device.

The WAP responds to both DHCP and BOOTP servers; however, preference is given to DHCP servers. If a BOOTP reply arrives at the WAP before any DHCP offers are received, the WAP waits an additional 4 seconds for a DHCP offer before responding. If a DHCP offer is received within the 4-second period, the BOOTP reply is ignored and the DHCP offer is accepted.

DHCP settings are:

Enabled	This setting allows you to enable DHCP without setting IP address to 0.0.0.0. If DHCP is enabled, the UAP will accept addresses from the DHCP server. You may find this setting helpful when troubleshooting your network.
Enabled, if IP address is zero	You must set IP address to 0.0.0.0 to enable DHCP. DHCP will then assign IP address, IP subnet mask, and IP router addresses.
Disabled	DHCP not used.

DHCP Server Name This parameter identifies the network server that the WAP accesses to automatically assign addresses to IP address, IP subnet mask, and IP router. The WAP only responds to address offer messages from the DHCP or BOOTP server specified. If no DHCP server name is specified, the client will respond to offers from any server.

DHCP server name can be from 0 to 31 characters. The name prevents the WAP from inadvertently obtaining an IP configuration from other servers on the network. The class identifier string for the WAP is “ ” (blank). Servers use this string to identify the WAP.

When the WAP responds to a DHCP or BOOTP server, it broadcasts a single ARP request to the address offered. If no ARP response is received within 3 seconds, the WAP assumes the IP address is unique and completes the negotiation for that address. If an ARP reply is received before the timeout, the WAP assumes the address is a duplicate and declines the offer.

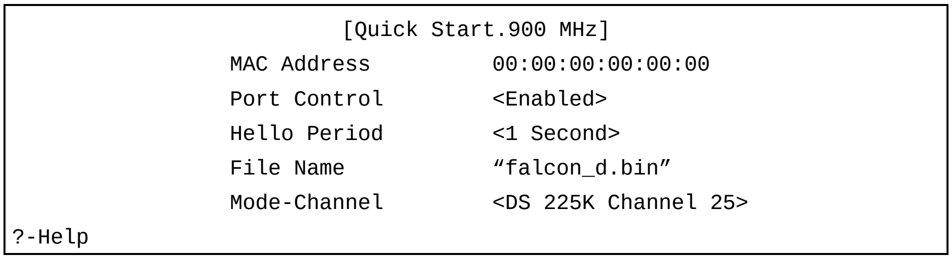
An address offer from a BOOTP server is treated as if it were an infinite lease from a DHCP server. For more information, see “Leases” in Chapter 2.

Auto ARP Minutes The WAP periodically sends an ARP request so that routers can update their routing tables. The request enables a network management platform to learn about the WAP on the network by querying routers. Auto ARP minutes controls the time interval between ARP broadcasts. The range is from 1 to 120 minutes. The default is 5 minutes. A setting of 0 disables auto ARP minutes.

If the address of the default router is 0.0.0.0, the WAP sends an unsolicited ARP request to its own IP address; otherwise, it sends an ARP request to the default router. Without this option, a WAP might not use its IP address for extended periods of time and the IP address expires from the router ARP table. If the IP address expires, the network management program needs to ping all potential addresses on a subnet to locate active IP addresses, or require the user to enter a list. You should not allow the IP address for the WAP to expire.

Configuring the 900 MHz Falcon Radio

You configure the 900 MHz Falcon radio in your WAP by selecting the 900 MHz Falcon command from the Quick Start menu. The 900 MHz Falcon menu appears.



```
                          [Quick Start.900 MHz]
                 MAC Address         00:00:00:00:00:00
                 Port Control        <Enabled>
                 Hello Period        <1 Second>
                 File Name           “falcon_d.bin”
                 Mode-Channel        <DS 225K Channel 25>
?-Help
```

MAC Address This read-only parameter displays the MAC address of this port.

Port Control This parameter allows you to enable or disable the 900 MHz Falcon port. The default is enabled.

Hello Period This parameter controls how frequently the WAP broadcasts hello messages on the 900 MHz port. On wireless links between WAPs, hello messages are used to maintain the spanning tree. Hello messages also serve as beacon messages to synchronize communications with power-managed end devices. You can specify hello messages to be broadcast every 1, 2, or 3 seconds. The default is 1 second.

File Name This parameter specifies the name of the radio’s driver software. The default file name is falcon_d.bin.

You should not need to change this name—only change this name when directed to do so by qualified Intermec personnel.

Mode-Channel Setting this parameter allows you to balance the need for radio coverage with the need for speed. Mode sets the bit rate option for the 900 MHz Falcon radio. Generally, the higher the bit rate, the lower the range of the WAP. Channel defines a frequency range that is a small portion of the available bandwidth.

Select the Mode-Channel parameter to display the list of mode and channel combinations that are available on your WAP. Mode-Channel options are country-dependent. For example, the following combinations are valid in the United States:

- DS 225K-Channel 25
- DS 090K-Channel 10
- DS 090K-Channel 15
- DS 090K-Channel 20
- DS 090K-Channel 25
- DS 090K-Channel 30

900 MHz Mode-Channels Valid in the United States (continued)

- DS 090K-Channel 35
- DS 090K-Channel 40
- DS 450K-Channel 25

Mode-Channel combinations are:

DS 225K-Channel 25	Uses one direct sequenced channel at 225,000 bits per second. This one moderate-speed channel uses all available bandwidth.
DS 090K-Channel 10 through DS 090K-Channel 40	Uses one of several direct sequenced channels at 90,000 bits per second. Seven low-speed channels share the available bandwidth.
DS 450K-Channel 25	Uses one direct sequenced channel at 450,000 bits per second. This one high-speed channel uses all available bandwidth.

Note: You can position your 900 MHz Falcon WAPs at least 15.24 meters (50 feet) apart. Positioning your WAPs closer than 15.24 meters will not increase throughput, but may provide redundancy.

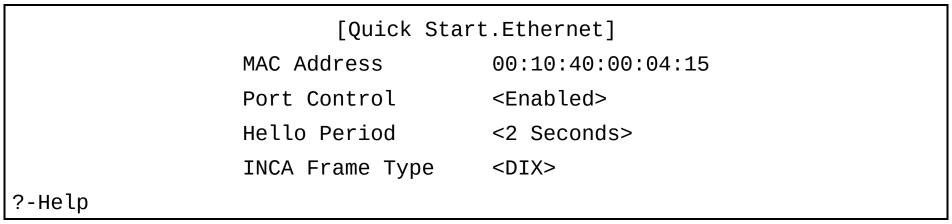
4

Configuring the Ports

This chapter explains how to configure the Ethernet, INCA/IP, and radio ports.

Configuring the Ethernet Port

You may need to configure some Ethernet parameters if your UAP is wired to your Ethernet network. To configure the Ethernet port, choose the Ethernet command from the Quick Start menu. The Ethernet menu appears.



```
                         [Quick Start.Ethernet]
                  MAC Address        00:10:40:00:04:15
                  Port Control       <Enabled>
                  Hello Period       <2 Seconds>
                  INCA Frame Type    <DIX>
?-Help
```

MAC Address This read-only parameter displays the MAC address of this port.

Port Control This parameter lets you enable or disable the Ethernet port. The default is enabled.

Hello Period This parameter controls how frequently the UAP broadcasts hello packets on the Ethernet network. Hello packets are used to maintain the spanning tree and serve as beacon messages to synchronize communications with power-managed stations. Only the root UAP sends hello packets on the primary Ethernet LAN. Only the designated bridge sends hello packets on a secondary LAN. You can specify hello packets to be broadcast every 1, 2, or 3 seconds. The default is 2 seconds.

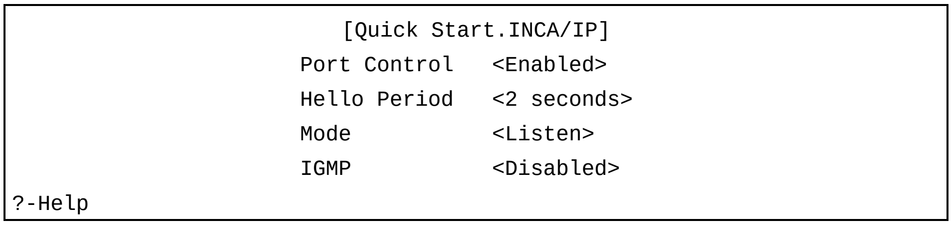
INCA Frame Type This parameter controls whether DIX (DIX type hex 875C) or 802.3 SNAP headers are used for INCA frames. The default INCA frame type is DIX.

Configuring the INCA/IP Port

The INCA/IP port is a logical port and does not exist in a physical sense. For ease of configuration, INCA/IP is referred to as a port. The INCA/IP port provides IP encapsulation services for frames that must be routed to reach their destination. After encapsulation, frames are transmitted or received through one of the physical ports.

INCA/IP is a protocol that is used to enhance the MAC layer for roaming functionality between UAPs on different IP subnets. You can think of the INCA/IP port as an IP tunnel that allows branches to be added to the INCA spanning tree. The INCA spanning tree facilitates the roaming functionality. For more information about INCA/IP, see Appendix B, “Understanding INCA/IP.”

To configure the INCA/IP port, choose the INCA/IP command from the Quick Start menu. The INCA/IP menu appears.



```
                         [Quick Start.INCA/IP]
                       Port Control   <Enabled>
                       Hello Period   <2 seconds>
                       Mode           <Listen>
                       IGMP           <Disabled>
?-Help
```

Port Control This parameter lets you enable or disable the INCA/IP port. The default is enabled.

Hello Period This parameter controls how frequently the UAP broadcasts hello packets on the network. Hello packets are used to maintain the spanning tree. Hello packets also serve as beacon messages to synchronize communications with power-managed stations. You can specify hello packets to be broadcast every 1, 2, or 3 seconds. The default is 2 seconds.

Mode This parameter controls whether the UAP listens for an INCA/IP tunnel or originates INCA/IP tunnel connections with other UAPs.

Mode settings are:

Listen (default) The UAP can serve as the termination of a tunnel if the UAP is the designated bridge for the subnet. The UAP cannot originate a tunnel.

Originate If Root The UAP can originate INCA/IP tunnels if it is functioning as the root for the network.

Note: A WAP should never be configured as the root. Be sure you configure the mode for a WAP to listen.

IGMP This parameter allows you to enable or disable the use of IGMP. The default is disabled.

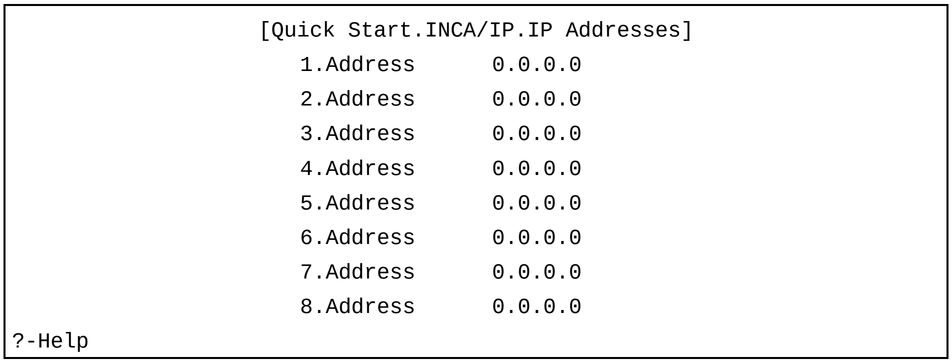
IGMP lets you establish multiple INCA/IP tunnels with a single multicast IP address. IGMP allows the root UAP to use a Class D IP multicast address to send INCA/IP hello packets through routers to UAPs on other IP subnets. Enabling IGMP on remote IP subnets causes intermediate IP routers to forward the INCA/IP hello packets to those subnets.

If you set IGMP to enabled, the Multicast Address field appears on the screen. The IGMP multicast address must match one of the IP addresses configured in the INCA/IP IP Address list in the root UAP.

For more information about configuring IGMP, see “Using IGMP” later in this section. For more information about IGMP and INCA/IP, see “IGMP” in Appendix B.

Multicast Address This field appears on the screen when IGMP is set to enabled. The Intermec Class D multicast IP address, 224.0.1.65, appears in this field by default. You can change the address to any Class D multicast IP address.

[IP Addresses] When the Mode parameter is set to originate if root, the IP Addresses command appears on the screen. When you select this command, the IP Addresses menu appears.



```
                    [Quick Start.INCA/IP.IP Addresses]
                       1.Address      0.0.0.0
                       2.Address      0.0.0.0
                       3.Address      0.0.0.0
                       4.Address      0.0.0.0
                       5.Address      0.0.0.0
                       6.Address      0.0.0.0
                       7.Address      0.0.0.0
                       8.Address      0.0.0.0
?-Help
```

You can define up to eight IP addresses for which your UAP can originate tunnels. The range for an address is 4 numbers from 0 to 255. Each entry can be a unicast, broadcast, or Class D multicast IP address. Class D IP addresses are mapped to multicast Ethernet addresses, per RFC 1112. If the UAP is functioning as the INCA root, it will send an INCA/IP hello packet to each address in the list, once per hello period. A remote UAP that receives an INCA/IP hello packet can establish an INCA/IP tunnel with the root UAP.

Using IGMP

Using IP multicast and IGMP for INCA/IP hello packets has these advantages:

- You can establish multiple tunnels with a single address.
- INCA/IP hello packets are only forwarded to those IP subnets that participate in the multicast group.
- Using IP multicast increases redundancy, because multiple UAPs on a remote subnet can receive INCA/IP hello packets.

To configure IGMP

1. Set these parameters on the originating UAP:
   - Set the IGMP parameter to enabled.
   - Set the Multicast Address parameter to a valid Class D multicast address.
   - Enter the same valid Class D address in the IP Addresses table.
2. Set these parameters on a UAP on the other side of a router:
   - Set the IGMP parameter to enabled.
   - Set the Multicast Address parameter to the same Class D multicast address.
3. Enable IGMP on all routers that are between the root UAP originating the INCA/IP tunnel and the UAPs configured to listen for the INCA/IP tunnel.

Configuring the 2.4 GHz OpenAir Port

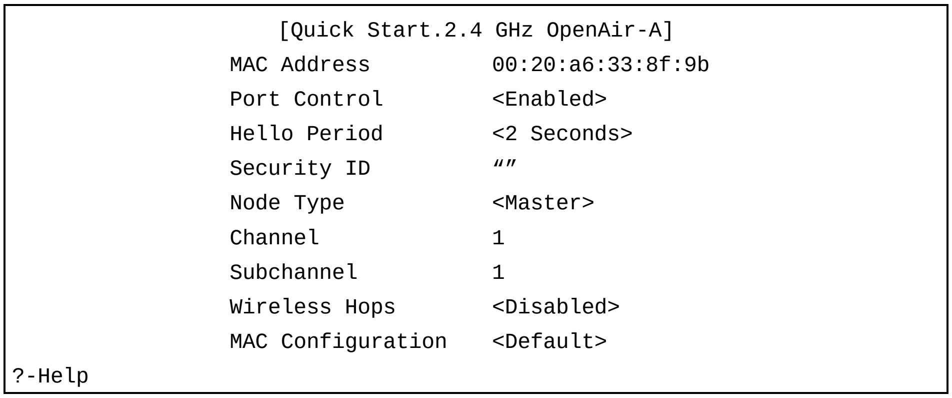
This section explains how to configure the 2.4 GHz OpenAir radio in a UAP that is wired to the Ethernet network. If you are configuring an OpenAir WAP, see "Configuring the 2.4 GHz OpenAir WAP" in Chapter 3. If you are configuring your 2100s for wireless bridging in a point-to-point arrangement, see "Configuring 2.4 GHz OpenAir UAPs for Point-to-Point Bridging " in Chapter 2.

The 2.4 GHz OpenAir radio will communicate with other 2.4 GHz OpenAir radios that have the same:

- LAN ID
- Channel
- Subchannel
- Security ID

You may need to set additional radio parameters. You use the Quick Start menu to set the LAN ID, and you use the 2.4 GHz OpenAir menu to set the radio parameters. When you select the 2.4 GHz OpenAir command from the Quick Start menu, the 2.4 GHz OpenAir menu appears.

2.4 GHz OpenAir Port Configuration Menu



```
                      [Quick Start.2.4 GHz OpenAir-A]
                  MAC Address         00:20:a6:33:8f:9b
                  Port Control        <Enabled>
                  Hello Period        <2 Seconds>
                  Security ID         “”
                  Node Type           <Master>
                  Channel             1
                  Subchannel          1
                  Wireless Hops       <Disabled>
                  MAC Configuration   <Default>
?-Help
```

MAC Address This read-only parameter displays the MAC address of this port.

Port Control This parameter allows you to enable or disable the 2.4 GHz OpenAir port. The default is enabled.

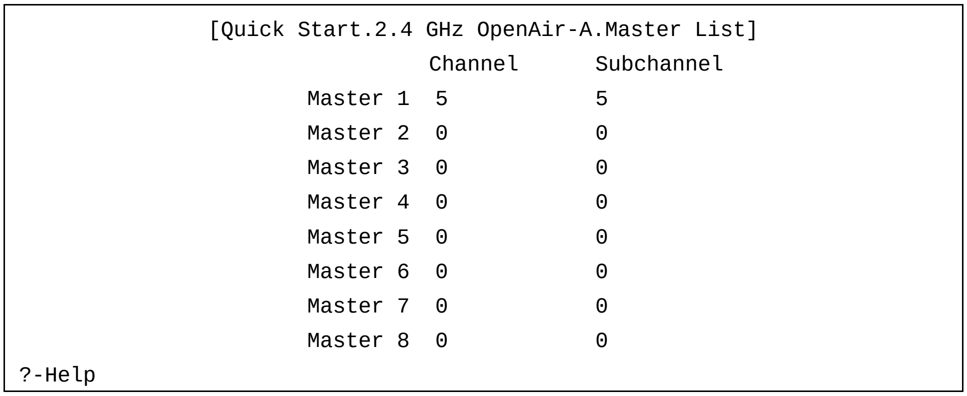
Hello Period This parameter controls how frequently the UAP broadcasts hello packets on the OpenAir port if the OpenAir radio is configured as a master and wireless hops is enabled. Hello packets are used to maintain the spanning tree. Hello packets also serve as beacon messages to synchronize communications with power-managed stations. You can specify hello packets to be broadcast every 1, 2, or 3 seconds. The default is 2 seconds.

Security ID All UAPs and end devices that use 2.4 GHz OpenAir radios in the same network must have the same security ID to communicate with each other. This security prevents unauthorized radios from communicating with the UAP. Security ID can be from 0 to 20 characters in length. The default is null or no security ID.

Note: If you are using RT1100, RT1700, or RT5900 devices with 2.4 GHz OpenAir radios, you must limit the security ID to a maximum length of 16 characters.

Node Type You can configure the UAP as a master or station. The default for OpenAir-A is master. If a second 2.4 GHz OpenAir radio is installed in the UAP, the default node type for OpenAir-B is station.

[Master List] This parameter only appears on the screen if you set node type to station. You use the master list to identify those master UAPs that the station UAP can synchronize with. When you select this option, the following screen appears.



```
                [Quick Start.2.4 GHz OpenAir-A.Master List]
                                 Channel      Subchannel
                        Master 1  5           5
                        Master 2  0           0
                        Master 3  0           0
                        Master 4  0           0
                        Master 5  0           0
                        Master 6  0           0
                        Master 7  0           0
                        Master 8  0           0
?-Help
```

The station UAP synchronizes with master UAPs whose channel and subchannel appear in its master list. You can specify up to eight masters. Precedence is given by the order of the masters in the list. Master 1 has the greatest priority and Master 8 has the lowest priority. Master 1 has a default channel of 5 and a default subchannel of 5. The remaining masters have default channels and subchannels of 0.

To enter a master in the list, select a master and press **Enter**. You can then specify the master's channel and subchannel. The range for channel and subchannel is from 0 to 15. You can use 0 as a wildcard. For example, if you set the Master 1 channel to 0 and the subchannel to 1, the station UAP synchronizes with any master on any channel as long as the master's subchannel is 1. If you set both the Master 1 channel and subchannel to 0, the station synchronizes with any master.

Channel This parameter only appears on the screen if node type is set to master. The channel parameter sets the hopping sequence for this master radio. You can set the channel to a value from 1 to 15. The default is 1.

Note: If you are using 2.4 GHz OpenAir radios and you have more than one UAP within the same coverage area, you must configure each UAP with a unique radio channel.

Subchannel This parameter only appears on the screen if node type is set to master. The subchannel parameter enables UAPs to share the same channel but have a unique subchannel so the UAP does not receive frames intended for another UAP. Two UAPs on different subchannels share the same hopping sequence, but behave as if they were on different channels. Subchannel can be set to a value from 1 to 15. The default subchannel is 1.

Wireless Hops This parameter only appears on the screen if node type is set to master. You can set wireless hops to either disabled or enabled. If you set wireless hops to enabled, this master UAP honors connections from 2.4 GHz OpenAir UAPs configured as stations. The station UAPs must have the same LAN ID, security ID, channel, and subchannel as the master. The default value is disabled.

You need to enable wireless hops for point-to-point bridging or for a master UAP that is to communicate with a WAP.

MAC Configuration You may be able to enhance the performance of your 2.4 GHz OpenAir radio by adjusting the MAC Configuration parameter. The possible settings for the MAC Configuration parameter are described in this section.

Note: An inefficient MAC configuration setting can adversely affect the performance of your open wireless LAN. You should change the MAC configuration setting only under the direction of Intermec Technical Support.

The MAC configuration settings are:

Default (default) Uses the factory settings for the radio protocol. You should use this setting for normal operation.

Interference Optimizes the settings for the radio protocol for better performance in environments with high interference or multipath.

Throughput Optimizes the settings for the radio protocol for better performance of file transfer operations in open or uncongested environments, such as office areas.

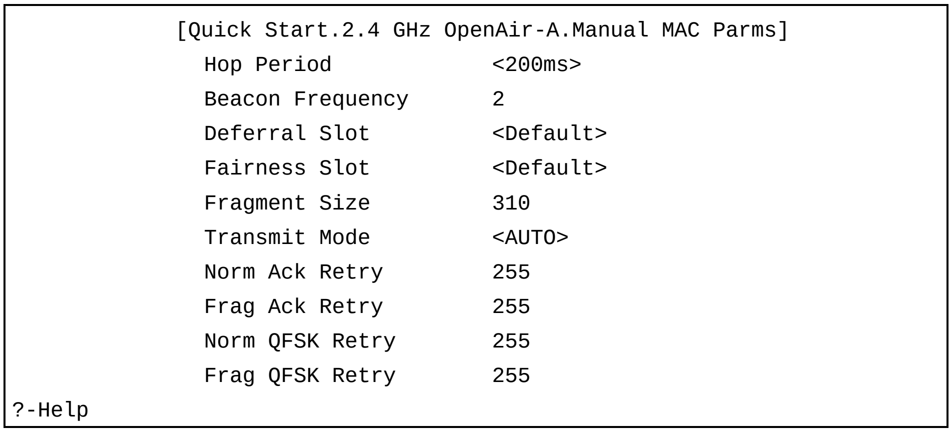
Manual Allows you to adjust 2.4 GHz OpenAir MAC parameters individually using the Manual MAC Parms command.

[Manual MAC Parms] This command only appears on the menu if you set the MAC Configuration parameter to manual. When you choose this command, you go to a menu where you can set specific MAC parameters. For help, see “Setting Manual MAC Parameters” in the next section.

Setting Manual MAC Parameters

Occasionally, you may need to fine-tune your 2.4 GHz OpenAir radio parameters. You can configure MAC settings manually by using the Manual MAC Parms menu. To access the Manual MAC Parms menu, you must set the MAC Configuration parameter to manual and then select the Manual MAC Parms command from the 2.4 GHz OpenAir configuration menu.

Note: Adjusting the manual MAC parameters is not advised unless instructed to do so by Intermec Technical Support.



```
             [Quick Start.2.4 GHz OpenAir-A.Manual MAC Parms]
               Hop Period             <200ms>
               Beacon Frequency       2
               Deferral Slot          <Default>
               Fairness Slot          <Default>
               Fragment Size          310
               Transmit Mode          <AUTO>
               Norm Ack Retry         255
               Frag Ack Retry         255
               Norm QFSK Retry        255
               Frag QFSK Retry        255
?-Help
```

Hop Period This parameter determines how long the radio stays on a frequency in the hopping sequence before stepping to the next frequency. You can set this parameter to 100, 200, or 400 milliseconds. A longer period results in better throughput; a shorter period results in faster roaming response and immunity from interference. The default is 200 milliseconds.

Beacon Frequency The UAP periodically transmits a beacon to allow stations to quickly scan each frequency to find a master UAP. Beacon frequency is the number of hops between beacons. You can set the beacon frequency to a value from 1 to 7. The default is 2.

Deferral Slot This parameter, along with the fairness slot, determines the average back-off time when the channel is sensed to be busy. You can set the deferral slot to 1, 3, 7, or default. The default value is default. You may want to reduce the number of slots on lightly loaded networks to increase throughput or increase the number to help prevent repeated collisions under a heavy load.

Fairness Slot This parameter, along with deferral slot, determines the average back-off time when the channel is sensed to be busy. You can set the fairness slot to 1, 3, 7, or default. The default value is default. You may want to increase the number to prioritize the channel access for nodes that have been waiting the longest to access the channel, or you may need to decrease the number to minimize initial back-off delays.

Fragment Size Fragments are created when errors occur in transmission. The Fragment Size parameter determines the maximum fragment size that can be sent over this radio during interference. You may want to set a smaller fragment size if your environment has a high level of interference. You can set fragment size to a value from 1 to 1540. The default is 310.

Transmit Mode This parameter modulates the transmit signal and sets the bits per second.

The transmit mode settings are:

BFSK (Binary Frequency Shift Keying)	Transmits at 0.8 Mbps. Data is transmitted by shifting between 2 frequencies to represent 1 bit of 0 or 1. BFSK has extended range over QFSK at the expense of throughput.
QFSK (Quadrature Frequency Shift Keying)	Transmits at 1.6 Mbps. Data is transmitted by shifting among four frequencies to represent 2 bits of 0 or 1. QFSK has better throughput than BFSK at the expense of range.
AUTO (default)	Automatically adapts the bit rate to the error conditions. The transmit mode is automatically selected for the best range and throughput.

Norm Ack Retry This parameter controls the number of times an unfragmented frame is resent unsuccessfully before fragmenting. You can set normal acknowledge retry to a value from 1 to 255. The default is 255, which allows the radio to choose an optimal value.

The norm ack retry count includes the norm QFSK retry count; therefore, norm ack retry should be greater than norm QFSK retry.

Frag Ack Retry This parameter controls the number of times any fragmented QFSK or BFSK frame is resent unsuccessfully before failing. You can set fragmented acknowledge retry to a value from 1 to 255. The default is 255, which allows the radio to choose an optimal value.

The frag ack retry count includes the frag QFSK retry count; therefore, frag ack retry should be greater than frag QFSK retry.

Norm QFSK Retry This parameter controls the number of times that an unfragmented QFSK frame is resent unsuccessfully before switching to BFSK. This parameter is only in effect when transmit mode is set to AUTO. You can set normal QFSK retry to a value from 1 to 255. The default value is 255.

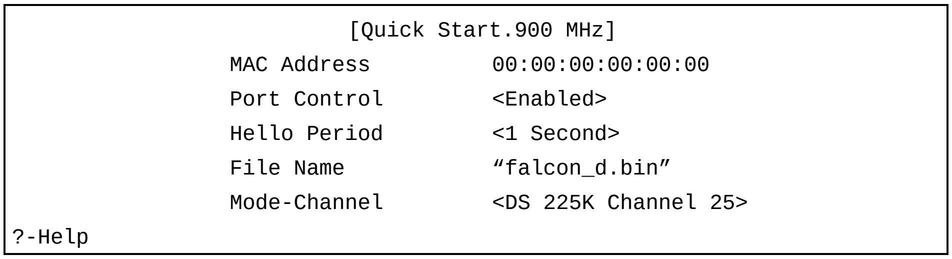
Frag QFSK Retry Fragmented QFSK retry controls the number of times a fragmented QFSK frame is resent unsuccessfully before switching to BFSK. This parameter is only in effect when transmit mode is set to AUTO. You can set fragmented QFSK retry to a value from 1 to 255. The default is 255.

Configuring the 900 MHz Falcon Port

The 900 MHz Falcon radio will communicate with other 900 MHz Falcon radios that have the same:

- LAN ID
- Mode-Channel

You use the Quick Start menu to set the LAN ID. Use the 900 MHz Falcon menu to set the radio parameters, including mode-channel. When you select the 900 MHz Falcon command from the Quick Start menu, the 900 MHz Falcon menu appears.



```
                           [Quick Start.900 MHz]
                 MAC Address         00:00:00:00:00:00
                 Port Control        <Enabled>
                 Hello Period        <1 Second>
                 File Name           “falcon_d.bin”
                 Mode-Channel        <DS 225K Channel 25>
?-Help
```

MAC Address This read-only parameter displays the MAC address of this port.

Port Control This parameter allows you to enable or disable the 900 MHz Falcon port. The default is enabled.

Hello Period This parameter controls how frequently the UAP broadcasts hello packets on the Falcon radio port. On wireless links between UAPs, hello packets are used to maintain the spanning tree. Hello packets also serve as beacon messages to synchronize communications with power-managed stations. You can specify hello packets to be broadcast every 1, 2, or 3 seconds. The default is 1 second.

File Name This parameter specifies the name of the radio’s driver software. The default file name is falcon_d.bin.

Note: You should not need to change this name—only change this name when directed to do so by Intermec Technical Support.

Mode-Channel Setting this parameter allows you to balance the need for radio coverage with the need for speed. Mode sets the bit rate option for the 900 MHz Falcon radio. Generally, the higher the bit rate, the lower the range of the UAP. Channel defines a frequency range that is a small portion of the available bandwidth.

Select the Mode-Channel command to display the list of mode and channel combinations that are available on your UAP. Mode-Channel options are country-dependent. For example, the following combinations are valid in the United States:

- DS 225K-Channel 25
- DS 090K-Channel 10
- DS 090K-Channel 15
- DS 090K-Channel 20
- DS 090K-Channel 25
- DS 090K-Channel 30
- DS 090K-Channel 35
- DS 090K-Channel 40
- DS 450K-Channel 25

Mode-Channel combinations are described here:

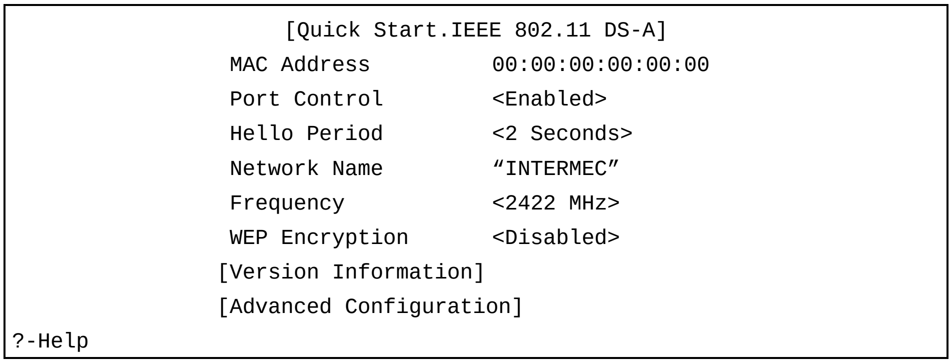
DS 225K-Channel 25 Uses one direct sequenced channel at 225,000 bits per second. This one moderate-speed channel uses all available bandwidth.

DS 090K-Channel 10 through DS 090K-Channel 40 Uses one of several direct sequenced channels at 90,000 bits per second. Seven low-speed channels share the available bandwidth.

DS 450K-Channel 25 Uses one direct sequenced channel at 450,000 bits per second. This one high-speed channel uses all available bandwidth.

Configuring the IEEE 802.11 Direct Sequence Port

Choose the IEEE 802.11 DS command from the Quick Start menu to configure your IEEE 802.11 DS port. The IEEE 802.11 DS menu appears.



```
                     [Quick Start.IEEE 802.11 DS-A]
                 MAC Address          00:00:00:00:00:00
                 Port Control         <Enabled>
                 Hello Period         <2 Seconds>
                 Network Name         "INTERMEC"
                 Frequency            <2422 MHz>
                 WEP Encryption       <Disabled>
                [Version Information]
                [Advanced Configuration]
?-Help
```

Note: Intermec does not support point-to-point bridging or wireless repeating functionality using the IEEE 802.11 DS radio in the UAP at this time. Intermec also does not support dual IEEE 802.11 DS radios or mixed radios in the UAP.

MAC Address This read-only parameter displays the MAC address of this port.

Port Control This parameter lets you enable or disable the IEEE 802.11 port. The default is enabled.

Hello Period This parameter controls how frequently the UAP broadcasts hello packets on the IEEE 802.11 DS port. Hello packets are used to maintain the spanning tree. They also serve as beacon messages to synchronize communications with power-managed stations. You can specify hello packets to be broadcast every 1, 2, or 3 seconds. The default is 2 seconds.

Network Name The IEEE 802.11 DS radio communicates with other IEEE 802.11 DS radios that have the same network name. Assign a network name to the UAP and then assign the same network name to the end devices that will connect to the UAP. The network name can be a maximum length of 32 alphanumeric characters. The default network name is INTERMEC (case sensitive).

You can also configure network name to ANY, which lets the UAP communicate with any IEEE 802.11 DS end device in the network, regardless of the network name configured in the end device.

Frequency This parameter determines the particular frequency within the 2400 to 2500 MHz range that the UAP uses to transmit and receive packets. The available frequencies are country-dependent and are determined by the radio.

For UAPs used in Spain, France, or Japan, you should configure all UAPs to a common frequency. For all other countries, you can either configure all UAPs to a common frequency, or you can select up to three frequencies that are three channels or 25 MHz apart. For instance, you could select 2412 MHz, 2437 MHz, and 2462 MHz.

You may want to use a single frequency to isolate the installation to part of the band. For example, use a single frequency if other DS systems are in use in the area or if numerous microwave ovens are used in the area.

Available Frequencies for the IEEE 802.11 DS Radio

Channel	FCC	ETSI	France	Japan
1	2412	2412		
2	2417	2417		
3	2422 (default)	2422		
4	2427	2427		
5	2432	2432		
6	2437	2437		
7	2442	2442		
8	2447	2447		
9	2452	2452		
10	2457	2457	2457	
11	2462	2462	2462 (default)	
12		2467	2467	
13		2472	2472	
14				2484

WEP Encryption If your IEEE 802.11 DS radio supports Wired Equivalent Privacy (WEP) data encryption for wireless communications, this option appears on the menu. You can enable or disable WEP encryption. The default is disabled.

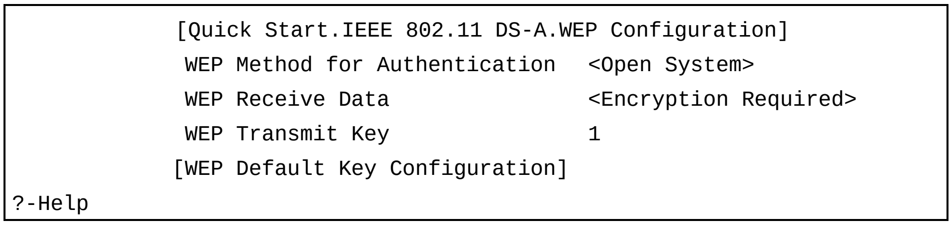
[WEP Configuration] This command only appears on the menu if your radio supports WEP encryption and you configure the WEP Enable parameter to enabled. When you select this command, the WEP Configuration menu appears. For more information, see “Setting WEP Configuration Parameters” in the next section.

[Version Information] You can use this command to display the firmware versions programmed into the IEEE 802.11 DS radio card. For more information, see “Viewing Version Information” later in this chapter.

[Advanced Configuration] This command lets you change parameters to tune your IEEE 802.11 DS radio performance for your specific environment. In general, you should not need to change the values of these parameters. For more information, see “Setting Advanced Configurations” later in this chapter.

Setting WEP Configuration Parameters

If your IEEE 802.11 DS radio supports WEP encryption and you set the WEP Encryption parameter to enabled, you can use the WEP Configuration menu to configure the WEP parameters.



```
              [Quick Start.IEEE 802.11 DS-A.WEP Configuration]
               WEP Method for Authentication   <Open System>
               WEP Receive Data                <Encryption Required>
               WEP Transmit Key                1
              [WEP Default Key Configuration]
?-Help
```

WEP Method for Authentication This parameter determines if WEP is used as part of the authentication algorithm when end devices attach to the UAP. This parameter has no effect on the use of WEP during regular wireless communications between this UAP and end devices.

The WEP method for authentication settings are:

Open System (default) WEP encryption is not used as part of the authentication algorithm with end devices.

Shared Key WEP encryption is used as part of the authentication algorithm with end devices.

WEP Receive Data This parameter determines if the UAP will receive transmissions from end devices that are not using WEP.

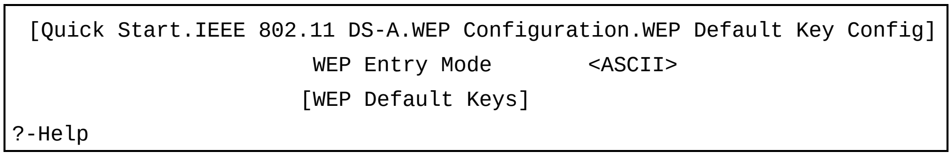
The WEP receive data settings are:

Unencrypted Allowed The UAP can communicate with end devices regardless of whether the end device has WEP enabled.

Encryption Required (default) End devices must have WEP enabled to communicate with the UAP.

WEP Transmit Key This parameter determines which of the four default WEP keys this UAP uses to transmit data. You can set this parameter to a value from 1 to 4. The default is 1, which means the UAP uses the first default WEP key in the WEP Default Keys list on the WEP Default Key Configuration menu.

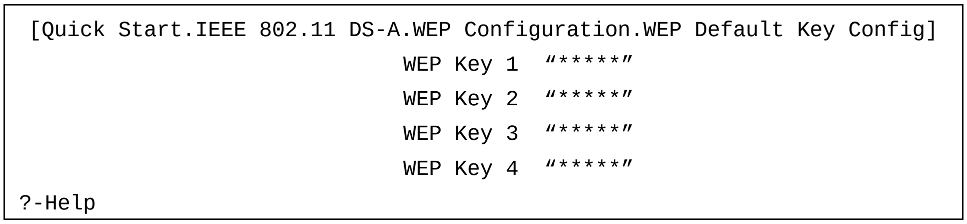
[WEP Default Key Configuration] This command lets you specify the values of the WEP default keys and the mode in which the keys are entered. When you select this command, the following menu appears.



```
 [Quick Start.IEEE 802.11 DS-A.WEP Configuration.WEP Default Key Config]
                       WEP Entry Mode       <ASCII>
                      [WEP Default Keys]
?-Help
```

WEP Entry Mode This parameter indicates whether the WEP default keys are entered in ASCII or hexadecimal (hex) format. The default is ASCII.

[WEP Default Keys] This command lets you set the values for the WEP default keys. The UAP can receive a WEP encryption that uses any of the four WEP default keys. When you select this command, the following menu appears.



```
 [Quick Start.IEEE 802.11 DS-A.WEP Configuration.WEP Default Key Config]
                              WEP Key 1  "*****"
                              WEP Key 2  "*****"
                              WEP Key 3  "*****"
                              WEP Key 4  "*****"
?-Help
```

Select a WEP key to configure and press **Enter**. If the WEP entry mode is ASCII, you must enter five ASCII characters in the key. If the WEP entry mode is hex, you must enter five hex pairs in the key. When the WEP entry mode is set to hex, you can type the hex pairs directly into the key. You do not need to enter a special character between each hex pair. The key appears on the screen as you type; however, after you press **Enter**, the key is encrypted and never appears again.

Note: You must enter either five ASCII characters or five hex pairs in a key. If you enter fewer than five ASCII characters or hex pairs, the key is not saved. If you enter more than five ASCII characters or hex pairs, the key is truncated.

Note these important points about using WEP encryption:

- WEP must be enabled on both the UAP and the end devices.
- The WEP default keys must appear in the same order on both the UAP and the end devices.
- The UAP and the end devices must use the same WEP transmit key.

Viewing Version Information

You can verify the version of the firmware in your IEEE 802.11 DS radio by viewing the Version Information menu. The Version Information menu displays the firmware versions in read-only format.

```
            [Quick Start.IEEE 802.11 DS-A.Version Information]
              Primary Firmware Version        “4.0”
              Station Firmware Version        “4.35”
              Tertiary Firmware Version       “4.43”
?-Help
```

Setting Advanced Configurations

You can set advanced configurations using the Advanced Configuration menu.

```
          [Quick Start.IEEE 802.11 DS-A.Advanced Configuration]
             Medium Reservation               <Enabled>
             Reservation Threshold            500
             AP Density                       <Low>
             DTIM Period                      1
             Multicast Rate                   <2 Mbits (Standard)>
            [Transmit Rate Configuration]
?-Help
```

Medium Reservation This parameter lets you enable or disable the use of a reservation threshold. If you enable this parameter, you can set a threshold value using the Reservation Threshold parameter. If you disable this parameter, you cannot set a reservation threshold value. In installations that primarily send very small frames or have no hidden stations, disabling this parameter may improve network response time. The default is disabled. Intermec recommends that you use the default.

Reservation Threshold This parameter only appears on the screen if the Medium Reservation parameter is set to enabled. Reservation threshold specifies the maximum frame size that can be transmitted without using the medium reservation mechanism. Frames equal to or greater than this threshold value use medium reservation to help prevent collisions with frames from other transmitters. The range is 0 to 2346. The default is 500.

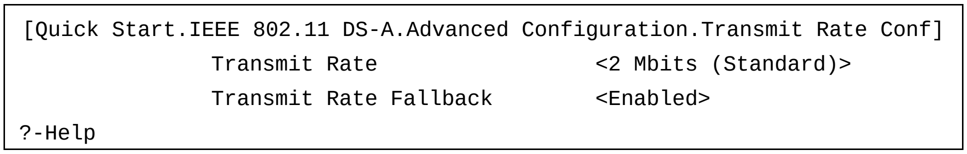
AP Density This parameter controls the roaming sensitivity of your IEEE 802.11 DS end devices. You can set AP density to low, medium, or high. The default AP density is low. You should set the AP density of your end devices to match the AP density of your UAPs.

You can use AP density to virtually reduce the range of your UAP. By increasing the AP density you do not reduce the absolute range of the radio, but the collision detection mechanism is modified to allow significant overlap of the wireless cells. Increasing the AP density allows you to create a higher performance radio network, but it also requires significantly more UAPs to cover a given area.

DTIM Period This parameter specifies the number of beacon frames to skip before including a DTIM (delivery traffic indication message) in a beacon frame. A higher DTIM period may conserve battery life in an end device but may decrease response time. You can set DTIM period to a value from 1 to 65535. The default is 1.

Multicast Rate This parameter determines the bit rate for multicast data transmission. In general, higher speeds mean shorter range and lower speeds mean longer range. If your installation has mixed speed settings, you should set the multicast rate no higher than the maximum speed of the lowest rate end device that must receive multicast traffic. You can set multicast rate to 2 Mbits (Standard) or 1 Mbits (Low). The default is 2 Mbits (Standard).

[Transmit Rate Configuration] This command lets you set the parameters that determine the speed at which this radio will operate. When you select this command, the following menu appears.



```
[Quick Start.IEEE 802.11 DS-A.Advanced Configuration.Transmit Rate Conf]
               Transmit Rate                <2 Mbits (Standard)>
               Transmit Rate Fallback       <Enabled>
?-Help
```

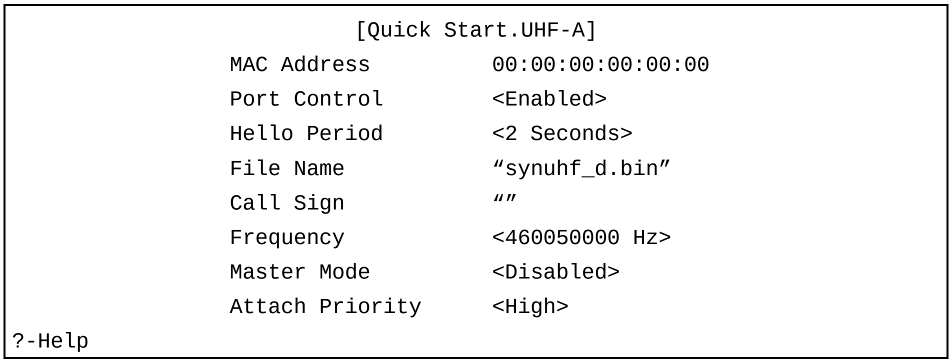
Transmit Rate This parameter lets you set the bit rate for data transmission. Slower transmission rates provide better range; however, faster transmission rates provide increased throughput. You can set the transmission rate to either 2 Mbits (Standard) or 1 Mbits (Low). The default is 2 Mbits (Standard).

Transmit Rate Fallback This parameter determines if the radio will try slower speeds than the specified transmit rate. You can disable or enable transmit rate fallback. A packet may be undeliverable to an end device at a given rate due to interference or range limitations. If you enable transmit rate fallback, the UAP will attempt to deliver the packet at a slower rate, which may have greater range or increased interference tolerance. The default is enabled.

Note: The IEEE 802.11 DS radio features antenna diversity. For information about positioning the antennas for a UAP with an IEEE 802.11 DS radio, see Appendix C, “Positioning Antennas.”

Configuring the UHF Port

You can configure the UHF port by selecting the UHF command from the Quick Start menu. The UHF menu appears.



```
                              [Quick Start.UHF-A]
                 MAC Address          00:00:00:00:00:00
                 Port Control         <Enabled>
                 Hello Period         <2 Seconds>
                 File Name            “synuhf_d.bin”
                 Call Sign            “”
                 Frequency            <460050000 Hz>
                 Master Mode          <Disabled>
                 Attach Priority      <High>
?-Help
```

MAC Address This read-only parameter displays the MAC address of this port.

Port Control This parameter lets you enable or disable the UHF port. The default is enabled.

Hello Period This parameter controls how frequently the UAP broadcasts hello packets on the UHF port. Hello packets are used to maintain the spanning tree. They also serve as beacon messages to synchronize communications with power-managed stations. You can specify hello packets to be broadcast every 1, 2, or 3 seconds. The default is 2 seconds.

File Name This parameter specifies the name of the radio’s driver software. The default file name is synuhf_d.bin.

Note: You should not need to change this name—only change this name when directed to do so by Intermec Technical Support.

Call Sign Agencies that allocate UHF frequencies, such as the Federal Communications Commission (FCC) in the United States, may require that this UAP periodically transmit a call sign. The call sign is granted as part of the FCC license process. Insert the call sign from the FCC license certificate in this parameter. Failure to transmit the call sign is a violation of United States law. Call sign can be from 0 to 12 characters in length.

Note: The Call Sign parameter only applies to radios in the United States. Ignore this parameter if you are outside the United States.

Frequency This parameter displays the frequencies available on your UAP. Some radios have multiple frequencies. The default frequency is the first frequency listed. Due to regulatory constraints in most countries, frequencies can only be programmed by the factory or at service centers equipped to make this change.

Master Mode This parameter determines how channel access is controlled. You can enable or disable master mode. If you enable master mode, the UAP controls channel access for end devices in its coverage area, and end devices automatically operate as slaves. If you disable master mode, all radios in the network cooperate as peers, and UAPs and end devices coordinate channel access as each radio bids for time. The default is disabled. Using the default often provides quicker access times on lightly to moderately loaded systems.

You should only configure master mode to enabled if the UAP radio coverage area does not overlap other access points operating in the same area. Enabling master mode may improve performance in some environments. If master mode is disabled, the UAP can overlap coverage areas with access points on the same or different frequencies.

Attach Priority This parameter only appears on the menu if master mode is disabled. When this radio is operating without a master, you can determine the likelihood that it will obtain media access by setting attach priority to high, medium, or low. An attach priority of high means this radio is more likely than an end device to obtain transmit time. An attach priority of medium means this radio is as equally likely as an end device to obtain transmit time, and an attach priority of low means this radio is less likely than an end device to obtain transmit time. The default attach priority is high.

Attach priority is used in combination with other factors such as loading and signal strength; therefore, an end device may attach to a lower priority access point that provides a better wireless link. End devices ignore the attach priority when selecting between two UAPs that have the same attach priority.

Attach priority is useful when you need a redundant network with some UAPs serving as standby units. If a higher priority UAP fails, end devices fall back to a lower priority UAP within the same coverage area.

Note: You should position the antenna at least 3 meters (10 feet) away from the UAP to achieve the specified performance for the UHF radio.

5

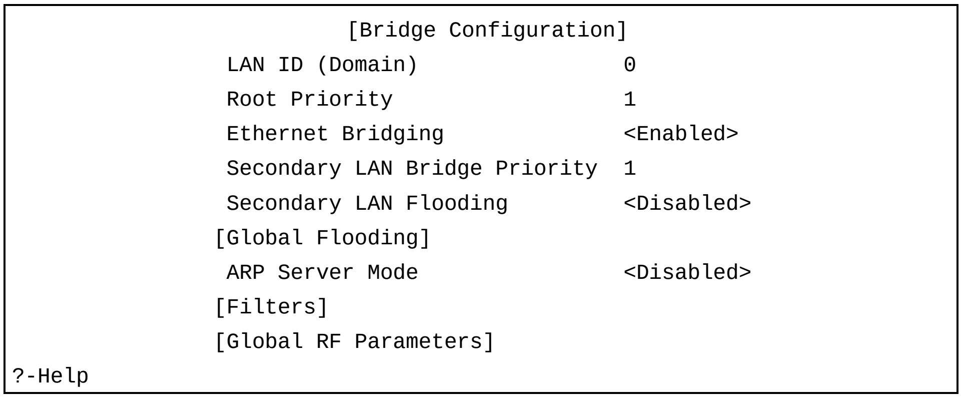
Configuring the Bridging Parameters

5 Configuring the Bridging Parameters

This chapter explains how to use the Bridge Configuration menus to set basic bridging parameters as well as filtering, flooding control, and global RF parameters.

Using the Bridge Configuration Menu

To configure your UAP as a bridge between your wireless devices and your Ethernet network, you may need to set some bridging parameters that define the UAP on your network. If you have more than one UAP on your network, you need to define the root candidates for your INCA primary Ethernet LAN. You may also want to set filters to reduce network traffic. You use the Bridge Configuration menu to set all of these parameters. You also use the Bridge Configuration menu to set global flooding and RF parameters in the root. The Bridge Configuration menu is shown here.



```
                           [Bridge Configuration]
                 LAN ID (Domain)               0
                 Root Priority                 1
                 Ethernet Bridging             <Enabled>
                 Secondary LAN Bridge Priority  1
                 Secondary LAN Flooding        <Disabled>
                [Global Flooding]
                 ARP Server Mode               <Disabled>
                [Filters]
                [Global RF Parameters]
?-Help
```

LAN ID (Domain) The LAN ID or domain identifies the INCA spanning tree. All devices in a wireless network must have the same LAN ID. The range is 0 to 254. The default value is 0.

Root Priority This parameter determines whether this UAP is a candidate to become the root on the primary LAN. The UAP with the highest root priority becomes the root of the network spanning tree whenever the UAP is powered on and active. The Ethernet segment that has the root attached to it is the primary LAN. The root UAP maintains the network spanning tree and can distribute global parameters network-wide.

You can set root priority to a value from 0 to 7. UAPs that have a root priority of 0 cannot become the root. The default root priority is 1. For more information, see “Assigning Root Priority” later in this section.

Note: Always set root priority for a WAP to 0 so it cannot become the root. Also, if the network contains 6710 access points and 21XX UAPs, be sure you configure a UAP as the root.

Ethernet Bridging Ethernet bridging determines how wireless frames are converted to Ethernet frames and vice versa. You can enable or disable Ethernet bridging. When Ethernet bridging is enabled, frames are forwarded directly to the Ethernet network. The default is enabled.

If you set Ethernet bridging to disabled, data link tunneling occurs. That is, the UAP forwards frames on the Ethernet link encapsulated in INCA data frames. Data link tunneling can be used to make roaming transparent to LAN protocols that are not designed to accommodate roaming. For instance, LANE does not accommodate roaming between Ethernet segments that are attached to LANE ATM/Ethernet bridges.

If your network contains LANE ATM/Ethernet bridges or switches that do not support backward learning, you may need to set Ethernet bridging to enabled on the root UAP and to disabled on all other UAPs.

Note: Ethernet bridging is automatically enabled on the root UAP even if you set the Ethernet Bridging parameter to disabled.

Secondary LAN Bridge Priority This parameter determines which UAPs on the secondary LAN are candidates for becoming the designated bridge for the segment. The designated bridge physically connects to a secondary Ethernet LAN and attaches to the distribution LAN through a radio or INCA/IP link. The range for secondary LAN bridge priority is 0 to 7. The default value is 0, which prevents the UAP from becoming the designated bridge. For more information, see “Configuring Bridging on a Secondary Ethernet LAN” later in this section.

Secondary LAN Flooding This option applies to a UAP that is functioning as a designated bridge for the secondary Ethernet LAN. You can enable or disable unicast and multicast flooding to a selected set of secondary LANs. You may need to use secondary LAN flooding to support wired hosts on the secondary LAN. Secondary LAN flooding information is forwarded to inbound UAPs.

The secondary LAN flooding settings are:

Disabled (default)	No flooding occurs (unless enabled by the root).
Multicast	Multicast flooding occurs unless disabled by the root.
Unicast	Unicast flooding occurs unless disabled by the root.
Enabled	Both multicast and unicast flooding occurs unless disabled by the root.

Note: You can enable flooding to all secondary Ethernet LANs by using the Global Flooding parameters. The Global Flooding parameters apply to the entire network and override these secondary LAN flooding settings in individual designated bridges. To enable global flooding, set the Multicast Outbound to Secondary LANs parameter to enabled, or set the Unicast Outbound to Secondary LANs parameter to enabled.

[Global Flooding] Global flooding parameters set in the root apply to the entire network. For more information, see “Using Global Flooding” later in this chapter.

ARP Server Mode This parameter determines how TCP/IP ARP requests are handled by the UAP. When ARP server mode is enabled, the ARP server learns the IP addresses of wireless stations by monitoring ARP packets and explicit IP address registration and then stores the addresses in its forwarding database.

ARP server mode converts multicast ARP requests to unicast ARP requests for end devices in its forwarding database. Using ARP server mode can significantly improve wireless network performance in busy IP networks. Additionally, some end devices may have the capability of explicitly registering IP addresses with the ARP server.

The ARP server mode settings are:

Disabled (default) No special action is taken when an ARP is received.

No Flooding ARP server tries to convert ARP requests from multicast to unicast. This is the most efficient setting because multicast ARPs are never forwarded. Use this setting if end devices do not need to respond to ARPs. You can also use this setting if end devices periodically register their IP addresses with the ARP server, or if end devices send an initial inbound ARP request before receiving any outbound data.

Normal Flooding If the destination address is unknown, the ARP request is flooded according to the multicast flood level settings. Use this setting when devices need to answer ARP requests but are not capable of registering IP addresses with the UAP. This setting filters ARP requests that have a target address for an end device on the Ethernet LAN, if the IP/MAC address bindings are known.

[Filters] This menu option takes you to the Filters menu. You can set filters so that particular types of frames are either passed or dropped. For more information, see “Using Filters” later in this chapter.

[Global RF Parameters] This menu option takes you to the Global RF Parameters menu. For more information, see “Setting Global RF Parameters” later in this chapter.

Assigning Root Priority

You should assign the highest root priority to one UAP on the primary LAN so that it serves as the primary root. You should configure one or two UAPs on the primary LAN with a lower priority so they can serve as fallback roots. You should configure the remaining UAPs on the primary LAN with a root priority of 0.

If the root becomes inactive, the remaining root candidates negotiate to determine which UAP becomes the new root. If you assign the same root priority to 2 or more UAPs, the UAP with the highest Ethernet address becomes the root.

Intermec recommends that the root be a UAP that is on the same LAN as your servers. The root UAP should also be a UAP that does not otherwise handle a large volume of traffic.

You should assign all UAPs on secondary LANs a root priority of 0 so they can never become the root. You should also configure all WAPs with a root priority of 0; you should never allow a WAP to become a root candidate.

If you are configuring OpenAir UAPs for point-to-point bridging, you must configure the OpenAir master on the primary LAN with a higher root priority than the OpenAir station UAP on the secondary LAN for the bridge to form correctly.

Note: If a UAP has a root priority of 0 and it cannot attach to the INCA network, it disables its radio ports. By disabling its radio ports, the UAP prevents end devices from associating with a UAP that cannot forward frames to or from the network.

Configuring Bridging on a Secondary Ethernet LAN

A secondary Ethernet LAN can be bridging or non-bridging. A bridging secondary Ethernet LAN interconnects UAPs and provides a wireless connection for wired Ethernet hosts. A bridging secondary Ethernet LAN also has a UAP that is the designated bridge to the primary LAN. A non-bridging secondary Ethernet LAN interconnects UAPs but has no designated bridge.

In general, you should enable bridging on a secondary LAN unless the inbound path is through an INCA/IP tunnel or through a bridge or switch that does not support roaming. Bridges and switches that adhere to the IEEE 802.1d standard support roaming. Some proprietary VLAN switches and ATM LANE bridges do not support roaming. If you have wired hosts on the secondary LAN, you must enable bridging to the secondary LAN.

To enable bridging, set the Secondary LAN Bridge Priority parameter to a value greater than zero. The UAP with the highest secondary LAN bridge priority becomes the designated bridge whenever it is powered on and connected to the secondary LAN, if it is within range of a UAP on the primary LAN.

If two UAPs have the same secondary LAN bridge priority, the UAP with the highest Ethernet address becomes the designated bridge. If the current designated bridge goes offline, the remaining candidates negotiate to determine which UAP becomes the new designated bridge.

If a UAP has the highest bridge priority on the secondary LAN, but it is not in the radio coverage area of a UAP on the primary LAN, it cannot become the designated bridge. In this case, a UAP with a lower bridge priority becomes the designated bridge.

A secondary LAN bridge priority of 0 prohibits the UAP from becoming the designated bridge. If all UAPs connected to a secondary LAN have a bridge priority of 0, then a non-bridging secondary LAN exists and bridging to the secondary LAN is automatically disabled.

Note: If a switch fails, then the INCA spanning tree protocol can automatically bridge around the failed switch with a wireless link. However, if your installation has switches that use a proprietary configuration protocol, you may not want to bridge around the switches. Set secondary LAN bridge priority to 0 in this case.

Using Global Flooding

You can use the Global Flooding menu to set system-wide flooding parameters in the root UAP that are distributed throughout the network. Note that a UAP makes flooding decisions only after frames have been received and filtered.

Unicast frames have a unique physical address. Multicast frames have group addresses. (Note that a broadcast frame is a special case of a multicast frame.) Many network protocols use multicast messages for establishing and maintaining connections and use unicast messages for data exchange. You can use the Global Flooding menu to set global flooding parameters for both unicast and multicast frames.

A UAP normally forwards frames only to destination addresses it has learned and stored in its forwarding database. Frames are forwarded only on the port that provides the shortest path to the destination address. You can configure a UAP to flood the frame in certain directions when it has not learned the direction of the shortest path. A UAP cannot learn the location of a multicast address; therefore, multicast frames are always flooded.

The Global Flooding menu is shown here.

```
                  [Bridge Configuration.Global Flooding]
        Multicast Flood Mode                 <Hierarchical>
        Multicast Outbound to Terminals      <Enabled>
        Multicast Outbound to Secondary LANs <Set locally>
        Unicast Flood Mode                   <Disabled>
?-Help
```

Multicast Flood Mode This network-wide parameter determines the flooding structure for multicast frames.

The multicast flood mode settings are:

Hierarchical (default) Nodes in the radio network communicate exclusively with nodes on the primary LAN. A node in the radio network does not communicate with other nodes in the radio network.

Universal Any node can communicate with any other node. For example, a device in the radio network may communicate with another device in the radio network or with a server on a secondary LAN.

Disabled Multicast frames are not flooded.

Multicast Outbound to Terminals This network-wide parameter controls if outbound multicast frames are flooded to wireless devices. This parameter may be set to enabled or disabled. The default is enabled.

Multicast Outbound to Secondary LANs This network-wide parameter controls if outbound multicast frames are flooded to secondary LAN segments. The possible settings are enabled and set locally. You can use the enabled setting to globally enable flooding to all secondary LANs. The setting of enabled allows the root to override local secondary LAN flooding options for all UAPs serving as designated bridges for secondary LANs. The set locally setting allows flooding to be controlled by the designated bridge on that secondary LAN. The default is set locally.

Unicast Flood Mode This network-wide parameter determines the flooding structure for unicast frames.

The unicast flood mode settings are:

Hierarchical	Nodes in the radio network communicate exclusively with nodes on the primary LAN. A node in the radio network does not communicate with other nodes in the radio network.
Universal	Any node can communicate with any other node. For example, a device in the radio network may communicate with another device in the radio network or with a server on a secondary LAN.
Disabled (default)	Unicast frames are not flooded. (Unicast flooding is not required for Intermec terminal emulation applications.)

Unicast Outbound to Terminals This parameter only appears if the Unicast Flood Mode parameter is set to hierarchical or universal. This network-wide parameter controls if outbound unicast frames are flooded to wireless devices. You can set this parameter to enabled or disabled. The default is disabled.

You can set the Unicast Outbound to Terminals parameter to disabled if any of the following statements apply to your network:

- All stations in the radio network periodically generate traffic as least once every four minutes.
- All stations in the radio network explicitly attach to the network.
- Any outbound unicast message that is destined to a station in the radio network is always preceded by an inbound message from the station. This situation occurs in some terminal emulation and client/server applications.

Unicast Outbound to Secondary LANs This option only appears if the Unicast Flood Mode parameter is set to hierarchical or universal. This option controls if outbound unicast frames are flooded to secondary LAN segments. The possible settings are enabled and set locally. A setting of enabled allows the root to control flooding for all UAPs that are serving as designated bridges for secondary LANs. Set locally allows flooding to be controlled by the designated bridge on that secondary LAN. The default is set locally.

Using Filters

You can use filters to help reduce unnecessary traffic on your network. The Ethernet receive filters prevent network traffic from being forwarded unnecessarily into the radio network. INCA/IP transmit filters limit the protocol types that can pass through an INCA/IP tunnel.

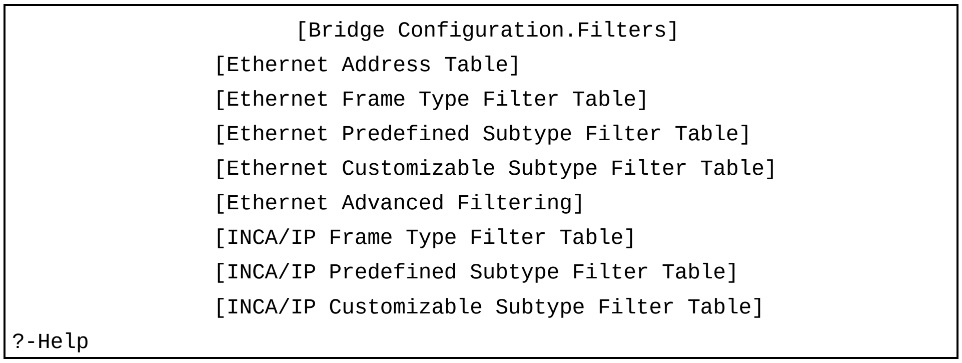
Consider these points before setting Ethernet filters:

- Set Ethernet input filters when you need to reduce the amount of traffic that is forwarded into the radio network.
- If you disabled unicast flooding in the root, you do not need to create Ethernet filters for unicast traffic.
- If you disabled multicast flooding in the root, you do not need to create Ethernet filters for multicast traffic.
- Unicast flooding is automatically disabled on 900 MHz Falcon and INCA/IP ports.

You must configure the filters on each UAP independently. For more information about INCA/IP and filtering, see Appendix B, “Understanding INCA/IP.”

Understanding the Filters Menu

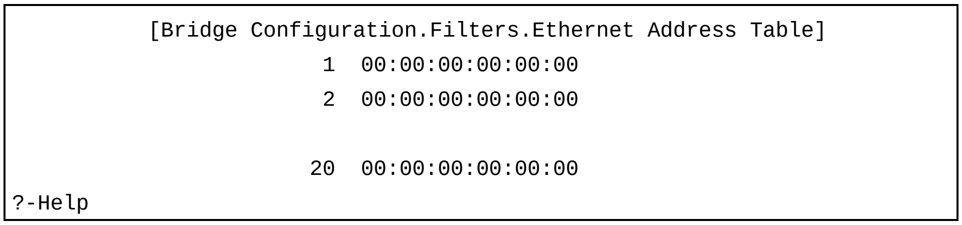
You can set both Ethernet and INCA/IP filters from the Filters menu. You use the Ethernet type and subtype menus to create protocol filters for predefined and user-defined protocol types. You use the Ethernet Advanced Filtering menu to define arbitrary frame filters based on frame content. When you select an option on the Filters menu, you go to a filter table where you can set specific filtering parameters. The filter tables are described in the following sections.



```
                       [Bridge Configuration.Filters]
                [Ethernet Address Table]
                [Ethernet Frame Type Filter Table]
                [Ethernet Predefined Subtype Filter Table]
                [Ethernet Customizable Subtype Filter Table]
                [Ethernet Advanced Filtering]
                [INCA/IP Frame Type Filter Table]
                [INCA/IP Predefined Subtype Filter Table]
                [INCA/IP Customizable Subtype Filter Table]
?-Help
```

Using the Ethernet Address Table Menu

You can use the Ethernet Address Table menu to define up to 20 permanent unicast 802 MAC addresses that are connected to this Ethernet port. These addresses become permanent entries in the route table of the UAP. The entries are useful when configuring designated bridges for secondary LANs because they reduce the need to flood frames to wired devices on the secondary LAN segments. A portion of the Ethernet Address Table menu appears below.



```
           [Bridge Configuration.Filters.Ethernet Address Table]
                        1  00:00:00:00:00:00
                        2  00:00:00:00:00:00

                       20  00:00:00:00:00:00
?-Help
```

Select an entry in the table and then enter a MAC address. The address must be 6 hex pairs separated by spaces, colons, or hyphens. The default is 00:00:00:00:00:00.

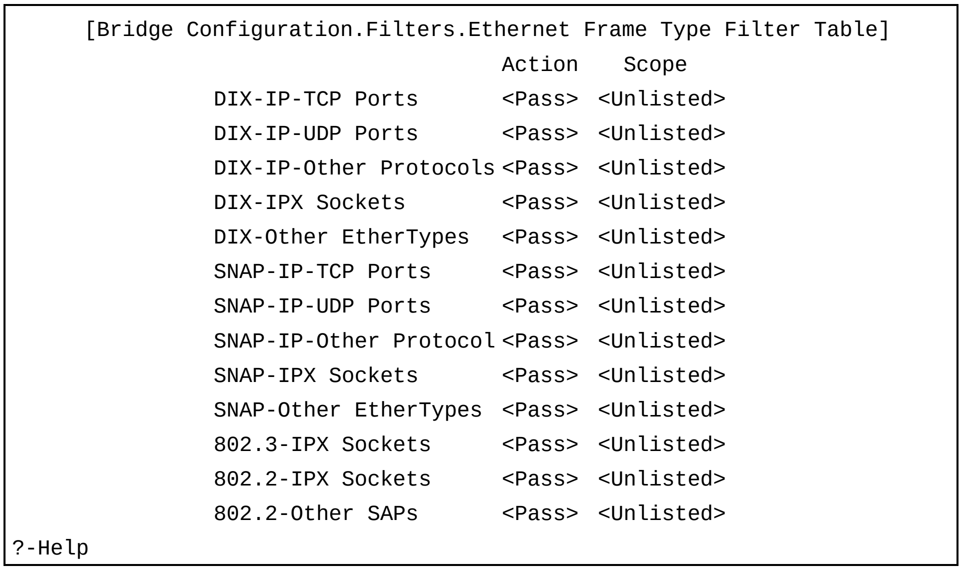
Using the Ethernet Frame Type Filter Table Menu

You can use the Ethernet Frame Type Filter Table menu to establish filters for common networking protocols such as IP, Novell IPX, and 802.2 LLC. You can set filters to pass only those Ethernet frame types found on your network.

Use the Ethernet Frame Type Filter Table menu to set the default action for general frame types. Use the subtype tables to set the action for specific frame types. For example, you can set the DIX-Other EtherTypes frame type parameter to drop, and then use the subtype menus to pass only those specific DIX types that are used in your radio network.

If you want to drop or pass all frames of a general protocol type, you can set the scope for that frame type to all in the Ethernet Frame Type Filter Table. For example, if you set the action to drop and the scope to all for DIX-IP-TCP Ports, then all IP packets with the TCP protocol type will be dropped even if specific TCP ports are set to pass in the subtype menus.

Ethernet Frame Type Filter Table Menu



```
      [Bridge Configuration.Filters.Ethernet Frame Type Filter Table]
                                      Action   Scope
                DIX-IP-TCP Ports      <Pass>  <Unlisted>
                DIX-IP-UDP Ports      <Pass>  <Unlisted>
                DIX-IP-Other Protocols<Pass>  <Unlisted>
                DIX-IPX Sockets       <Pass>  <Unlisted>
                DIX-Other EtherTypes  <Pass>  <Unlisted>
                SNAP-IP-TCP Ports     <Pass>  <Unlisted>
                SNAP-IP-UDP Ports     <Pass>  <Unlisted>
                SNAP-IP-Other Protocol<Pass>  <Unlisted>
                SNAP-IPX Sockets      <Pass>  <Unlisted>
                SNAP-Other EtherTypes <Pass>  <Unlisted>
                802.3-IPX Sockets     <Pass>  <Unlisted>
                802.2-IPX Sockets     <Pass>  <Unlisted>
                802.2-Other SAPs      <Pass>  <Unlisted>
?-Help
```

Action You can set the action so the UAP will either pass or drop all frames of a specified type. The default is pass.

Scope Scope can be set to unlisted or all. If you select all, then all frames of that type are unconditionally passed or dropped, depending upon the action specified. If you select unlisted, frames of that type are passed or dropped only if the frame type is not listed in the predefined or customizable tables.

The following table provides information about various frame types.

DIX IP TCP Ports DIX IP UDP Ports SNAP IP TCP Ports SNAP IP UDP Ports	Primary Internet Protocol Suite (IP) transport protocols.
DIX IP Other Protocols SNAP IP Other Protocols	IP protocols other than TCP or User Datagram Protocol (UDP).
DIX IPX Sockets	Novell NetWare protocol over Ethernet II frames.
SNAP IPX Sockets	Novell NetWare protocol over 802.2 SNAP frames.
802.3 IPX Sockets	Novell NetWare protocol over 802.3 RAW frames.

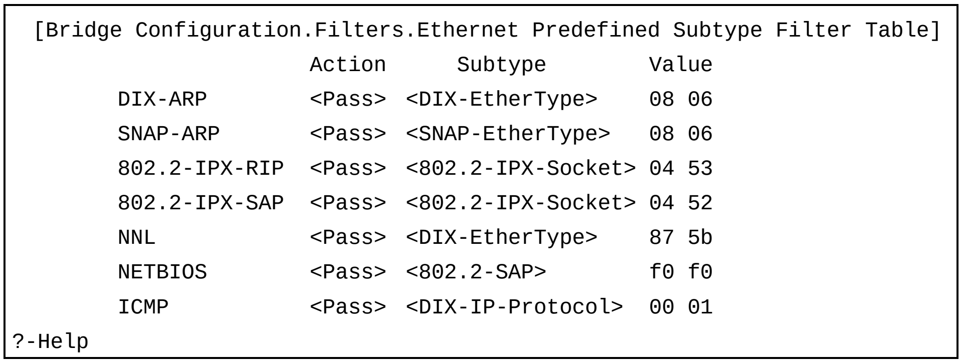
Frame Types (continued)

DIX Other Ethernet Types SNAP Other Ethernet Types	DIX or SNAP registered protocols other than IP or IPX.
802.2 IPX Sockets	Novell running over 802.2 Logical Link Control (LLC).
802.2 Other SAPs	802.2 SAPs other than IPX or SNAP.

Note: You cannot filter HTTP, Telnet, SNMP, and ICMP protocol ports because they are used for configuration and management of the UAP. Additionally, you cannot filter broadcast ARP request frames if the target IP address belongs to the local UAP or to a UAP in the sub tree rooted at the local UAP.

Using the Ethernet Predefined Subtype Filter Table Menu

You can use the Ethernet Predefined Subtype Filter Table menu to set filters on certain frame subtypes.



```
 [Bridge Configuration.Filters.Ethernet Predefined Subtype Filter Table]
                      Action     Subtype        Value
       DIX-ARP        <Pass>  <DIX-EtherType>    08 06
       SNAP-ARP       <Pass>  <SNAP-EtherType>   08 06
       802.2-IPX-RIP  <Pass>  <802.2-IPX-Socket> 04 53
       802.2-IPX-SAP  <Pass>  <802.2-IPX-Socket> 04 52
       NNL            <Pass>  <DIX-EtherType>    87 5b
       NETBIOS        <Pass>  <802.2-SAP>        f0 f0
       ICMP           <Pass>  <DIX-IP-Protocol>  00 01
?-Help
```

Action You can set the action to either pass or drop all frames of that type.

Subtype This read-only field displays the frame subtype.

Value This read-only field provides information about the subtype value.

Using the Ethernet Customizable Subtype Filter Table Menu

You can use the Ethernet Customizable Subtype Filter Table menu to create customized filters. You can define the Subtype, Action, and Value parameters. Value allows you to specify an individual DIX type, protocol port, socket, or SAP to be specified for each of the listed frame types. The filter is applied if either the source or destination field in the frame matches the specified DIX type, port, socket, or SAP. A value of 00 00 denotes the subtype as unlisted.

A portion of the Customizable Subtype Filter Table menu is shown here.

```
 [Bridge Configuration.Filters.Ethernet Customizable Subtype Filter Tbl]
                  Action       SubType       Value
               1  <Pass>  <DIX-IP-TCP-Port>  00 00
               2  <Pass>  <DIX-IP-TCP-Port>  00 00

               12 <Pass>  <DIX-IP-TCP-Port>  00 00
?-Help
```

When you select a filter, the following menu appears.

```
 [Bridge Configuration.Filters.Ethernet Predefined Subtype Filter Tbl.1]
                           Action     <Pass>
                           SubType    <DIX-IP-TCP-Port>
                           Value      00 00
?-Help
```

Action You can set the action to either pass or drop all frames of that type.

Subtype When you select subtype, the SubType dialog box appears. You can select the frame subtype you wish to filter.

Value Refer to the next table for the value for a specific subtype. The value must be 2 hex pairs. To enter a port value, you must enter it as a decimal. For example, enter “23.” for port 23. The UAP displays the hexadecimal equivalent in the values field on the menu. When a match is found between frame subtype and value, the specified action is taken.

The following table describes frame subtypes and their values.

Subtype	Value
DIX-IP-TCP-Port	Port value in hexadecimal.
DIX-IP-UDP-Port	Port value in hexadecimal.
DIX-IP-Protocol	Protocol number in hexadecimal.
DIX-IPX-Socket	Socket value in hexadecimal.
DIX-EtherType	Specify the registered DIX type in hexadecimal.
SNAP-IP-TCP-Port	Port value in hexadecimal.
SNAP-IP-UDP-Port	Port value in hexadecimal.
SNAP-IP-Protocol	Port value in hexadecimal.
SNAP-IPX-Socket	Socket value in hexadecimal.

Frame Subtypes and Values (continued)

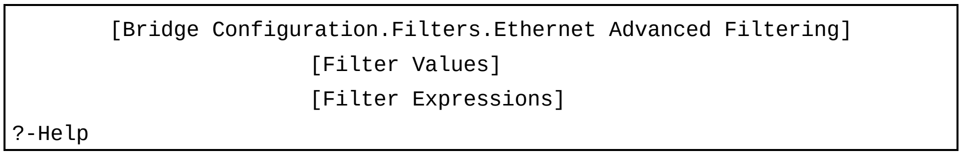
Subtype	Value
SNAP-EtherType	SNAP type in hexadecimal. To filter on both SNAP type and OUI, use advanced filters.
802.3-IPX-Socket	Socket value in hexadecimal.
802.2-IPX-Socket	Socket value in hexadecimal.
802.2-SAP	802.2 SAP in hexadecimal.

Using Ethernet Advanced Filtering

If you need more flexibility in your filtering, you can use the Ethernet Advanced Filtering menu. Settings for advanced filters execute after those for other filters. That is, advanced filters are only applied if the frame has passed the other filters. If the frame was dropped by earlier filters, the advanced filter will not be applied.

You can use filter values and filter expressions to minimize network traffic over the RF links; however, you should only use advanced Ethernet filtering if you have an extensive understanding of network frames and their contents. You should use other existing filters whenever possible.

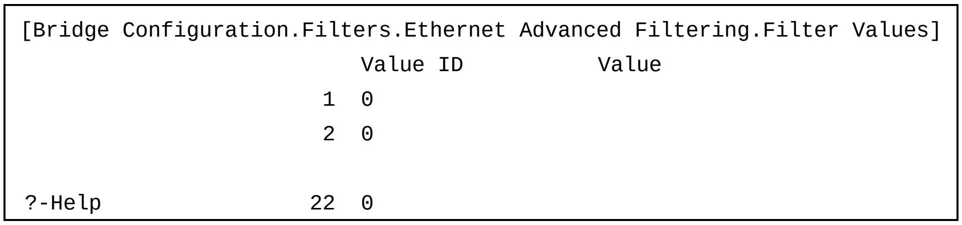
You can delete a protocol filter by setting its value to 0. You can delete an advanced filter expression or value by setting the ExprSeq or Value ID parameter to 0. When you select Ethernet Advanced Filtering, the following menu appears.



```
        [Bridge Configuration.Filters.Ethernet Advanced Filtering]
                        [Filter Values]
                        [Filter Expressions]
?-Help
```

Setting Filter Values

You can use the Filter Values menu to associate an ID with a pattern value. Select a filter, and then enter an ID and a value. You can enter up to 22 values. A value can be from 0 to 8 hexadecimal bytes. All values that have the same value ID belong to the same list. The Filter Values menu is shown here.



```
[Bridge Configuration.Filters.Ethernet Advanced Filtering.Filter Values]
                           Value ID          Value
                        1  0
                        2  0

?-Help                 22  0
```

Value ID You can set the value ID to any value from 0 to 255.

Value You can set the value for the filter. The range is 8 hex pairs.

Setting Filter Expressions

You can set filter expressions by specifying parameters for packet filtering. You can enter up to 22 expressions. A portion of the Filter Expressions menu is shown below.

```
[Bridge Configuration.Filters.Ethernet Advanced Filtering.Filter Expns]
        ExprSeq   Offset         Mask        OP      Value ID    Action
  1     0          0                         <EQ>    0           <And>
  2     0          0                         <EQ>    0           <And>

?-22    0          0                         <EQ>    0           <And>
```

You can create a filter expression. These expressions are executed in ascending order based on the ExprSeq values until the UAP determines whether to pass or drop the frame. When you select an option from the Filter Expressions menu, the following menu appears.

```
 [Bridge Configuration.Filters.Ethernet Advanced Filtering.Filter Exp.1]
                              ExprSeq   0
                              Offset    0
                              Mask
                              Op        <EQ>
                              Value ID  0
                              Action    <And>
?-Help
```

ExprSeq You can use the expression sequence parameter to chain expressions together for filtering. The ExprSeq parameter works with the Action parameter. For example, if the action is set to And, then the next sequence in another expression is processed. After you change the parameter, the statements are physically reordered and renumbered so the expression sequence order is maintained. The range is from 0 to 255.

Offset You can use the offset to identify a point inside a packet where testing for the expression is to start. Offset values can range from 0 to 65535.

Mask You can enter a data pattern that is applied to the packet. If the data pattern in the mask matches the packet, then the specified action is performed. The mask indicates the bits that are significant at the specified offset. A bit is significant if a bit in the mask is set to one. If this field is empty, the length of the field is determined by the longest value in the Filter Values menu for the specified value ID. The mask values are entered in hexadecimal pairs. You can enter 0 to 8 pairs.

Op (Operation) When a data pattern matches a value in the Filter Values menu, a logical operation is performed to determine if the specified action should be taken. Valid operations include:

- EQ (equal)
- NE (not equal)
- GT (greater than)
- LT (less than or equal)

Value ID Each expression contains a value ID. Value ID represents a value in the Filter Values menu. The bytes after the packet offset are compared to the data pattern indicated by the value. Value ID can be from 0 to 255 and must match one or more value IDs in the Filter Values menu.

Action You can set the action to pass, drop, or and. If you set the action to and, then the filter expression that has the next highest expression sequence is applied.

Ethernet Advanced Filtering Example

This example shows how to use the Ethernet advanced filters to

- discard all DIX IP multicast frames except those from a selected list of Ethernet stations.

The following menu shows the filter values for this example.

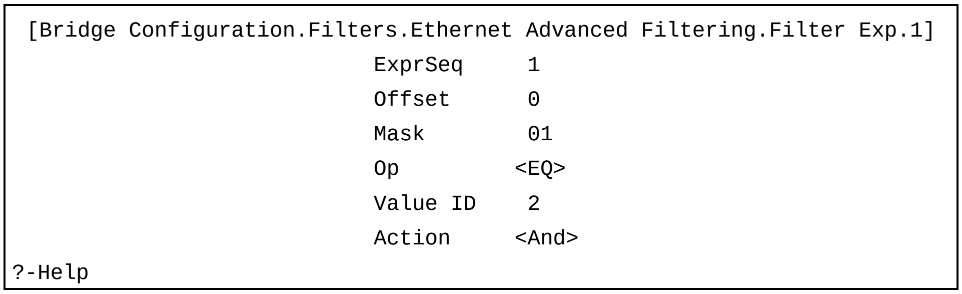
```
[Bridge Configuration.Filters.Ethernet Advanced Filtering.Filter Values]
                   Value ID          Value
                1  1                 0800
                2  2                 01
                3  3                 00c0b2000001
                4  3                 00c0b2000002
                5  3                 00c0b2000003

?-Help          22 0
```

Note that three entries in the value column all have the same value ID of 3. This example demonstrates how to enter a list—all entries that have the same value ID belong to the same list.

The following table describes the values shown in the filter values example.

Value ID	Value	Description
1	0800	Check for a DIX IP frame.
2	01	Check for a multicast/broadcast frame.
3	00c0b2000001 00c0b2000002 00c0b2000003	Check for these specific Ethernet station addresses.

The following menu shows the first filter expression.

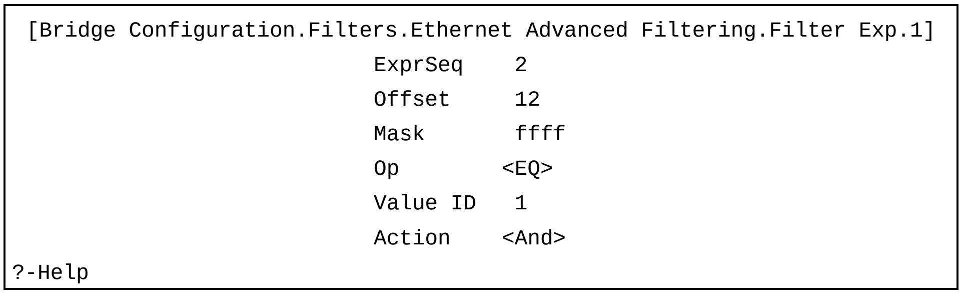


```
 [Bridge Configuration.Filters.Ethernet Advanced Filtering.Filter Exp.1]
                          ExprSeq     1
                          Offset      0
                          Mask        01
                          Op         <EQ>
                          Value ID    2
                          Action     <And>
?-Help
```

The following table explains the first filter expression.

Parameter	Value	Explanation
ExprSeq	1	This is the first expression.
Offset	0	The offset is zero. Look at the first byte of the destination address.
Mask	01	Only check the Ethernet multicast bit.
OP	EQ	Compare the value at the offset to the value specified on the Filter Values menu to see if they are equal. (If the value at the offset equals the specified value on the Filter Values menu, the frame is multicast, in this example.)
Value ID	2	Use the value from the Filter Values menu whose value ID is 2.
Action	And	If this filter expression is true, continue to the next expression.

The following menu shows the second filter expression.

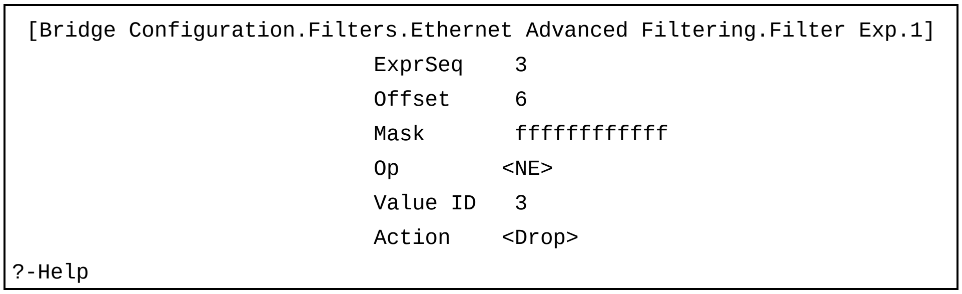


```
 [Bridge Configuration.Filters.Ethernet Advanced Filtering.Filter Exp.1]
                            ExprSeq    2
                            Offset     12
                            Mask       ffff
                            Op        <EQ>
                            Value ID   1
                            Action    <And>
?-Help
```

The following table explains the second filter expression.

Parameter	Value	Explanation
ExprSeq	2	This is the second expression.
Offset	12	The data for this expression begins at an offset of 12 bytes from the beginning of the destination address. (Check for DIX IP frame type, in this example.)
Mask	ffff	Check two bytes for an exact match.
OP	EQ	Compare the value at the offset to the value specified on the Filter Values menu to see if they are equal. (If the value at the offset equals the specified value from the Filter Values menu, the frame is DIX IP, in this example.)
Value ID	1	Use the value from the Filter Values menu whose value ID is 1.
Action	And	If this filter expression is true, continue to the next expression.

The following menu shows the third filter expression.



```
 [Bridge Configuration.Filters.Ethernet Advanced Filtering.Filter Exp.1]
                            ExprSeq    3
                            Offset     6
                            Mask       ffffffffffff
                            Op        <NE>
                            Value ID   3
                            Action    <Drop>
?-Help
```

The following table explains the third filter expression.

Parameter	Value	Explanation
ExprSeq	3	This is the third expression.
Offset	6	The data for this expression begins at an offset of 6 bytes from the beginning of the destination address. (Check the source Ethernet address, in this example.)
Mask	ffffffffffff	Check six bytes for an exact match.
OP	NE	Compare the value at the offset to the value specified on the Filter Values menu to see if they are not equal. (Compare the source Ethernet address with the list of Ethernet addresses from the Filter Values menu.)
Value ID	3	Use the value from the Filter Values menu whose value ID is 3.
Action	Drop	If the source Ethernet address does not match any address included in the list on the Filter Values menu, then drop the frame.

The three expressions in this example combine to form a single compound expression. The compound expression forms an advanced filter that drops all DIX IP multicast frames except those from the three Ethernet stations whose addresses are listed on the Filter Values menu.

The default action is always the opposite of the action specified in the last expression. In this example, the action of the last expression is drop; therefore, the default action is pass. Any frame that meets the conditions specified in the advanced filter is passed.

Using the INCA/IP Frame Type Filter Table Menu

You can use the INCA/IP Frame Type Filter Table menu to set output INCA/IP port filters for certain types of INCA/IP frames. You configure INCA/IP output filters the same way that you configure Ethernet input filters.

Permanent INCA/IP output port filters prevent unwanted frame forwarding through an INCA/IP tunnel. For detailed information about frames that are never forwarded, see “Frame Types That Are Never Forwarded” in Appendix B. IP ICMP packets with the following types are forwarded:

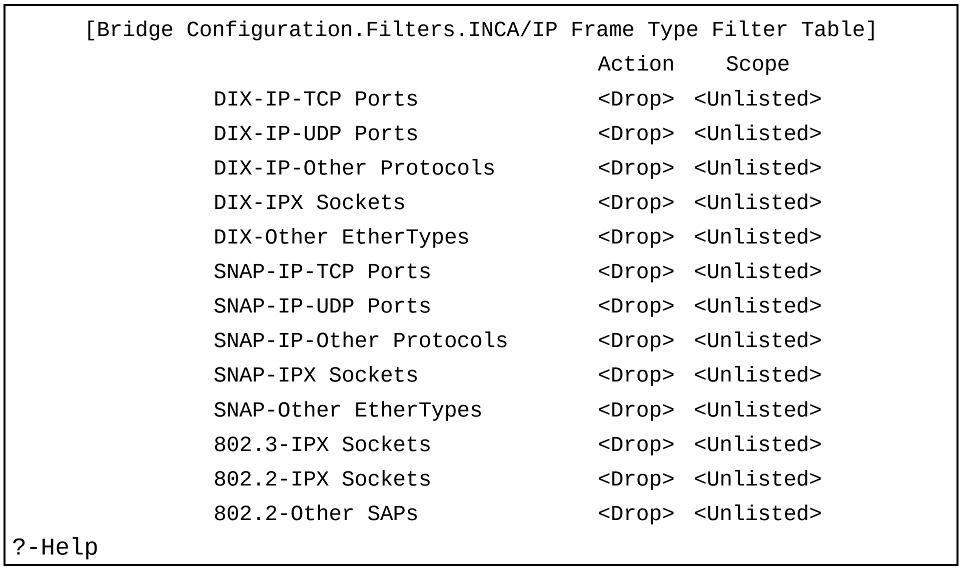
- Echo Request
- Echo Reply
- Destination Unreachable
- Source Quench
- Redirect
- Alternate Host Address

ICMP Packet Types That Are Forwarded (continued)

- Time Exceeded
- Parameter problem
- Time Stamp
- Time Stamp Reply
- Address Mask Request
- Address Mask Reply
- Trace Route

An IP or ARP frame is never forwarded inbound through an INCA/IP tunnel unless the source IP address belongs to the home IP subnet. The home subnet is the IP subnet that is physically connected to the root UAP. An IP frame is never forwarded outbound through an INCA/IP tunnel unless the destination belongs to the home subnet.

The INCA/IP Frame Type Filter Table menu is shown here.



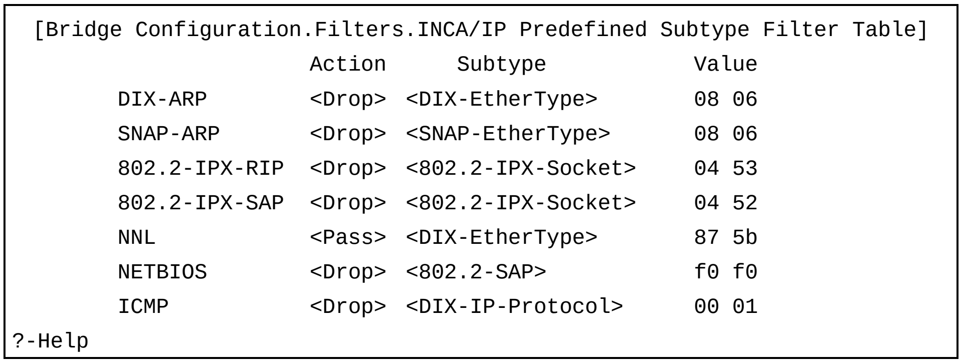
```
      [Bridge Configuration.Filters.INCA/IP Frame Type Filter Table]
                                              Action    Scope
                DIX-IP-TCP Ports              <Drop> <Unlisted>
                DIX-IP-UDP Ports              <Drop> <Unlisted>
                DIX-IP-Other Protocols        <Drop> <Unlisted>
                DIX-IPX Sockets               <Drop> <Unlisted>
                DIX-Other EtherTypes          <Drop> <Unlisted>
                SNAP-IP-TCP Ports             <Drop> <Unlisted>
                SNAP-IP-UDP Ports             <Drop> <Unlisted>
                SNAP-IP-Other Protocols       <Drop> <Unlisted>
                SNAP-IPX Sockets              <Drop> <Unlisted>
                SNAP-Other EtherTypes         <Drop> <Unlisted>
                802.3-IPX Sockets             <Drop> <Unlisted>
                802.2-IPX Sockets             <Drop> <Unlisted>
                802.2-Other SAPs              <Drop> <Unlisted>
?-Help
```

Action You can set the filter to either pass or drop that type of frame.

Scope The scope can be set to either unlisted or all. If you select all, then all frames of that type are filtered. If you set the scope to unlisted, then frames of that type are filtered only if they are not in the predefined or customizable INCA/IP tables described later in this chapter.

Using the INCA/IP Predefined Subtype Filter Table Menu

You can use the INCA/IP Predefined Subtype Filter Table menu to set filters on certain frame subtypes.



```
 [Bridge Configuration.Filters.INCA/IP Predefined Subtype Filter Table]
                      Action     Subtype           Value
       DIX-ARP        <Drop>  <DIX-EtherType>       08 06
       SNAP-ARP       <Drop>  <SNAP-EtherType>      08 06
       802.2-IPX-RIP  <Drop>  <802.2-IPX-Socket>    04 53
       802.2-IPX-SAP  <Drop>  <802.2-IPX-Socket>    04 52
       NNL            <Pass>  <DIX-EtherType>       87 5b
       NETBIOS        <Drop>  <802.2-SAP>           f0 f0
       ICMP           <Drop>  <DIX-IP-Protocol>     00 01
?-Help
```

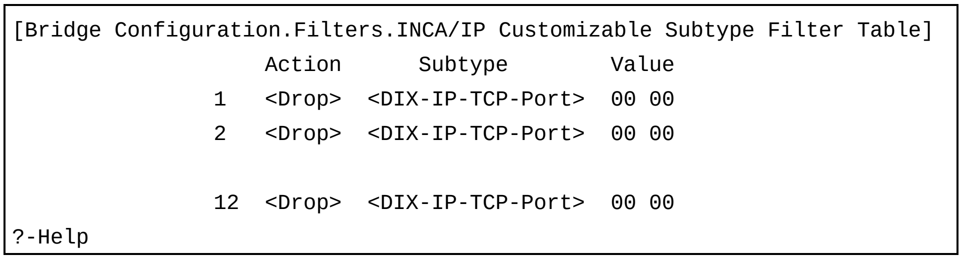
Action You can set the filter to either pass or drop the frame subtype.

Subtype This read-only field provides information about the subtype.

Value This read-only field provides information about the subtype value.

Using the INCA/IP Customizable Subtype Filter Table Menu

You can use the INCA/IP Customizable Subtype Filter Table menu to create customized filters. A portion of the INCA/IP Customizable Subtype Filter Table menu is shown here.



```
[Bridge Configuration.Filters.INCA/IP Customizable Subtype Filter Table]
                   Action      Subtype        Value
               1   <Drop>  <DIX-IP-TCP-Port>  00 00
               2   <Drop>  <DIX-IP-TCP-Port>  00 00

               12  <Drop>  <DIX-IP-TCP-Port>  00 00
?-Help
```

Action You can set the filter to either pass or drop the frame subtype.

Subtype When you select subtype, the SubType dialog box appears. You can select the frame subtype you wish to filter.

Value Refer to the table on the following page for information about the value for a specific subtype. The value must be 2 hex pairs. To enter a port value, you must enter it as a decimal. For example, enter “23.” for port 23. The UAP displays the hexadecimal equivalent in the values field on the menu. When a match is found between the frame subtype and the value, the specified action is taken.

Frame Subtypes and Values

Subtype	Value
DIX-IP-TCP-Port	Port value in hexadecimal.
DIX-IP-UDP-Port	Port value in hexadecimal.
DIX-IP-Protocol	Protocol number in hexadecimal.
DIX-IPX-Socket	Socket value in hexadecimal.
DIX-EtherType	Specify the registered DIX type in hexadecimal.
SNAP-IP-TCP-Port	Port value in hexadecimal.
SNAP-IP-UDP-Port	Port value in hexadecimal.
SNAP-IP-Protocol	Port value in hexadecimal.
SNAP-IPX-Socket	Socket value in hexadecimal.
SNAP-EtherType	SAP in hexadecimal. To filter on both SAP and OUI, use advanced filters.
802.3-IPX-Socket	Socket value in hexadecimal.
802.2-IPX-Socket	Socket value in hexadecimal.
802.2-SAP	SAP in hexadecimal

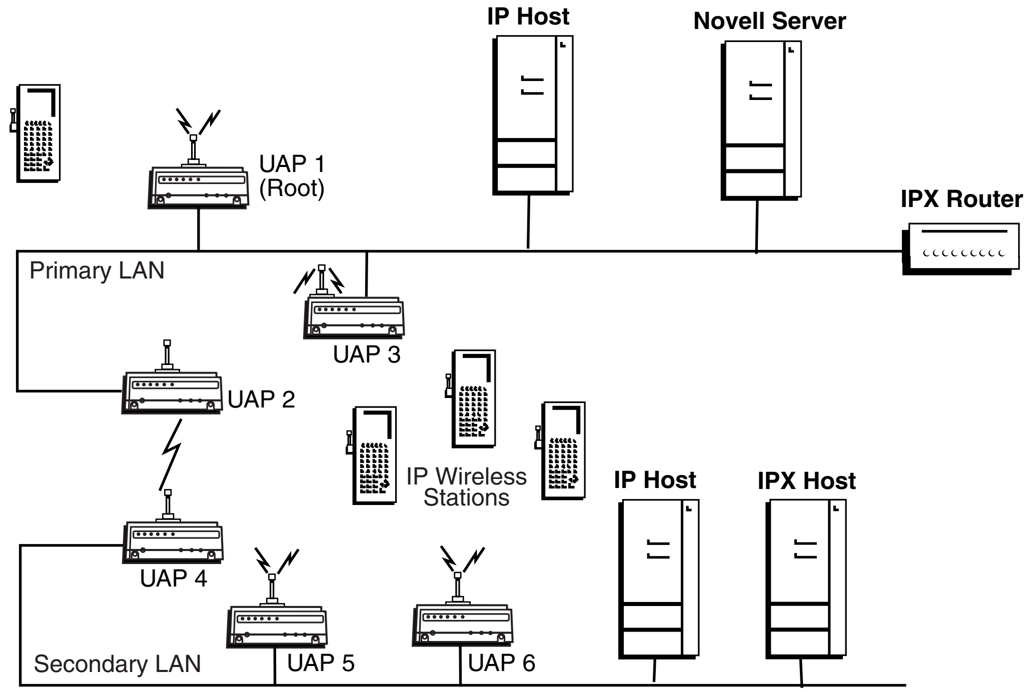
Filtering Examples

The examples in this section illustrate how to set filters to optimize wireless performance. The sample network illustrated next includes

- wireless stations using IP.
- a secondary LAN containing IP and IPX hosts, linked by UAP 2 and UAP 4.
- an IPX router connecting to another Novell network.
- DIX and 802.3 SNAP frames.

Many networks use only one Ethernet frame type. DIX is the most common type. Set filters only for the Ethernet types found on your network.

Network Filter Example

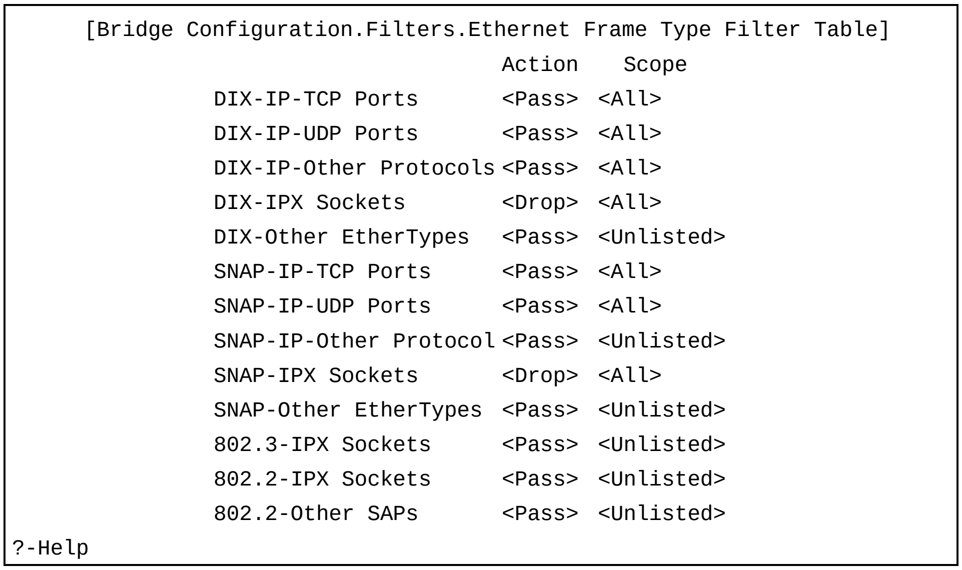


21XXT027.eps

Example 1

UAPs 1, 3, 5, and 6 service only IP end devices. These UAPs need to pass IP traffic, but eliminate IPX traffic that does not need to be forwarded to the primary or secondary LAN. You use the Ethernet Frame Type Filter Table menu to filter the IPX frames. No subtype filters are needed. The Ethernet Frame Type Filter Table menu is shown on the next page.

Ethernet Frame Type Filter Table Menu for Example 1



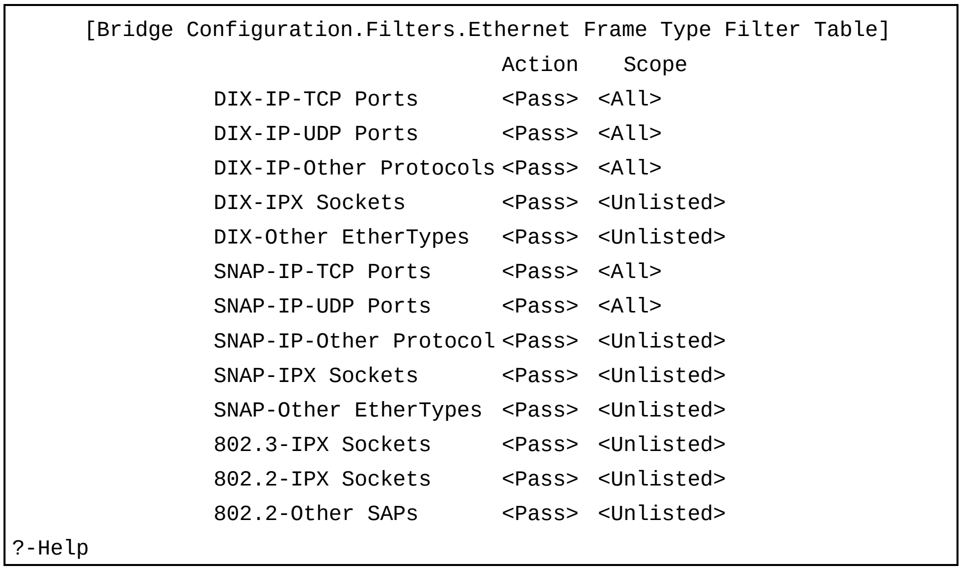
```
      [Bridge Configuration.Filters.Ethernet Frame Type Filter Table]
                                      Action   Scope
                DIX-IP-TCP Ports      <Pass>  <All>
                DIX-IP-UDP Ports      <Pass>  <All>
                DIX-IP-Other Protocols<Pass>  <All>
                DIX-IPX Sockets       <Drop>  <All>
                DIX-Other EtherTypes  <Pass>  <Unlisted>
                SNAP-IP-TCP Ports     <Pass>  <All>
                SNAP-IP-UDP Ports     <Pass>  <All>
                SNAP-IP-Other Protocol<Pass>  <Unlisted>
                SNAP-IPX Sockets      <Drop>  <All>
                SNAP-Other EtherTypes <Pass>  <Unlisted>
                802.3-IPX Sockets     <Pass>  <Unlisted>
                802.2-IPX Sockets     <Pass>  <Unlisted>
                802.2-Other SAPs      <Pass>  <Unlisted>
?-Help
```

Example 2

UAPs 2 and 4 service IP end devices as well as wired IP and IPX hosts on the secondary LAN. In addition, these UAPs pass IPX traffic. The IPX router in this network periodically sends IPX RIP frames for coordinating with other routers. These do not need to be forwarded to the secondary LAN because the secondary LAN does not contain a router.

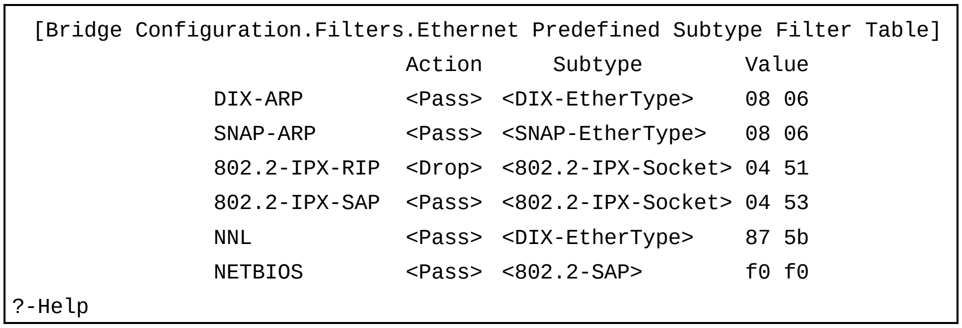
To filter the IPX RIP frames, you need to configure subtype filters. This example sets filters for three different cases: DIX, 802.2, and 802.3 SNAP frames. In many actual networks, only one type of filter is required because all stations are configured using one of the three options.

Ethernet Frame Type Filter Table Menu for Example 2



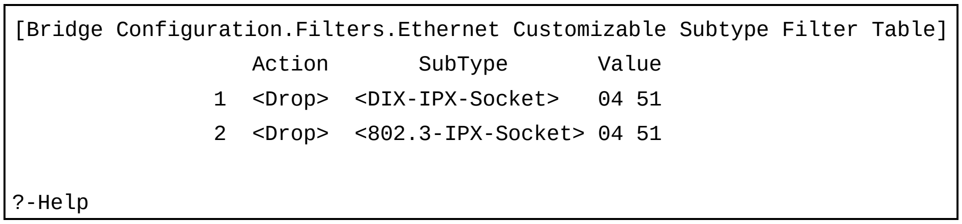
```
      [Bridge Configuration.Filters.Ethernet Frame Type Filter Table]
                                      Action   Scope
                DIX-IP-TCP Ports      <Pass>  <All>
                DIX-IP-UDP Ports      <Pass>  <All>
                DIX-IP-Other Protocols <Pass>  <All>
                DIX-IPX Sockets       <Pass>  <Unlisted>
                DIX-Other EtherTypes  <Pass>  <Unlisted>
                SNAP-IP-TCP Ports     <Pass>  <All>
                SNAP-IP-UDP Ports     <Pass>  <All>
                SNAP-IP-Other Protocol <Pass>  <Unlisted>
                SNAP-IPX Sockets      <Pass>  <Unlisted>
                SNAP-Other EtherTypes <Pass>  <Unlisted>
                802.3-IPX Sockets     <Pass>  <Unlisted>
                802.2-IPX Sockets     <Pass>  <Unlisted>
                802.2-Other SAPs      <Pass>  <Unlisted>
?-Help
```

You need to use subtype filters to drop IPX RIP for 802.2, DIX, and 802.3 frames. Use the settings shown here on the Ethernet Predefined Subtype Filter Table menu to filter IPX RIP for 802.2 frames.



```
  [Bridge Configuration.Filters.Ethernet Predefined Subtype Filter Table]
                               Action      Subtype        Value
                DIX-ARP        <Pass>  <DIX-EtherType>    08 06
                SNAP-ARP       <Pass>  <SNAP-EtherType>   08 06
                802.2-IPX-RIP  <Drop>  <802.2-IPX-Socket> 04 51
                802.2-IPX-SAP  <Pass>  <802.2-IPX-Socket> 04 53
                NNL            <Pass>  <DIX-EtherType>    87 5b
                NETBIOS        <Pass>  <802.2-SAP>        f0 f0
?-Help
```

Use the settings shown here on the Ethernet Customizable Subtype Filter Table menu to filter DIX-IPX and 802.3 IPX.



```
[Bridge Configuration.Filters.Ethernet Customizable Subtype Filter Table]
                   Action       SubType       Value
                1  <Drop>  <DIX-IPX-Socket>   04 51
                2  <Drop>  <802.3-IPX-Socket> 04 51


?-Help
```

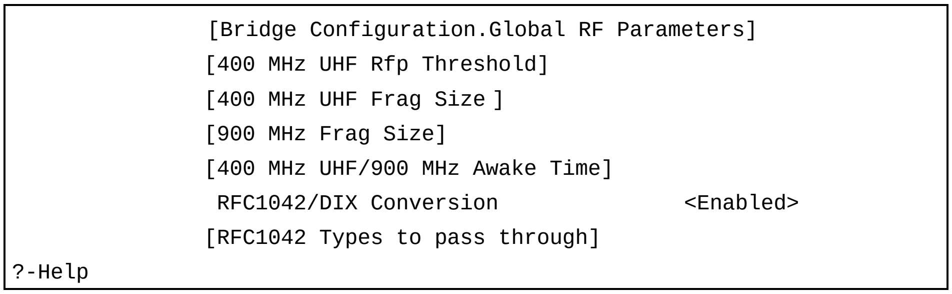
Setting Global RF Parameters

You can use the Global RF Parameters menu to set configuration parameters in the root UAP that are distributed throughout the network. All UAPs that are root candidates should have the same global RF parameters.

Note that several of the global RF parameters have a Set Globally parameter that you can either enable or disable. If you are configuring the root UAP and you set a global RF parameter to enabled, the value for that parameter is set globally for all end devices and UAPs in the network. If you set the value to disabled, the root does not distribute the global parameters and each device uses its local or default setting. The Set Globally parameter has no effect in UAPs that are not the root.

Note: If you do not have any 400 MHz or 900 MHz devices on your network, you can ignore the 400 MHz and 900 MHz parameters on this menu.

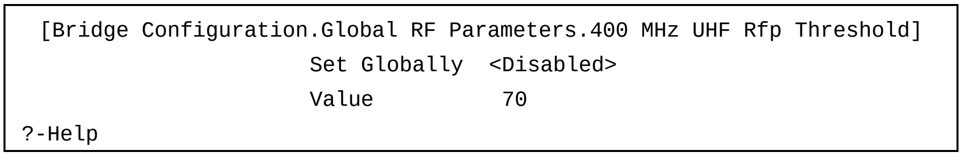
The Global RF Parameters menu is shown here.



```
               [Bridge Configuration.Global RF Parameters]
               [400 MHz UHF Rfp Threshold]
               [400 MHz UHF Frag Size ]
               [900 MHz Frag Size]
               [400 MHz UHF/900 MHz Awake Time]
                RFC1042/DIX Conversion              <Enabled>
               [RFC1042 Types to pass through]
?-Help
```

400 MHz UHF Rfp Threshold UHF Rfp threshold is the largest size of data packets that you can send without reserving air time. Air time is normally reserved to help prevent collisions with other transmitters; however, you can send a small amount of data without a reservation.

When you select this option, the following screen appears:



```
  [Bridge Configuration.Global RF Parameters.400 MHz UHF Rfp Threshold]
                      Set Globally  <Disabled>
                      Value          70
?-Help
```

You can enable or disable the Set Globally parameter. The default is disabled. The recommended setting in most cases is disabled.

You can set the value to a range from 0 to 250 octets. Value is the largest number of octets that a transmitter can send without reserving air time. The default is 70.

If your installation sends primarily very small frames, you may want to set the Set Globally parameter to enabled and use the default value of 70 to improve network response time.

400 MHz UHF Frag Size You can use UHF fragmentation size to determine the largest 400 MHz packet that will be transmitted without fragmentation. Larger packet sizes can improve throughput on a reliable connection. Smaller packet sizes can improve throughput on a poor connection. When you select this option, the following screen appears:

```
    [Bridge Configuration.Global RF Parameters.400 MHz UHF Frag Size]
                       Set Globally  <Disabled>
                       Value          250
?-Help
```

You can enable or disable the Set Globally parameter. The default is disabled. Intermec recommends that you do not change this parameter.

You can set the value to a range from 50 to 250 octets. Value represents the largest number of octets that a transmitter can send without fragmentation by the transmitter and reassembly by the receiver. The default is 250. If the Set Globally parameter is set to disabled, the default value is used.

900 MHz Frag Size You can use 900 MHz fragmentation size to determine the largest 900 MHz packet that you can transmit without fragmentation. Larger packet sizes can improve throughput on a reliable connection. Smaller packet sizes can improve throughput on a poor connection. When you select this option, the following screen appears:

```
      [Bridge Configuration.Global RF Parameters.900 MHz Frag Size]
                       Set Globally  <Disabled>
                       Value          250
?-Help
```

You can enable or disable the Set Globally parameter. The default is disabled. Intermec recommends that you do not change this parameter.

You can set the value to a range from 50 to 250 octets. The value represents the largest number of octets that a transmitter can send without fragmentation by the transmitter and reassembly by the receiver. The default is 250. If you set the 900 MHz Frag Size parameter to disabled, the terminal default is used.

400 MHz UHF/900 MHz Awake Time Awake time is the amount of time that an end device stays awake after a transmission. A sleeping end device is less responsive to radio activity; however, a longer awake time places a greater drain on the battery. You should set awake time so that an end device stays awake long enough to receive an expected reply to a transmission and short enough to reduce power consumption. If an end device is asleep when a reply arrives at its parent UAP, the reply is buffered in the UAP until the next scheduled hello message is transmitted.

When you select 400 MHz UHF/900 MHz Awake Time, the following screen appears:

```
Bridge Configuration.Global RF Parameters.400 MHz UHF/900 MHz Awake Time]
                       Set Globally  <Disabled>
                       Value          0
 ?-Help
```

You can enable or disable the Set Globally parameter. The default is disabled. When awake time is set to disabled, each station uses its own default.

Awake time is specified in tenths of a second. For example, to specify 7 seconds, set awake time to 70. You can set the awake time value to a number from 0 to 250. The default for 900 MHz stations is 1 second. The default for UHF stations is 2 seconds. An awake time of 0 is the same as an awake time to 1—the radio sleeps for .1 seconds.

Awake time does not pertain to OpenAir or IEEE 802.11 DS radios; however, you may need to set awake time for other types of radios on your network.

RFC1042/DIX conversion This parameter determines how the UAP will handle the conversion of RFC1042 frames that are received on its IEEE 802.11 DS radio ports. You can set RFC1042/DIX conversion to either enabled or disabled. The default is enabled.

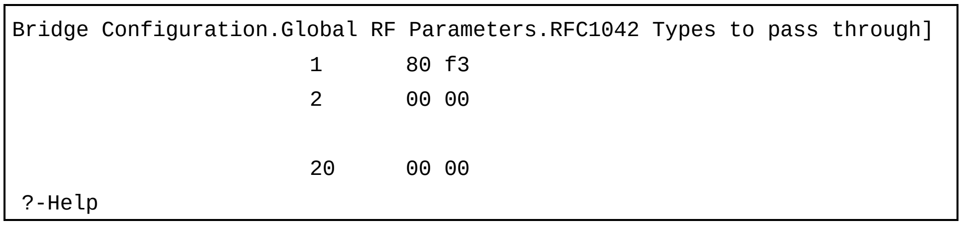
When RFC1042/DIX conversion is set to enabled, frames received from an IEEE 802.11 DS radio with a protocol type equal to a value in the RFC1042 types to pass through list are forwarded without conversion. Frames with protocol types that are not found in the list are converted to DIX format before forwarding.

To convert all 000000 OUI (Organizationally Unique Identifier) SNAP frame types to DIX frames, set RFC1042/DIX conversion to enabled and make sure that all entries in the RFC1042 types to pass through list are 00 00.

When RFC1042/DIX conversion is set to disabled, frames received from an IEEE 802.11 DS radio port will not be translated from RFC1042 format to DIX. That is, when a SNAP frame is received from an IEEE 802.11 DS radio with an OUI equal to 000000, the frame is forwarded without conversion.

Note: RFC1042/DIX conversion only applies to frames received on an IEEE 802.11 DS radio port. All DIX frames received on an Ethernet port are converted to 802.1H (0000F8 OUI SNAP types) before being sent on the IEEE 802.11 DS radio network.

[RFC1042 Types to pass through] This parameter only appears on the menu if RFC1042/DIX conversion is set to enabled. When you select this option, the following screen appears:



```
Bridge Configuration.Global RF Parameters.RFC1042 Types to pass through]
                       1       80 f3
                       2       00 00

                       20      00 00
 ?-Help
```

Enter values for protocol types that are to be passed without conversion. By default the list includes the Apple Talk protocol type, value 80F3.

6

Managing the UAP Remotely

This chapter describes how to access and configure a UAP using Telnet or a Web browser.

Requirements for Establishing a Remote Session

After you have configured the IP address and other basic network parameters, you can access the UAP from a remote location. You can manage the device remotely using either of these methods:

- PC or workstation that is running Telnet software on the Ethernet network
- Web browser that has an Internet or local area network connection

You must know the IP address of the UAP to access it remotely. If a DHCP server assigned the IP address, you must determine the IP address from the DHCP server.

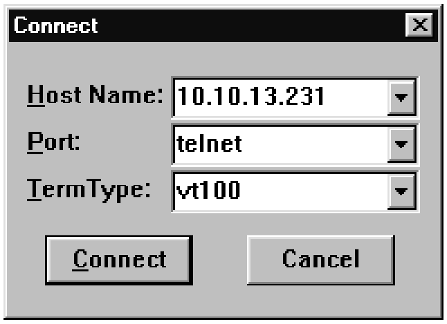
Only one session can be active with the UAP at a time. If your session terminates abruptly or a new signon screen appears, someone else may have accessed the UAP.

Establishing a Telnet Session

You must allow the UAP to go through its boot sequence before you can access the UAP using Telnet. If you reboot the UAP from a Telnet session, the session terminates. You can establish a new Telnet session with the UAP after it reboots. The following example uses Microsoft Telnet.

To establish a Telnet session with the UAP

1. Identify the IP address of the UAP.
2. Verify that your PC or workstation is connected to the Ethernet network and has a Telnet VT emulator installed.
3. Ensure that the UAP is powered up and has completed its boot sequence.
4. On the PC or workstation, open a Telnet session.
5. Choose Connect, then choose Remote System. The Connect dialog box appears.

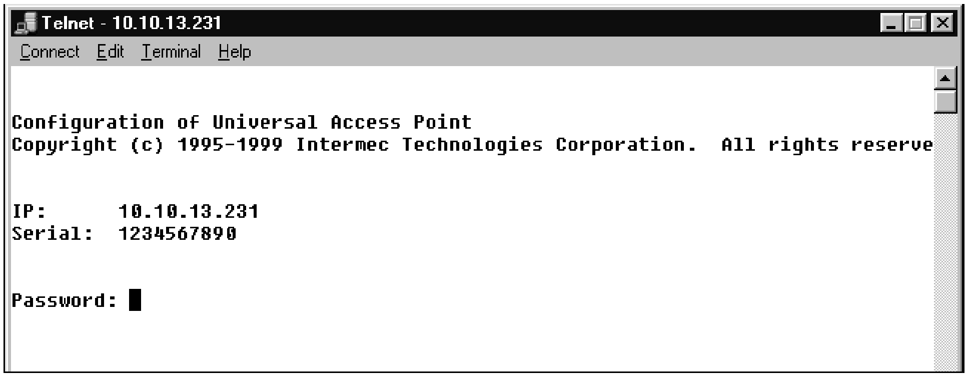


Host Name: 10.10.13.231

Port: telnet

TermType: vt100

6. In the Host Name field, enter the IP Address of the UAP.
7. Click Connect. The UAP logon screen appears.



```
Configuration of Universal Access Point
Copyright (c) 1995-1999 Intermec Technologies Corporation.  All rights reserve


IP:      10.10.13.231
Serial:  1234567890


Password: █
```

8. In the Password field, enter the password. The default is `Intermec`.
9. Press **Enter**. The Configuration menu appears.

```
                        [Quick Start]
                        [Network Configuration]
                        [Bridge Configuration]
                        [Summary]
                        [Maintenance]
                         Save Configuration
                         Reboot
?-Help
```

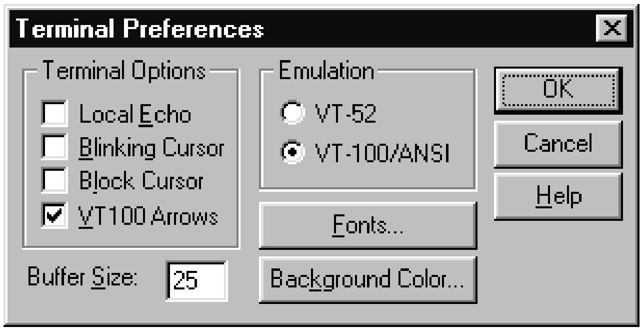
You can now configure the UAP remotely using Telnet. The same configuration menus that are available through a serial connection are available through the Telnet session. For more information about configuring the UAP, see Chapter 2, “Installing and Configuring the UAP.”

Note: If you restore the factory default values during your Telnet session, be sure you reset the DHCP parameters or the IP Address, IP Subnet Mask, and IP Router parameters before you reboot the UAP. If you do not reset these parameters before you reboot, you must connect to the UAP using the serial port to reset them.

To use the arrow keys to navigate through the configuration menus, you may need to enable VT100 Arrows.

To enable VT100 Arrows

1. Choose Terminal from the Telnet tool bar.
2. Choose Preferences. The Terminal Preferences dialog box appears.



Terminal Preferences

Terminal Options

☐ Local Echo
☐ Blinking Cursor
☐ Block Cursor
☑ VT100 Arrows

Emulation

○ VT-52
● VT-100/ANSI

Buffer Size: 25

3. Select VT100 Arrows.
4. Click OK.

Using a Web Browser

You can configure the UAP using a Web browser; however, note these important points:

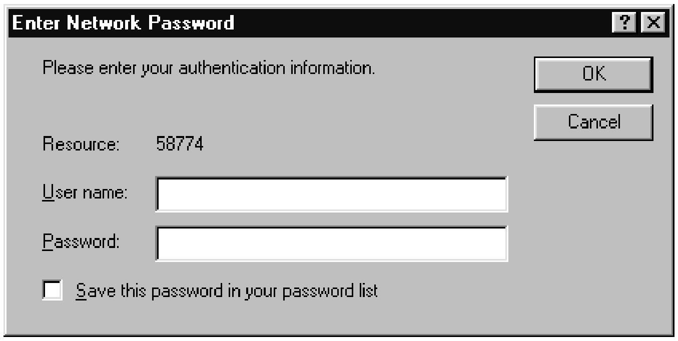
- Your session terminates if there is no activity for 15 minutes.
- Console Command mode is not available.

The Web browser interface for the UAP has been tested using Netscape v3.0 and above, and Internet Explorer v3.0 and above. Remotely accessing the UAP using other browsers may provide unpredictable results.

Establishing a Web Browser Session

1. Identify the IP address of the UAP.
2. Start the Web browser application.
3. Access the UAP using one of these methods:
   - In the Address field, enter the IP address of the UAP. Press **Enter**.
   - Choose File and then choose Open. In the Open field, enter the IP address of the UAP. Press **Enter**.

   The Enter Network Password dialog box appears.



Enter Network Password

Please enter your authentication information.

Resource: 58774

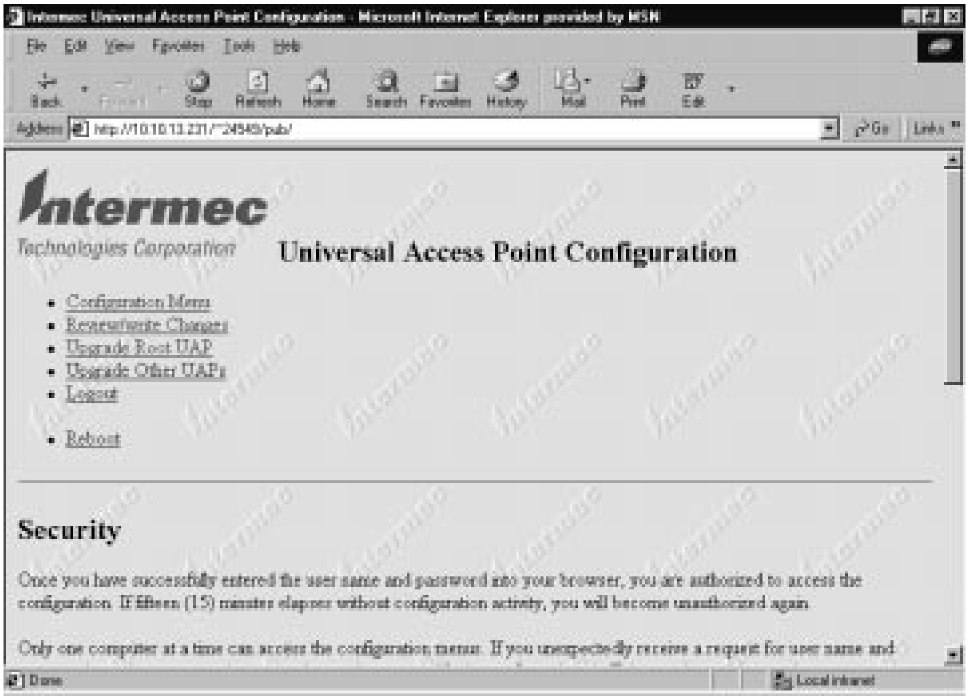
User name:

Password:

□ Save this password in your password list

4. In the User name field, enter the random number that appears on the screen. This number is 1 to 5 digits long and changes every time you establish a new session.
   - If you are using Microsoft Internet Explorer 4.X, this is the number that appears in the Resource field.
   - If you are using Microsoft Internet Explorer 5.X, this is the number that appears in the Realm field.
   - If you are using Netscape, this is the number that appears at the top of the screen.
5. In the Password field, enter the password. The default password is `Intermec`.

6. Press **Enter**. The Universal Access Point Configuration Web page appears.


Intermec Universal Access Point Configuration - Microsoft Internet Explorer provided by MSN
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit
Address http://10.10.13.231/~24545/pub/
Go Links
Intermec
Technologies Corporation
Done
Local intranet

Universal Access Point Configuration

- Configuration Menu
- Review/write Changes
- Upgrade Root UAP
- Upgrade Other UAPs
- Logout

- Reboot

Security

Once you have successfully entered the user name and password into your browser, you are authorized to access the configuration. If fifteen (15) minutes elapses without configuration activity, you will become unauthorized again.

Only one computer at a time can access the configuration menus. If you unexpectedly receive a request for user name and

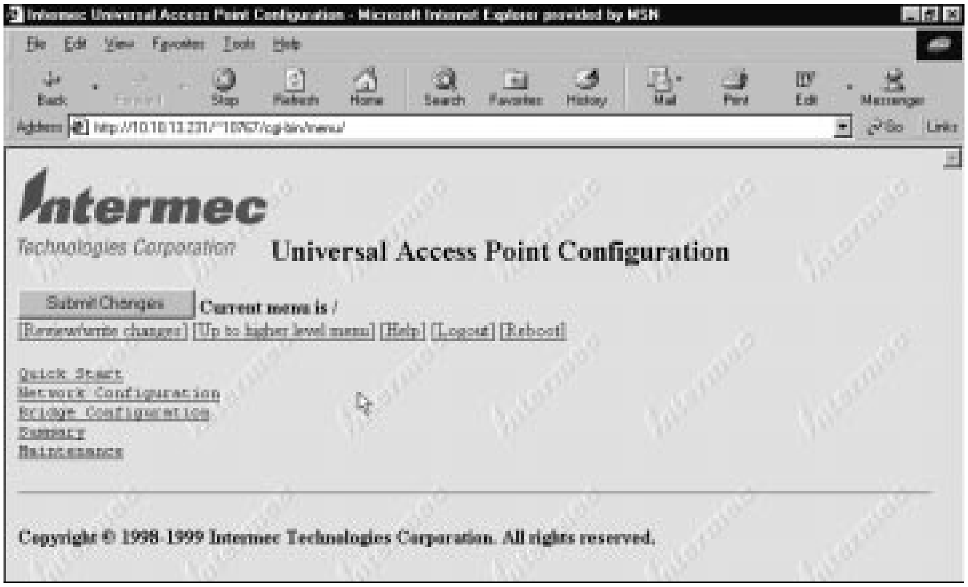
7. Choose one of the following commands:

- Choose Configuration Menu to configure the UAP. For more information, see the next section, “Configuring the UAP.”
- Choose Review/write Changes to view a list of parameters that were changed from the default values. You can also restore default values. For more information, see “Restoring the Factory Default Settings” later in this chapter.
- Choose Upgrade Root UAP to perform a TFTP firmware upgrade to the root UAP. For more information, see Appendix D, “Upgrading the UAP.”
- Choose Upgrade Other UAPs to distribute the firmware installed on the root UAP to the other UAPs in the network. For more information, see “Upgrading Other UAPs” in Appendix D.
- Choose Logout to end the Web browser session.
- Choose Reboot to boot the UAP.

Configuring the UAP

You can configure the UAP remotely using your Web browser. The configuration commands you execute through the Web browser are similar to the commands that you execute when you access the Configuration menu through a serial or Telnet connection.

When you select the Configuration Menu command, the following screen appears.



http://10.10.13.231/^10767/cgi-bin/menu/

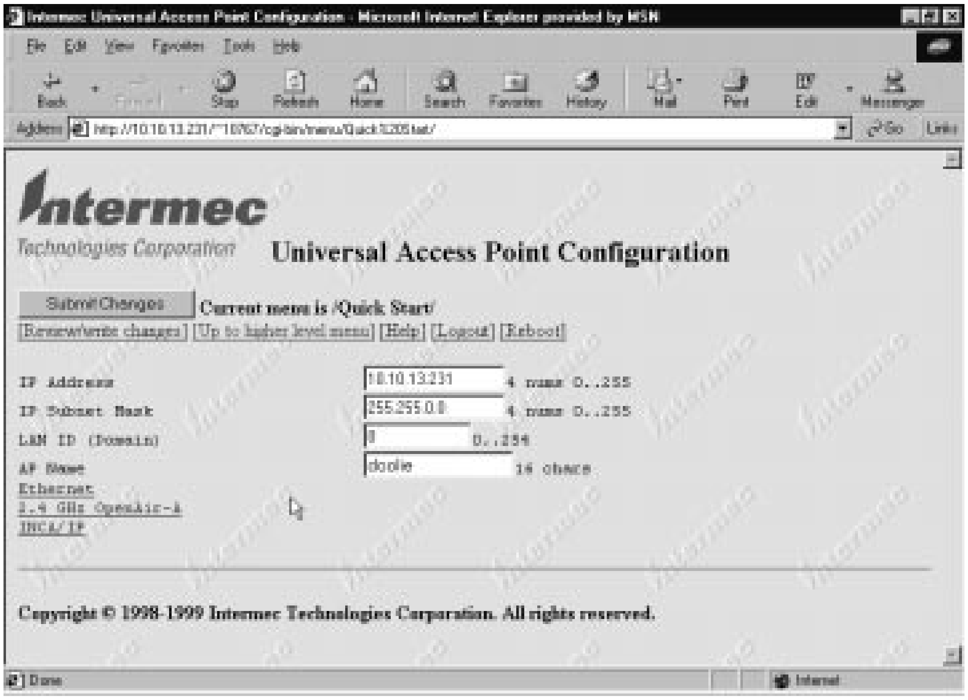
Universal Access Point Configuration

Current menu is /

Copyright © 1998-1999 Intermec Technologies Corporation. All rights reserved.

To configure the UAP

1. Choose a command from the Universal Access Point Configuration menu. For example, if you choose Quick Start, the following screen appears.



Intermec Universal Access Point Configuration - Microsoft Internet Explorer provided by MSN
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Messenger
Address
Go Links
Intermec Technologies Corporation
Submit Changes
[Review/write changes] [Up to higher level menu] [Help] [Logout] [Reboot]
Done
Internet

http://10.10.13.231/"10767/cgi-bin/menu/Quick1205tat/

Universal Access Point Configuration

Current menu is /Quick Start/

IP Address	10.10.13.231	4 nums 0..255
IP Subnet Mask	255.255.0.0	4 nums 0..255
LAN ID (Domain)	0	0..254
AP Name	doolie	16 chars

Ethernet
2.4 GHz OpenAir-A
INCA/IP

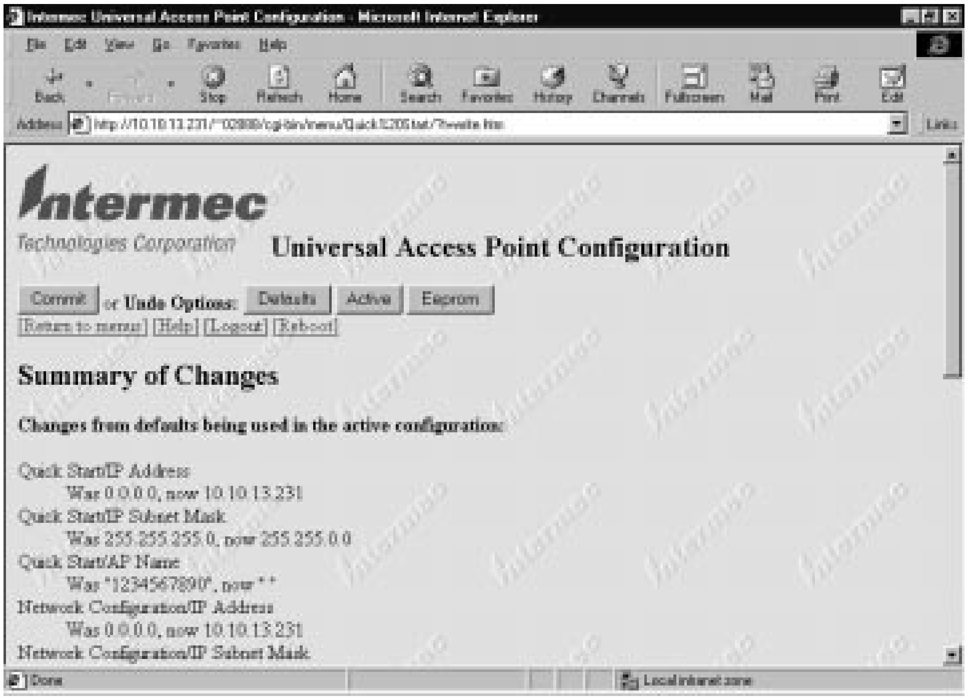
Copyright © 1998-1999 Intermec Technologies Corporation. All rights reserved.

2. Configure the parameters for your installation.
3. Click Submit Changes. When the Operation Complete screen appears, click Back.

Note: You must click the Submit Changes button and then the Back button on every Web page where you make a change or your changes are not saved.

4. To configure more parameters, repeat Steps 1 through 3.

5. Click Review/write changes. The Summary of Changes screen appears.



Universal Access Point Configuration

Commit or **Undo Options:** Defaults Active Eeprom

Summary of Changes

Changes from defaults being used in the active configuration:

Quick Start/IP Address
Was 0.0.0.0, now 10.10.13.231
Quick Start/IP Subnet Mask
Was 255.255.255.0, now 255.255.0.0
Quick Start/AP Name
Was "1234567890", now " "
Network Configuration/IP Address
Was 0.0.0.0, now 10.10.13.231
Network Configuration/IP Subnet Mask

6. Confirm that your changes appear.
7. Click Commit to save your configuration. When the Operation Complete screen appears, click Back.
8. You can either reboot or logout.
   - Click Reboot to boot the UAP and make your changes effective immediately.
   - Click Logout to terminate the browser session. Your changes become effective the next time the UAP boots.

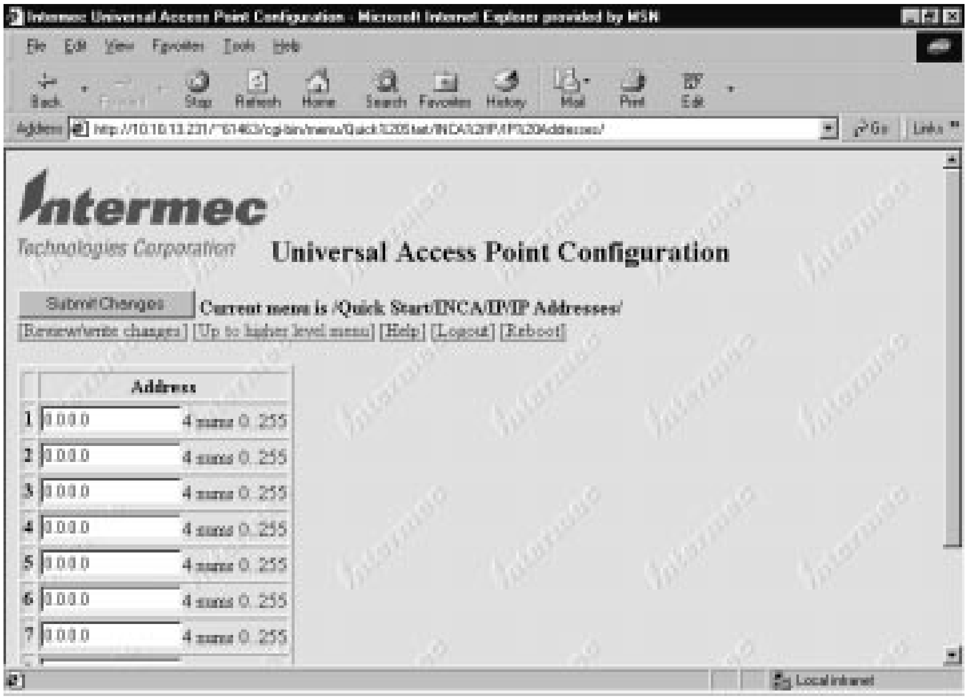
Creating INCA/IP Tunnels

To create INCA/IP tunnels, you configure the root UAP to originate the tunnels, and then you specify the IP addresses of the UAPs that are to listen at the other end of each tunnel. For more information about INCA/IP and configuring INCA/IP tunnels, see Appendix B, “Understanding INCA/IP.”

When you configure INCA/IP tunnels through the Web browser, you must configure the root to originate tunnels, and then you must submit the change and commit the change before the IP Addresses command appears on the screen.

To create INCA/IP tunnels

1. From the Configuration menu, choose the Quick Start command and then choose the INCA/IP command.
2. Configure the Mode parameter to Originate If Root.
3. Click Submit Changes. When the Operation Complete screen appears, click Back.
4. Choose the Review/write Changes command. The Summary of Changes screen appears.
5. Confirm that the change appears.
6. Click Commit. When the Operation Complete screen appears, click Back.
7. Click Return to menus. The IP Addresses command now appears on the screen.
8. Choose the IP Addresses command. The IP Addresses screen appears.



Universal Access Point Configuration

Submit Changes Current menu is /Quick Start/INCA/IP/IP Addresses/

[Review/write changes] [Up to higher level menu] [Help] [Logout] [Reboot]

	Address	
1	0.0.0.0	4 nums 0..255
2	0.0.0.0	4 nums 0..255
3	0.0.0.0	4 nums 0..255
4	0.0.0.0	4 nums 0..255
5	0.0.0.0	4 nums 0..255
6	0.0.0.0	4 nums 0..255
7	0.0.0.0	4 nums 0..255

9. Enter the IP addresses of the UAPs that are to listen for INCA/IP tunnels.
10. Press **Enter**. When the Operation Complete screen appears, click Back.
11. Click Submit Changes. When the Operation Complete screen appears, click Back.
12. Choose the Review/write Changes command. The Summary of Changes screen appears.
13. Confirm that the change appears.
14. Click Commit. When the Operation Complete screen appears, click Back.

The changes become effective the next time you boot the UAP.

Restoring the Factory Default Settings

If you restore the factory default values during your Web browser session, be sure you reset the DHCP parameters or the IP Address, IP Subnet Mask, and IP Router parameters before you reboot the UAP. If you do not reset these parameters before you reboot, you must connect to the UAP using the serial port to reset them.

To restore factory defaults

1. If you are using a DHCP or BOOTP server to assign values to the IP Address, IP Subnet Mask, and IP Router parameters, note the values in the DHCP and DHCP Server Name fields.

   If the UAP was assigned specific IP values and no DHCP or BOOTP server was used, note the values in the IP Address, IP Subnet Mask, and IP Router fields.
2. Choose the Review/write Changes command. The Summary of Changes screen appears.
3. Click Defaults to load the factory defaults. When the Operation Complete screen appears, click Back.
4. Choose the Return to menus command.
5. Choose the Network Configuration command.
6. Reset either the DHCP parameters or the IP parameters using the values you noted in Step 1.
7. Click Submit Changes. When the Operation Complete screen appears, click Back.
8. Choose the Review/write Changes command. The Summary of Changes screen appears.
9. Confirm that your changes appear.
10. Click Commit. When the Operation Complete screen appears, click Back.
11. Choose the Reboot command. Your UAP reboots with the factory default settings and your network parameters.

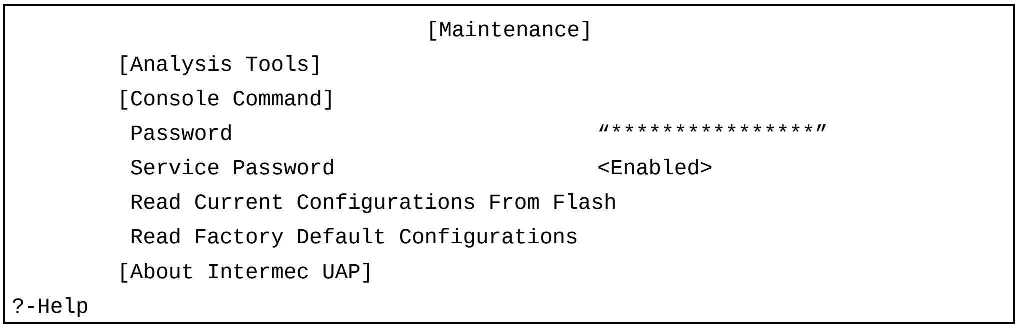
7

Maintenance and Troubleshooting

This chapter describes the commands on the Maintenance menu and the status of the LEDs during the boot process. It also includes information on troubleshooting the radios. Some commonly asked technical support questions and answers are provided, as well as information about how to obtain help.

Understanding the Maintenance Menu

From the Maintenance menu you can perform a variety of functions such as changing your password, viewing the devices that are connected to your UAP, and resetting your UAP to factory default values.



```
                                [Maintenance]
         [Analysis Tools]
         [Console Command]
          Password                            "****************"
          Service Password                    <Enabled>
          Read Current Configurations From Flash
          Read Factory Default Configurations
         [About Intermec UAP]
?-Help
```

[Analysis Tools] Select this option to access the Analysis Tools menu. From this menu you can select the UAP Connections screen or the Port Statistics screen. For more information, see “Using Analysis Tools” later in this section.

[Console Command] When you select this option from the Maintenance menu, you go to Console Command mode where you can manipulate the UAP files and upgrade the UAP firmware. To return to the UAP monitor from Console Command mode, type `exit` and press **Enter**. For more information about using Console Command mode, see Chapter 8, “Advanced Features.”

Password You can change the password that allows access to these UAP configuration menus. The password can be up to 16 characters in length and is not case sensitive. The default is `Intermec`.

Service Password Intermec maintains a service password so that an Intermec Service representative can configure this UAP if necessary. For example, if you forget the configuration password, the Intermec representative can access the menus using the service password. By default, the service password is enabled. If setting a service password violates your security guidelines, you can disable the service password.

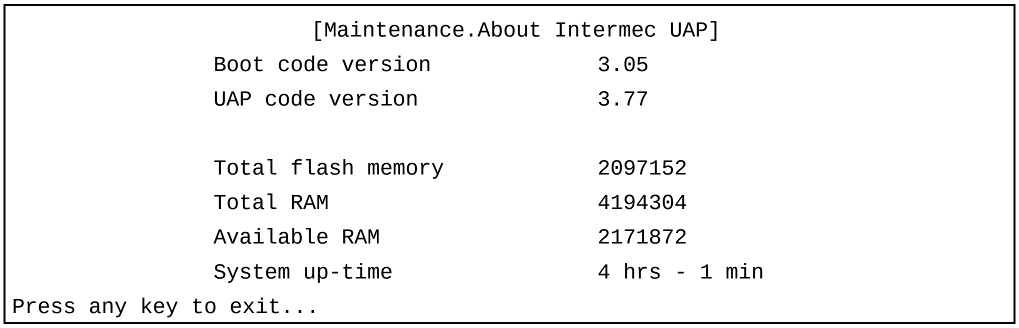
Note: If you set Service Password to disabled, and then you forget your configuration password, you may need to send this UAP to a Service Center to be reconfigured.

Read Current Configurations From Flash When you select this option, the UAP loads the configuration that is presently stored in flash memory and then the Maintenance menu reappears.

Read Factory Default Configurations When you select this option, the UAP reloads the factory default configurations and then the Maintenance menu reappears. To make the default settings active, you must reboot the UAP.

Note: After you restore the factory defaults, you should reset the DHCP parameters or the IP Address, IP Subnet Mask, and IP Router parameters before you reboot so that you can continue to manage the UAP over the network. If you do not reset these values before you reboot, you will have to reset these parameters using the serial port.

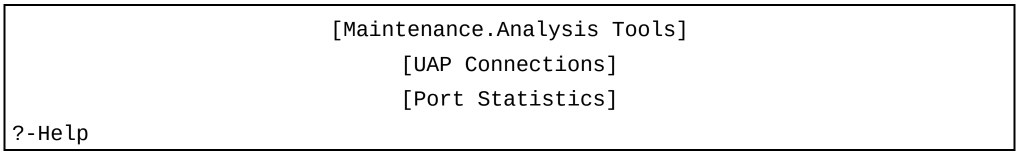
[About Intermec UAP] When you select this option, the read-only About Intermec UAP screen appears. You can obtain basic information about the firmware and memory of the UAP by viewing this screen. You need to know the firmware version of your boot code and UAP code when you call Intermec Technical Support. The boot code version displayed on the screen is the UAP Monitor code that boots your UAP. The UAP code version is the UAP Program code.



```
                          [Maintenance.About Intermec UAP]
                Boot code version            3.05
                UAP code version             3.77

                Total flash memory           2097152
                Total RAM                    4194304
                Available RAM                2171872
                System up-time               4 hrs - 1 min
Press any key to exit...
```

Using Analysis Tools

When you select the Analysis Tools command from the Maintenance menu, the following menu appears:

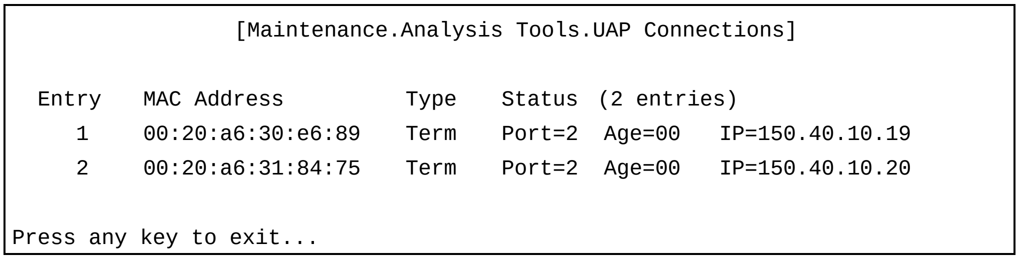


```
                         [Maintenance.Analysis Tools]
                              [UAP Connections]
                              [Port Statistics]
?-Help
```

Viewing UAP Connections

The UAP Connections screen is a read-only screen that displays information about the devices that are communicating with the UAP. The MAC address and other information is displayed for those devices that are one hop outbound from your UAP. You should note that it may take one to two minutes for an end device to appear on the UAP Connections screen.

Note: To view IP addresses on the UAP Connections screen, you must set the ARP Server Mode parameter to normal flooding or no flooding.



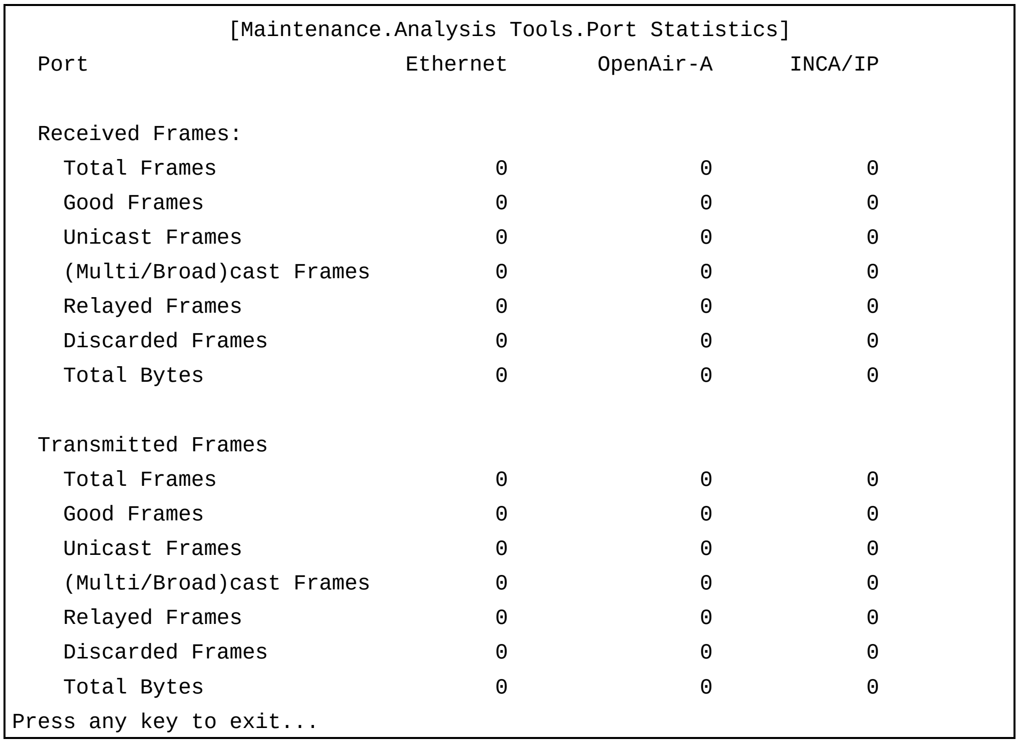
```
                  [Maintenance.Analysis Tools.UAP Connections]

  Entry   MAC Address         Type   Status  (2 entries)
     1    00:20:a6:30:e6:89   Term   Port=2  Age=00   IP=150.40.10.19
     2    00:20:a6:31:84:75   Term   Port=2  Age=00   IP=150.40.10.20

Press any key to exit...
```

These categories of devices display in the type column on the UAP Connections screen:

Type	Explanation
Term	Terminal or end device
WAP	A wireless access point
AP	An access point configured to listen for an INCA/IP tunnel
AP-Tnl	An access point configured to originate an INCA/IP tunnel (root AP)
Ehost	Ethernet host on a secondary LAN

Viewing Port Statistics

The Port Statistics screen is a read-only screen that displays total transmitted and received frames and bytes for each port since the UAP was last powered up.



```
               [Maintenance.Analysis Tools.Port Statistics]
  Port                         Ethernet       OpenAir-A      INCA/IP


  Received Frames:
    Total Frames                      0               0            0
    Good Frames                       0               0            0
    Unicast Frames                    0               0            0
    (Multi/Broad)cast Frames          0               0            0
    Relayed Frames                    0               0            0
    Discarded Frames                  0               0            0
    Total Bytes                       0               0            0

  Transmitted Frames
    Total Frames                      0               0            0
    Good Frames                       0               0            0
    Unicast Frames                    0               0            0
    (Multi/Broad)cast Frames          0               0            0
    Relayed Frames                    0               0            0
    Discarded Frames                  0               0            0
    Total Bytes                       0               0            0
Press any key to exit...
```

Understanding the LED Lighting Sequence

When the UAP is powered on, the LEDs flash as the UAP boots and performs internal diagnostics. The table below describes the LED activity during the boot process.

	Wireless	Wireless	Wired	Root/	
Power	**#1**	**#2**	**LAN**	**Error**	**Description**
On	Off	Off	Off	On	Flash checksum being calculated.
On	On	Off	Off	On	Flash checksum failure.
On	Off	Off	On	Off	RAM test in progress.
On	On	Off	On	Off	RAM test failure.
On	Off	On	Off	Off	Loading of monitor in progress.
On	Off	On	Off	On	Ethernet test in progress.
On	On	On	Off	On	Ethernet test failure.

After the UAP successfully boots, the LEDs display the following pattern:

Power	Wireless #1	Wireless #2	Wired LAN	Root/Error
On	Flashes	Flashes (if radio installed)	Flashes	Flashes if this UAP is configured as the root.

Troubleshooting the Radios

If the radio is faulty or the configuration matrix string is incorrect, the LEDs on the UAP display the following pattern after the UAP boots:

Power	Wireless #1	Wireless #2	Wired LAN	Root/Error
On	Off	Off	On	On

If you are connected to the UAP through its serial port, an error message also appears on your terminal or PC. The error messages are described here. In the following table, radio A refers to the radio in slot 1, and radio B refers to the radio in slot 2. These error messages may appear for either radio A or radio B.

Error Message	Explanation
Couldn’t read country code from radio A	The radio may be faulty. Contact your Intermec representative.
Radio A has unknown country code	The radio may have been configured incorrectly at the factory. Contact your Intermec representative.
Invalid country code in string for radio A	The country code in the configuration matrix string does not match the country code in the radio in the UAP. Contact your Intermec representative.
Radio string doesn’t match radios installed	When this error message appears, additional information appears on the screen. For example, “Expected 504,000 but found 491 in slot A, nothing in slot B” may appear. You may have a faulty radio—contact your Intermec representative.

Commonly Asked Technical Support Questions

Problem/Symptom/Question	Possible Solution/Answer
Is the UAP fully booted?	The Power LED remains steady green and the Wired LAN LED flashes when the UAP is fully booted.
The Power LED is not on.	You may have a hardware problem with your UAP. 1. Unplug the UAP and then plug it back in to cycle the power. Verify that the Power LED remains on. 2. Call Intermec Technical Support.
I cannot configure the UAP locally using the serial port.	1. Verify that you are using a null-modem cable to connect the UAP to your terminal or PC. 2. Verify that the terminal or PC is set to 9600, N, 8, 1, no flow control. 3. Your system may be in autobaud mode. Reboot and press a key once per second until the signon screen appears.
I cannot ping or Telnet to my new UAP.	The UAP does not come with a default IP address. Before you can remotely connect to it, you must set an IP address and subnet mask using the serial port.
The end device cannot connect to the network.	• Choose Analysis Tools from the Maintenance menu, and then choose UAP Connections. Verify that the MAC address of your end device displays on the screen. If the MAC address of your device does not appear, your device is not communicating with the UAP. Check your radio configuration settings. • Verify the UAP is not filtering out the type of traffic you are trying to pass through it.
The end device cannot synch to the UAP.	If you are using 900 MHz Falcon radios: • Verify that the end device and UAP have the same LAN ID and mode-channel. If you are using 2.4 GHz OpenAir radios: 1. Verify that the end device and UAP have the same LAN ID, security ID, channel, and subchannel. 2. Verify that the UAP is configured as a master and the end device is configured as a station. If you are using IEEE 802.11 radios: • Verify that the end device and UAP have the same frequency and network name. If you are using UHF radios: • Verify that the end device and UAP have the same frequency.

Commonly Asked Technical Support Questions (continued)

Problem/Symptom/Question	Possible Solution/Answer
My end devices are unable to roam between 21XX and 011X devices.	1. Choose the Global Flooding command from the Bridge Configuration menu. 2. Set the Unicast Flood Mode parameter to hierarchical.
My end devices are unable to roam to another 21XX.	Roaming through switches requires backward learning, which is part of the IEEE 802.1d standard. If your network has switches that do not support backward learning, you can create a data link tunnel to force all radio traffic through a fixed point so roaming is transparent to the bridges or switches. To create a data link tunnel: 1. Set the Ethernet Bridging parameter to enabled on the root UAP. 2. Set the Ethernet Bridging parameter to disabled on all UAPs that are separated from the root UAP by a bridge or switch that does not support backward learning.
My filters aren’t filtering properly.	Check all of your filter settings. You may have conflicts between the various filters.
The throughput seems slow.	1. Verify that your antennas are well-placed, that they are not behind metal, and that there are few obstacles in their path. 2. If you move the antenna closer to the end device and throughput increases, you may want to add a second UAP and implement roaming. 3. You may be able to set filters to eliminate Ethernet traffic on the wireless side of the network.

Obtaining Help With Your Installation

The 21XX Universal Access Point is designed to be easy to install and configure. If you are having trouble with your installation, you may need to call Intermec Technical Support. Before calling Intermec, be sure you can answer the following questions:

- What kind of network are you using?
- What were you doing when the error occurred?
- What error message did you see?
- Can you reproduce the problem?
- What versions of UAP firmware are you using?

Choose the About Intermec UAP command from the Maintenance menu to confirm the firmware versions on your UAP. The About Intermec UAP screen displays the version of your boot code and UAP program code.

In the United States, call Intermec Technical Support at 1-800-755-5505. In Canada, call 1-800-688-7043.

8

Advanced Features

This chapter describes the UAP monitor, Console Command mode, and how to use script files to update the system files.

Using the UAP Monitor

The UAP monitor is the system software that controls the UAP. You can use UAP monitor commands to manipulate the UAP file segments.

Understanding UAP Segments

The UAP has five segments in its file system. The segments are described here.

- The current active boot or startup segment (can be segment 1 or 2).
- The current inactive boot or startup segment (can be segment 1 or 2).
- The current active data segment (can be segment 3 or 4).
- The current inactive data segment (can be segment 3 or 4).
- The RAM memory segment.

You can enter commands to manipulate the boot and data segments. For instance, you typically download a new firmware version into an inactive segment and then make that segment active the next time the UAP boots. For more information on upgrading the UAP firmware, see Appendix D, “Upgrading the UAP.”

Entering the UAP Monitor

You can access the UAP monitor only through the serial port and only during the boot process.

To enter the UAP Monitor

- Press any key on the keyboard when you see this message displayed during the boot process:

  ```
  <Press any key within 5 seconds to enter the UAP monitor>
  ```

Note: Certain functions available through the UAP monitor can erase your configuration information. Intermec strongly recommends that you only use the UAP monitor when absolutely necessary. For example, you might use the UAP monitor to upgrade your firmware or when instructed to do so by qualified Intermec personnel.

Using UAP Monitor Commands

When you are in the UAP monitor, the UAP prompt (uap>) appears. You can display a list of UAP monitor commands anytime you see the UAP prompt.

To display UAP monitor commands

- Press a letter or number key on the keyboard, and then press **Enter**. A list of UAP monitor commands appears.

Note: If you type the letter B (upper or lower case) and press **Enter**, the UAP will reboot. Type any letter or number OTHER than B to display UAP commands.

The following example shows UAP monitor mode and the list of available commands. The commands are not case sensitive; you can type the commands using either upper or lower case.

```
UAPBOOT V3.05 March 5, 1999
<Press any key within 5 seconds to enter the UAP monitor>
uap>d
------------------------------------------------------------------------
”uap>“ commands...
------------------------------------------------------------------------
        -Reboot                  |              -Device IDs menu
FX s    -Ymodem File Download    | MR           -Display Mfg Record
FD      -File System Directory   | TEST         -Test Menu
FR      -Run Flash Boot File     | SRVC         -Service Menu
        -Manufacturing Menu      | SR z         -Serial Baud Rate
------------------------------------------------------------------------
uap>
```

B

You reboot the UAP by typing B and pressing **Enter**. Reboot resets the system software. Reboot is similar to unplugging the UAP and then plugging it back in. The format to reboot the system is:

```
B
```

FX

The FX command performs a Ymodem batch protocol download of a file into the flash segment that is specified by *s*. The format is:

FX *s*

where *s* is segment 1, 2, 3, or 4.

FD

The FD command displays the flash file system directory, including information about the boot file. The format is:

```
FD
```

FR

The FR command finds the first executable file in the UAP boot segment and tries to run it; therefore, the first executable file in the UAP boot segment must be the boot file. The format is:

```
FR
```

MR

The MR command displays the manufacturing record for the UAP. You use the MR command to display the MAC address, configuration string, and serial number for your UAP. The format is:

```
MR
```

SR

The SR command sets the baud rate of the UAP. The format is:

```
SR z
```

where `z` is the baud rate. Acceptable values for baud rate are:

0 (autobaud)

2400

4800

9600 (default)

19200

38400

57600

115200

The UAP ships with the default baud rate of 9600. You can change the baud rate by using the SR command and entering the desired baud rate. You must enter the baud rate as a whole number with no commas. For example, to enter a baud rate of 19,200, you must enter `19200`.

You can use autobaud to let the UAP set its baud rate to match the baud rate of your terminal, up to a baud rate of 115200. For autobaud, use the SR command and set the baud rate to 0. You will then be instructed to press **Enter** twice so that the UAP can detect the baud rate of your terminal. The autobaud feature automatically detects the baud rate of your terminal and sets the baud rate of the UAP to match.

Using Service Mode Commands

Within the UAP monitor, service mode allows you to perform certain file functions. The commands can cause undesirable results if not properly executed. If you are unsure about the proper procedure to use, contact Intermec Technical Support for assistance.

SRVC

Use the SRVC command to enter service mode where you perform file functions such as deleting a file and performing a Ymodem download through the serial port.

To enter service mode

1. Type SRVC and press **Enter**.
2. Enter a password. The default password is EV98203S (case sensitive).

When you are in service mode, the service prompt (service>) appears. Service mode has a set of defined commands that you can use.

To display service mode commands

- Type any letter or number (other than B) and press **Enter**. The service commands appear on the screen.

```
UAPBOOT V3.05 March 5, 1999
<Press any key within 5 seconds to enter the UAP monitor>
uap>srvc
Enter password : ********
service>d
---------------------------------------------------------------------
”service>“ commands...
---------------------------------------------------------------------
FD        - File System Directory| FB bs (ds) - Set Boot/Data Segment
FDEL f (s)- File Delete          | PN         - Normal power up
FE <s|all>- Erase Segment(s)     | PQ         - Quiet power up
FI        - File System Reset    | B          - Reboot
FFR f (s) - Run File             | X          - Exit
FX s      - Ymodem File Download |
---------------------------------------------------------------------
service>
```

Most of the commands that you use in service mode are also used in the UAP monitor or console command mode and are described in those sections in this chapter. Some additional service commands you may need are listed next.

FFR

The FFR command runs a program that is specified by `f,` from a location specified by `s.` The format is:

```
FFR f (s)
```

where:

`f` is the program name.

`s` is the optional segment location of the program.

For example, to run program UAPBOOT.PRG from segment 1, you could enter:

```
FFR UAPBOOT.PRG 1
```

PN

The PN command returns the UAP to normal mode from quiet mode. The format is:

```
PN
```

To return the UAP to normal mode

1. Reboot the UAP.
2. The LEDs flash on and off during the reboot. When the LEDs flash off and only the Power LED remains lit, type `!!!` (three exclamation points). The UAP prompt (uap>) appears.
3. Type `SRVC` and press **Enter**.
4. Type the service password (the default is `EV98203S`) and press **Enter**. The service prompt (service>) appears.
5. Type `PN` and press **Enter**.
6. Type `B` to reboot the UAP in normal mode.

PQ

The PQ command puts the UAP in quiet mode. When the UAP is in quiet mode, you cannot access the UAP monitor. You may want to use quiet mode for security reasons. The format is:

```
PQ
```

Using Test Mode Commands

Within the UAP monitor, test mode allows you to perform certain test functions. The commands can cause undesirable results if not properly executed. If you are unsure about the proper procedure to use, contact Intermec Technical Support for assistance.

TEST

The TEST command allows you to enter test mode where you can perform a variety of test functions.

To enter test mode

1. Type `TEST` and press **Enter**.
2. Enter a password. The default password is `EV98203T` (case sensitive).

When you are in test mode, the test prompt (test>) appears. Test mode has a set of defined commands that you can use.

To display test mode commands

- Type any letter or number other than B and press **Enter**. The test commands appear on the screen.

```
UAPBOOT V3.05 March 5, 1999
<Press any key within 5 seconds to enter the UAP monitor>
uap>test
Enter password : ********
test>d
---------------------------------------------------------------------
”test>“ commands...
---------------------------------------------------------------------
LT          - LED Test          | MWW s d .. d  - Memory word Write
MACE        - MACE Test Menu    | MRB s l       - Memory byte Read
MF s l      - Memory Fill       | MWB s d .. d  - Memory byte Write
MV s l      - Memory Verify     | SD            - Get DRAM Size (K)
MR s 1      - Memory dword Read | SF            - Get Flash Size (K)
MW s d .. d - Memory dword Write| X             - Exit
MRW s l     - Memory word Read
---------------------------------------------------------------------
test>
```

Using Console Command Mode

Another way you can access the UAP file system is through Console Command mode. You enter Console Command mode from the UAP Maintenance menu. You use Console Command mode to upgrade UAPs using TFTP and Script files.

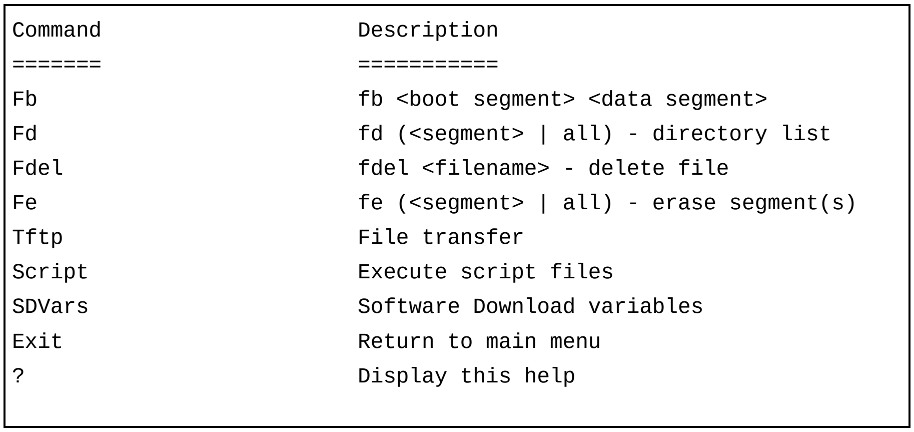
To enter Console Command mode

- Choose Command Console from the Maintenance menu.

When you first enter Console Command mode, a list of valid console commands appears. You can display the console commands any time you are in Console Command mode.

To display console commands

- Type F and press **Enter**. The following screen appears.



```
Command                     Description
=======                     ===========
Fb                          fb <boot segment> <data segment>
Fd                          fd (<segment> | all) - directory list
Fdel                        fdel <filename> - delete file
Fe                          fe (<segment> | all) - erase segment(s)
Tftp                        File transfer
Script                      Execute script files
SDVars                      Software Download variables
Exit                        Return to main menu
?                           Display this help
```

To exit Console Command mode

- Type `exit` and press **Enter**.

Several file menu commands require that you enter file names. To indicate the segment where the file is located, you can precede the file name with either a segment number or name followed by a colon. For example:

```
1:uap.prg
```

refers to the file named UAP.PRG that is located in segment 1. If you do not specify a segment name or number, the UAP searches the segments in the following order until it finds a file that matches the file name:

RAM, 1, 2, 3, 4

Using Console Commands

This section describes the console commands.

fb

You use the fb command to make an inactive segment the active segment. The format is:

```
fb boot segment data segment
```

where:

boot segment is the name or number of the boot segment to be activated.

data segment is the name or number of the data segment to be activated.

For example, to make segment 2 the active boot segment and segment 4 the active data segment, you enter:

```
fb 2 4
```

You can use an asterisk instead of a segment name if you want to leave that segment unchanged. For example, to leave the active boot segment unchanged and make segment 4 the active data segment, you could enter:

```
fb * 4
```

fd

You use the fd command to display the flash file system directory, which includes information about the boot file. The format is:

```
fd
```

You should use the fd command to ensure that the correct version of the file is in the active boot segment.

Note: If the active segment contains no files when you reboot the UAP, the unit enters the UAP monitor and you lose the ability to Telnet to it during this session. If this occurs, you must access the UAP through its serial port to correct the problem.

fdel

You use the fdel command to delete a particular file name from a segment. The format is:

```
fdel filename
```

where *filename* is the name of the file to be deleted.

For example, to delete the file UAP.PRG from the inactive boot segment, you could enter:

```
fdel ib:uap.prg
```

Note: When you use the fdel command, the file is marked as invalid and remains in the file system. To reclaim the file space, you must erase the entire segment. Use the fe command to erase a segment.

fe

You use the fe command to erase the files in a particular segment. To recover the files after they have been erased, you must reload them from another source. The format is:

```
fe segment
```

where *segment* is the name or number of the segment to be erased.

For example, to erase the contents of segment 1, you could enter:

```
fe 1
```

You can enter `ALL` instead of a segment name or number if you want to erase segments 1 through 4.

Note: You must execute the fe command before you can execute a TFTP transfer.

script

The script command executes a specified file as a list of console commands. You can create a script file to automate a software download.

The format is:

```
script filename
```

where *filename* is the name of the script file to be executed.

For more information about using the script command, see “Creating Script Files” later in this chapter.

Using Sdvars Commands

You use sdvars commands in Console Command mode to manipulate certain software download variables. Sdvars commands support both GET and SET arguments. You can enter sdvars commands to GET a software download object, and then issue the sdvars command using the SET argument to assign the object a specified value.

The sdvars commands are described in this section using the SET argument. To execute an sdvars command using the GET argument, omit the variable from the end of the command.

sdvars set serveripaddress

You use the sdvars set serveripaddress command to set the internal variable called serveripaddress to a specified address. The format is:

```
sdvars set serveripaddress ip address
```

where *ip address* is the address of the server.

For example, to set the IP address of the server to 1.2.3.4, enter:

```
sdvars set serveripaddress 1.2.3.4
```

sdvars set scriptfilename

You use the sdvars set scriptfilename command to set the internal variable scriptfilename to a specified string. The specified string should be the filename of the script to be retrieved from the TFTP server. The format is:

```
sdvars set scriptfilename foreign filename
```

where *foreign filename* is a script filename on the TFTP server.

For example, to set the scriptfilename to SCRIPT.DAT, enter:

```
sdvars set scriptfilename script.dat
```

sdvars set starttime

You use the sdvars set starttime command to set the internal variable starttime. Starttime is a countdown time such that when zero is reached, the software download process begins. You set this variable to reflect how long into the future the UAP is to begin downloading and executing the script file from the TFTP server. When the timer reaches 0, the UAP uses the values in serveripaddress and scriptfilename to get the script file that is to be executed. If either serveripaddress or scriptfilename contains no value, an error is noted in the status variable and the software download process is terminated. The format is:

```
sdvars set starttime dd:hh:mm:ss
```

where *dd:hh:mm:ss* is how far in the future the download is to begin.

For example, to begin the script file download in 5 minutes, enter:

```
sdvars set starttime 00:00:05:00
```

Note: If you need to stop the download, you can do so by setting starttime to 0 if it has not already been reached by the countdown. Resetting starttime to 0 stops the timer and the download process.

sdvars set checkpoint

You use the sdvars set checkpoint command to set the internal variable called checkpoint to a specified value. The checkpoint variable is useful for monitoring the progress of a script file as it is executed. You can set the checkpoint variable to a different value after each script command and then query the checkpoint value using SNMP to determine the progress of the download. The format is:

```
sdvars set checkpoint value
```

where *value* is a whole number.

For example, consider the following script file commands:

```
sdvars set checkpoint 1
fe ab
sdvars set checkpoint 2
TFTP get * uap.prg ab
sdvars set checkpoint 3
reboot
```

When the software download is started, you can use SNMP to query its progress by reading the checkpoint variable. If the variable has a value of 2, you know that the UAP is trying to execute the TFTP get statement. If the value is 3, you know the script has completed and the reboot was executed. The value of the checkpoint variable may also be helpful in determining where an error occurred if the script fails.

sdvars set terminate

You use the sdvars set terminate command to set the internal variable terminate to a specified value. Use terminate to stop a countdown process in the UAP. If either starttime or nextpoweruptime is counting down, setting this variable stops the timer and halts the countdown process. The format is:

```
sdvars set terminate
```

Note: You should use caution when using this command. If the script file is being downloaded or executed, setting this variable interrupts the processing and can leave the UAP in an undetermined state that may require user intervention.

sdvars set setactivepointers

You use the sdvars set setactivepointers command to change inactive segments to active segments the next time the UAP is rebooted. This command is usually used with the nextpoweruptime command. The format is:

```
sdvars set setactivepointers none/boot/data/both
```

where:

none does not change the active segments. *None* is the default. Also, when the reboot is completed, the UAP resets this value to *none*.

boot changes the inactive boot segment to the active boot segment.

data changes the inactive data segment to the active data segment.

both changes both the boot and data inactive segments to the active segments.

For example, to change the inactive boot and data segments to active at the next reboot, enter:

```
sdvars set setactivepointers both
```

sdvars set nextpoweruptime

You use the sdvars set nextpoweruptime command to set the internal variable nextpoweruptime to a countdown time so that when 0 is reached, the UAP will reboot. When the nextpoweruptime counter reaches 0, the UAP checks the value of the setactivepointers variable, takes the appropriate action, and then reboots. The format is:

```
sdvars set nextpoweruptime dd:hh:mm:ss
```

where *dd:hh:mm:ss* is how far in the future the reboot is to begin.

For example, to reboot the UAP 2 hours from now, enter:

```
sdvars set nextpoweruptime 00:02:00:00
```

Note: If you need to terminate the reboot, you can do so by setting nextpoweruptime to 0 if it has not already been reached by the countdown. By resetting nextpoweruptime to 0, the timer is stopped so the unit does not reboot.

Using TFTP Commands

TFTP commands are file transfer commands that you execute when you are in Console Command mode. A UAP can act as either a client or server in the TFTP environment. As a server, the UAP can service read and write requests from a UAP client. As a client, the UAP can read files from and write files to any TFTP server on the network. Both the client and server must operate in octet, or 8-bit, mode.

When executing a script file, the UAP retries TFTP client commands get and put until the command completes successfully. If the first attempt fails, the UAP retries after a one-minute delay. With each successive failure, the retry time doubles until it reaches 8 minutes. Once this limit is reached, it remains at 8 minutes until the command completes.

In general, TFTP client sessions should fail only if the server is not responding either because it is busy serving other clients or because it has not been started. In either case, the UAP backoff algorithm should prevent excessive network traffic when many UAPs are trying to contact a TFTP server.

tftp get

The TFTP client in the UAP supports standard get and put commands. You can use the TFTP get command to start a client session that gets a file from the TFTP server. The format is:

```
tftp get IP address foreign filename local filename
```

where:

IP address is the IP address of the server. You can use an asterisk (*) here if you want to use the value in serveripaddress.

foreign filename is the name of the file on the server. The file name can contain directory path information and must be in the format required by the server operating system. The file must already have the appropriate file header before the transfer to the UAP.

local filename is the name you wish to call the file on the UAP. The name must include a segment number or name followed by a colon. An actual file name is optional. If only the segment name is supplied, the file name is set equal to the file name that is embedded in the file header on the server.

For example, the following command gets file UAP.DNL from a directory on a PC server with IP address 1.2.3.4 and stores it in the inactive boot segment on the UAP.

```
tftp get 1.2.3.4 c:\startup\uap.dnl ib:
```

Note: You must use the fe command to erase the segment before you execute a TFTP get command. If you do not erase the segment, you may get a “can’t write file” error.

The following error messages may be generated by the UAP when the UAP issues a TFTP get command. Other error messages may be returned from the server and displayed by the UAP. See your server documentation for additional information.

Error Message	Explanation
Can’t write file	The file may be too big.
	The file may not have a UAP file header (filehdr.exe).
	The file name may be incorrectly formed.
	The file may already exist in the segment and cannot be overwritten. You must erase the file first.
Invalid opcode during read	This error should not occur under normal operating conditions. This error indicates a TFTP protocol error that will not occur when you use TFTP servers that conform to the protocol.

tftp put

TFTP put is another client command. You can use TFTP put to copy a file from a client to the server or to another UAP. The format is:

```
tftp put IP address foreign filename local filename
```

where:

IP address is the IP address of the server. You can use an asterisk (*) here if you want to use the value in the serveripaddress.

foreign filename is the name of the file as it will appear on the server. The file name can contain directory path information and must be in the format required by the server operating system.

local filename is the name of the file to be sent from the UAP.

For example, the following command takes file UAP.PRG that is saved in the active boot drive on the UAP client and stores it in the inactive boot segment on the UAP server that has IP address 1.2.3.4.

```
tftp put 1.2.3.4 ib:uap.prg ab:uap.prg
```

The following error messages may be generated by the UAP when the UAP issues a TFTP put command. Other error messages may be returned from the server and displayed by the UAP. See your server documentation.

Error Message	Explanation
Can’t read file	The requested file may not exist.
Invalid opcode during put	This error should not occur under normal operating conditions. This error indicates a TFTP protocol error that will not occur when you use TFTP servers that conform to the protocol.

tftp server log

Your UAP can function as a TFTP server. You can use the TFTP server log command to save a history of TFTP client requests. The format is:

```
tftp server log
```

The TFTP server log contains useful TFTP server status information. The log begins when you set up the server. You must reboot the UAP to clear the log.

tftp server start

A UAP can obtain files from a TFTP server. You can enable one UAP to act as a TFTP server and download files to additional UAPs. You use the TFTP server start command to enable your UAP to act as a server. The format is:

```
tftp server start
```

After you issue this command, the UAP responds to TFTP client requests that are directed to its IP address. When acting as a server, the UAP supports up to 4 concurrent TFTP sessions.

tftp server stop

When you are done transferring files, you can stop the UAP from being a TFTP server by using the TFTP server stop command. The format is:

```
tftp server stop
```

After you issue this command, the UAP no longer responds to TFTP client requests; however, current TFTP sessions with the server are allowed to complete.

The following table lists error messages that can be issued from the TFTP server. These messages are sent to the client and are meant to be read from the client perspective.

Error Message	Explanation
TFTP server only supports octet mode	The client is attempting to transfer a file in ASCII mode. The UAP TFTP server only supports octet mode, which includes binary and image.
Unable to open remote file	The TFTP server cannot open the file that is named in the read or write request. If you are trying to read a file, the file may not exist. If you are trying to write a file, the file may be too big, the file may not have a UAP file header, or the file name may be incorrectly formed.
Can’t read remote file	The server returns this message if the UAP file system returns an error while the server is attempting to read the file. This message is unlikely to occur.

Error Messages Issued by the TFTP Server (continued)

Error Message	Explanation
Can’t write remote file	The server returns this message if the UAP file system returns an error while the server is attempting to write the file. This message is unlikely to occur.
TFTP opcode not read or write request	This error should not occur under normal operating conditions. This error indicates that the TFTP client does not conform to the protocol.
Invalid opcode during read	This error should not occur under normal operating conditions. This error indicates that the TFTP client does not conform to the protocol.
Invalid opcode during write	This error should not occur under normal operating conditions. This error indicates that the TFTP client does not conform to the protocol.

Creating Script Files

You can create a script file that will execute a series of commands. Script files are ASCII text files with a 32-byte file system header appended. You may need to contact your local Intermec representative for a copy of the header file called filehdr.exe. The total file size including the header must be less than 4096 bytes, the size of the RAM file segment.

Each line in the script file must have fewer than 80 characters and be terminated by a line feed or carriage return. There can only be one command per line. You can include comments on a line by using the pound (#) sign; all characters after a pound sign are ignored.

When you upgrade the UAP, you typically need to erase the appropriate file segments, download the new files, and reboot using the new software. You can create a script file to perform these commands. To test a script file, you can log onto a UAP and type each of the script file commands. A sample script file is shown here.

```
#Sample script file for upgrading a UAP
#Step 1. Delete files
file sdvars set checkpoint 1
file fe ib:
file fe id:

#Step 2. Get boot files
file sdvars set checkpoint 2
file tftp get *\data\bootchk.dnl ib:
file tftp get *\startup\uap.dnl ib:
file tftp get *\startup\uapboot.dnl ib:
```

Sample Script File (continued)

```
#Step 3. Get data files
file sdvars set checkpoint 3
file tftp get *\data\bkgrnd.dnl id:
file tftp get *\data\bootchk.dnl id:
file tftp get *\data\discinca.dnl id:
file tftp get *\data\falcon_.dnl id:
file tftp get *\data\help.dnl id:
file tftp get *\data\hlp.dnl id:
file tftp get *\data\intermec.dnl id:
file tftp get *\data\menu.dnl id:
file tftp get *\data\sftdwnl.dnl id:
file tftp get *\data\welcome.dnl id:
file tftp get *\data\write.dnl id:

#Step 4. Set checkpoint to show completed
file sdvars set checkpoint 4
```

Using SNMP

The UAP supports SNMP management. Contact your Intermec representative for information about obtaining a copy of the MIB. The passwords for accessing the SNMP communityTable are shown below.

Type of Access	MIB Password
read only	public
read/write	CR52401

A

Specifications

This appendix provides technical specifications and system defaults for reference purposes only. Actual product performance and compliance with local telecommunications regulations may vary from country to country. Intermec only ships products that are type approved in the destination country.

Physical Specifications - 2100

Operating Temperature	
Standard Unit	0°C to 50°C (+32°F to +122°F)
Heater Module (optional)	-20°C to +50°C (-4°F to +122°F)
Heater Module (optional) and Insulated Bag (optional)	-30°C to 0°C (-22°F to +32°F)
Storage Temperature	-40°C to +70°C (-40°F to +158°F)
Humidity (non-condensing)	10 to 90%
Electrical	~100 to 240V 1.0 to 0.5A 50 to 60 Hz
Weight	2.63 kg (5.8 lb)
Height	95 mm (3.75 in)
Length	355 mm (14.00 in)
Width	236 mm (9.3 in)

Physical Specifications - 2101

Operating Temperature	0°C to +40°C (+32°F to +104°F)
Storage Temperature	-20°C to +70°C (-4°F to +158°F)
Humidity (non-condensing)	10 to 90%
Electrical	~100 to 240V 1.0 to 0.5A 50 to 60 Hz
Weight	526 g (1.16 lb)
Height	38 mm (1.49 in)
Length	250 mm (9.84 in)
Width	160 mm (6.27 in)

Radio Specifications - 900 MHz Falcon

Data rate	90, 225, or 450 Kbps (depends on installation)
Channels	7 @ 90 Kbps, 1 @ 225 or 450 Kbps
Range	Up to 600 m (2,000 ft) line of sight
Coverage	9,290 to 32,515 sq m (100,000 to 350,000 sq ft)
Frequency band	902 to 928 MHz (not available in Europe)
Radio type	Direct sequence, spread spectrum
Radio power output	Minimum 24dBm (250 mW) Typical 25.5dBm (350 mW) Maximum 27dBm (500 mW)

Radio Specifications - 2.4 GHz OpenAir

Data rate	1.6 Mbps
Channels	15
Range	Up to 150 m (500 ft) indoors Up to 300 m (1,000 ft) outdoors
Frequency band	2.4 to 2.5 GHz world-wide
Radio type	Frequency hopping, spread spectrum
Radio power output	
2100	500 mW 100 mW (Europe)
2101	100 mW

Radio Specifications - IEEE 802.11 Direct Sequence

Data rate	2 Mbps or 1 Mbps
Channels	11 (North America), 13 (Europe), 4 (France), 1 (Japan)
Range	425 m (1,400 ft) open environment 198 m (650 ft) semi-open environment 76 m (250 ft) semi-obstructed environment 40 m (130 ft) heavily obstructed environment
Frequency band	2.4 to 2.5 GHz world-wide
Radio type	Direct sequence, spread spectrum
Radio power output	15dBm

Radio Specifications - UHF

Data rate	19.2 Kbps (14.4 Kbps with forward error correction)
Channels spacing	20 KHz or 25 KHz
Receiver sensitivity	-105dBm
Range	Up to 1,067 m (3,500 ft) line of sight
Coverage	
0.5 W	74,320 sq m (800,000 sq ft) indoors
10 mW	9,290 sq m (100,000 sq ft) indoors
Frequency band	
Low band	430-450 MHz
High band	450-470 MHz
Radio type	Synthesized UHF (four-level frequency shift keying)
Radio power output	0.5 W (27dBm) low band 0.5 W (27dBm) high band 10 mW (10dBm) low band (must meet local regulatory requirements)

Other Specifications

Architecture	Transparent bridge
Ethernet interfaces	
2100	10Base2 (thin coaxial BNC) 10BaseT (twisted-pair)
2101	10BaseT (twisted-pair)
Data rate	10 Mbps (Ethernet)
Media Access protocol	CSMA/CD
Ethernet compatibility	Ethernet packet types and Ethernet addressing
Filtering rate	14,880 frames per second
Filters (protocol)	AppleTalk, NetBEUI, IPX, IP, DECNET, Other
Filters (others)	IP ARP, Novell RIP, SAP, LSP
Serial port max data rate	115,200 bps
Management access (Telnet, Web browser)	Intermec wireless LAN, serial, Ethernet
Software upgrades	Downloadable over the network or serial port
SNMP agent	Version 1 RFC 1213

Default Settings

The factory default settings for the UAP are listed in this section. You can record the settings for your installation in the table for reference.

Quick Start Menu Defaults

Parameter Name	Range	Default	Site Setting
IP Address	4 nodes, 0 to 255	0.0.0.0	
IP Subnet Mask	4 nodes, 0 to 255	255.255.255.0	
LAN ID	0 to 254	0	
AP Name	0 to 16 characters	(UAP serial number)	

Ethernet Port Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Hello Period	1, 2, or 3 seconds	2	
INCA Frame Type	DIX/SNAP	DIX	

2.4 GHz OpenAir Port Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Hello Period	1, 2, or 3 seconds	2	
Security ID	0 to 20 characters	(no password)	
2.4 GHz OpenAir-A			
Node Type	Master/Station	Master	
Channel	1 to 15	1	
Subchannel	1 to 15	1	
Wireless Hops	Disabled/Enabled	Disabled	

2.4 GHz OpenAir Port Configuration Menu Defaults (continued)

Parameter Name	Range	Default	Site Setting
2.4 GHz OpenAir-B			
Node Type	Master/Station	Station	
Channel	1 to 15	9	
Subchannel	1 to 15	9	
Wireless Hops	(does not apply)	(does not apply)	
MAC Configuration	Default/Manual/ Interference/ Throughput	Default	
Manual MAC Parms			
Hop Period	100/200/400 ms	200 ms	
Beacon Frequency	1 to 7	2	
Deferral Slot	Default/1/3/7	Default	
Fairness Slot	Default/1/3/7	Default	
Fragment Size	1 to 1540	310	
Transmit Mode	AUTO/BFSK/QFSK	AUTO	
Norm Ack Retry	1 to 255	255	
Frag Ack Retry	1 to 255	255	
Norm QFSK Retry	1 to 255	255	
Frag QFSK Retry	1 to 255	255	

900 MHz Falcon Port Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Hello Period	1, 2, or 3 seconds	1	
File Name	falcon_d.bin	falcon_d.bin	

IEEE 802.11 DS Port Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Hello Period	1, 2, or 3 seconds	2	
Network Name	0 to 32 characters	INTERMEC	
Frequency	2400 to 2500 MHz	2422 MHz	
WEP Encryption	Enabled/Disabled	Disabled	
WEP Configuration			
WEP Method for Authentication	Open System/Shared Key	Open System	
WEP Receive Data	Unencrypted Allowed/ Encryption Required	Encryption Required	
WEP Transmit Key	1 to 4	1	
WEP Default Key Configuration			
WEP Entry Mode	ASCII/hex	ASCII	
Advanced Configuration			
Medium Reservation	Enabled/Disabled	Disabled	
Reservation Threshold	0 to 2346	500	
AP Density	Low/Medium/High	Low	
DTIM Period	1 to 65535	1	
Multicast Rate	2 Mbits (Standard)/ 1 Mbits (Low)	2 Mbits (Standard)	
Transmit Rate Configuration			
Transmit Rate	2 Mbits (Standard)/ 1 Mbits (Low)	2 Mbits (Standard)	
Transmit Rate Fallback	Enabled/Disabled	Enabled	

UHF Port Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Hello Period	1, 2, or 3 seconds	2	
File Name	synuhf_d.bin	synuhf_d.bin	
Call Sign	0 to 12 characters	none	
Frequency	(programmed at factory based on regulatory requirements)	(first frequency in list)	
Master Mode	Enabled/Disabled	Disabled	
Attach Priority	Low/Medium/High/	High	

INCA/IP Port Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Hello Period	1, 2, or 3 seconds	2	
Mode	Originate If Root/ Listen	Listen	
IGMP	Enabled/Disabled	Disabled	

Network Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
IP Address	4 nodes, 0 to 255	0.0.0.0	
IP Subnet Mask	4 nodes, 0 to 255	255.255.255.0	
IP Router	4 nodes, 0 to 255	0.0.0.0	
IP Frame Type	DIX/SNAP	DIX	
DHCP	Enabled/Disabled/ Enabled (if 0)	Enabled (if IP Address = 0)	
DHCP Server Name	0 to 31 characters	(blank)	
Auto ARP Minutes	0 to 120	5	

Bridge Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
LAN ID	0 to 254	0	
Root Priority	0 to 7	1	
Ethernet Bridging	Enabled/Disabled	Enabled	
Secondary LAN Bridge Priority	0 to 7	0	
Secondary LAN Flooding	Disabled/Enabled/ Multicast/Unicast	Disabled	
Global Flooding			
Multicast			
Flood Mode	Hierarchical/ Universal/Disabled	Hierarchical	
Outbound to Terminals	Enabled/Disabled	Enabled	
Outbound to Secondary LANs	Set Locally/Enabled	Set Locally	
Unicast			
Flood Mode	Hierarchical/ Universal/Disabled	Disabled	
Outbound to Terminals	Enabled/Disabled	Disabled	
Outbound to Secondary LANs	Set Locally/Enabled	Set Locally	
ARP Server Mode	Disabled/ No Flooding/ Normal Flooding	Disabled	

Bridge Configuration Menu Defaults (continued)

Parameter Name	Range	Default	Site Setting
Global RF Parameters			
400 MHz UHF Rfp Threshold			
Set Globally	Enabled/Disabled	Disabled	
Value	0 to 250	70	
400 MHz UHF Frag Size			
Set Globally	Enabled/Disabled	Disabled	
Value	50 to 250	250	
900 MHz Frag Size			
Set Globally	Enabled/Disabled	Disabled	
Value	50 to 250	250	
400 MHz UHF/900 MHz Awake time			
Set Globally	Enabled/Disabled	Disabled	
Value	0 to 250	0	

Maintenance Menu Defaults

Parameter Name	Range	Default	Site Setting
Password	16 characters	Intermec	
Service Password	Enabled/Disabled	Enabled	

B

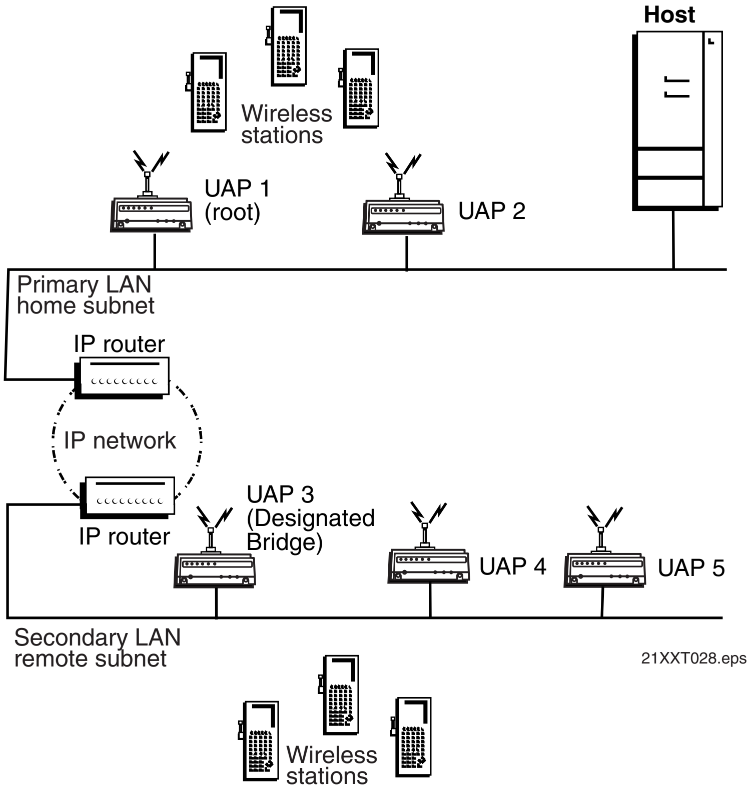
Understanding INCA/IP

This appendix provides additional information about INCA/IP.

An Overview of INCA/IP

The presence of an IP router generally defines the physical boundary of a wireless network. Multiple independent wireless networks may exist, each with its own LAN ID, root, and set of end devices. In this environment, an end device can only operate within the limited coverage area of its own network and cannot roam across IP subnet boundaries. Intermec's Integrated Network Communication Architecture/Internet Protocol (INCA/IP) allows end devices to roam across subnet boundaries.

The INCA/IP extension to the open wireless LAN architecture enables a wireless LAN installation to span multiple IP subnets. INCA/IP uses a standard IP protocol called Generic Routing Encapsulation (GRE) to encapsulate a frame within an IP/GRE packet that uses normal IP routing to pass through IP routers. Using INCA/IP, end devices can roam across IP network subnets without losing network connectivity. INCA/IP can also be used to route protocols that are normally not routable.



You should have a basic understanding of IP addressing conventions and routing before you attempt to configure and use the advanced capability of INCA/IP. INCA/IP does the following:

- Enables access points on different IP subnets to belong to the same wireless network
- Supports transparent roaming of end devices between access points that are on different IP subnets without losing network connections
- Supports end devices using both IP and other routable or nonroutable protocols

You activate INCA/IP by configuring the root UAP to originate INCA/IP tunnels. The IP tunnel originates at the root UAP on the home IP subnet and terminates at a UAP on a remote IP subnet. Frames forwarded through the tunnel are encapsulated using the standard GRE protocol running over IP.

The INCA/IP port differs from the physical ports within the UAP. The INCA/IP port is a logical port that provides IP encapsulation services for frames that must be routed to reach their destination. After encapsulation, frames are transmitted or received through the physical Ethernet ports.

INCA/IP Restrictions

This section will help you understand operational requirements for INCA/IP.

Address Restrictions

End devices that are using IP must be assigned IP addresses that are on the home IP subnet. The home IP subnet is the subnet connected to the root UAP. There are no address restrictions for non-IP end devices.

Installation Restrictions

Servers that use a routable network protocol such as IP or IPX may be located on any subnet; however, triangular routing can be minimized if servers are located on the home subnet for end devices. (Note that this is also true for standard Mobile IP.) INCA/IP does not require changes to default INCA flooding and bridging settings if it is only used for routable protocols, even if servers are located on remote subnets.

The Intermec NNL protocol is a simple Non-routable Network Layer protocol that is used to carry high-layer data in a local area network environment. An Intermec NNL gateway forwards NNL traffic to non-NNL hosts such as TCP/IP. You can use the default INCA flooding and bridging settings, and minimize triangular routing, if NNL gateways are located on the home subnet. You must enable outbound multicast flooding and secondary bridging for remote INCA/IP subnets that contain NNL gateways.

Bridging Restrictions

By default, wireless traffic is not bridged to a remote INCA/IP subnet. If bridging to a remote subnet is enabled, then the subnet functions as a secondary LAN and a single UAP functions as the designated bridge for the INCA/IP secondary LAN. (You may need to enable bridging on an INCA/IP remote subnet if an Intermec NNL gateway is attached to the subnet.) Non-routable network protocols that an IP router is configured to bridge should not be forwarded through an INCA/IP tunnel if bridging is enabled on the respective INCA/IP secondary LAN. Many routers may be configured to bridge specific non-routable frame types. These routers are often referred to as B routers.

Bridging must not be enabled on remote INCA/IP subnets if INCA/IP is used to provide mobility for routable protocols other than IP, such as IPX.

Bridging can be enabled on remote INCA/IP subnets if INCA/IP is used to provide mobility for IP and other non-routable protocols, because INCA/IP has built-in safeguards and filters for the IP protocol. You may need to enable bridging if your end devices use both IP and NNL, and NNL gateways are connected to remote INCA/IP subnets.

INCA/IP Safeguards

The purpose of a router is to segment traffic on a local network and selectively forward frames destined to network addresses on other networks. Routers avoid problems such as broadcast storms that are often associated with bridges. INCA/IP is designed to safely and transparently coexist with routed IP installations while supporting mobility for end devices. This section details the safeguards built into INCA/IP.

Wireless Hop Restriction

To use INCA/IP, you must configure UAPs that are on different IP subnets so that they have the same INCA LAN ID. INCA hello messages contain the IP subnet ID of the UAP that originated the message. The INCA protocol does not allow wireless links to exist between UAPs that do not have matching subnet IDs.

Tunnels Manually Enabled

By default, INCA/IP tunnel origination is disabled on the UAP. You must manually enable INCA/IP tunnel origination in the root UAP before any INCA/IP tunnels can be established.

INCA/IP Virtual Subnet

INCA/IP provides a virtual subnet for end devices because INCA/IP tunnels logically extend the home subnet. The UAP's default bridge priority of zero disables the bridging of wireless traffic to remote INCA/IP subnets. The default setting allows terminals that are connected to UAPs on a remote INCA/IP subnet to communicate with hosts on the primary LAN or home subnet without bridging wireless traffic to the remote INCA/IP subnet. Frames that originate on a remote INCA/IP subnet are not forwarded inbound through an INCA/IP tunnel.

Permanent and User-Defined Filters

The UAP provides extensive filtering capabilities so that only traffic destined to end devices is allowed.

ARP Server

For wireless IP devices, ARP requests that originate on the home subnet must be forwarded outbound to remote INCA/IP subnets. An ARP server capability can be enabled to restrict the propagation of ARP packets through tunnels to only those packets that are destined for end devices.

Forwarding Restrictions

Unicast frames are only forwarded outbound through an INCA/IP tunnel if the destination address identifies an end device that has roamed to a remote subnet. By default, wireless traffic is not bridged to remote INCA/IP subnets; traffic from a remote IP subnet is never forwarded inbound through an INCA/IP tunnel.

Permanent Filters

Certain frame types are never forwarded through tunnels; other frames are always forwarded. Frame types that are never forwarded include IP protocols used for coordinating routers and MAC frames used for coordinating bridges.

Frame Types That Are Never Forwarded

- 802.1d bridge frames
- Proprietary VLAN switch frames
- IP frames with a broadcast or multicast Ethernet address

Frame Types That Are Never Forwarded (continued)

- IP frames with the following router protocol types and decimal values:
  - DGP (86) (Dissimilar Gateway Protocol)
  - EGP (8) (Exterior Gateway Protocol)
  - IDPR (35) (Inter-Domain Policy Routing Protocol)
  - IDRP (45) (Inter-Domain Routing Protocol)
  - IGP (9) (Interior Gateway Protocol)
  - IGRP (88)
  - MHRP (48) (Mobile Host Routing Protocol)
  - OSPFIGP (89) (Open Shortest Path First Interior Gateway Protocol)
- IP ICMP (Internet Control Message Protocol) types:
  - IPv6
  - Mobile IP
  - Router Advertisement
  - Router Selection
- IP/UDP (User Datagram Protocol) frames with the following destination protocol port numbers:
  - BGP (179) (Border Gateway Protocol)
  - RAP (38) (Route Access Protocol)
  - RIP (520) (Routing Information Protocol)
- IP/TCP frames with the following destination or source protocol port numbers:
  - BGP (179) (Border Gateway Protocol)
  - RAP (38) (Route Access Protocol)

User-Defined Filters

You can define output filters that restrict protocol types that can pass through an INCA/IP tunnel. Frames can be filtered by the DIX, 802.2, or 802.3 SNAP type, the IP protocol type, or the TCP or UDP protocol port number.

By default, the filters drop all protocol types except the NNL DIX Ethernet type (hexadecimal 875B). You can configure the INCA/IP filters to pass additional frame types by choosing the Filters option from the Bridge Configuration menu. Filters must be configured in all root candidates and in any UAP that can attach to the remote end of an INCA/IP tunnel.

IP/ARP Subnet Filtering

INCA/IP automatically provides subnet filtering for IP end devices. IP and ARP frames are never forwarded inbound through an INCA/IP tunnel to the home subnet unless the source IP address belongs to the home subnet. (Frames are only forwarded inbound if the source IP address in the IP or ARP packet identifies an end device that has roamed away from its home subnet.)

IP and ARP frames are never forwarded outbound through an INCA/IP tunnel by the root UAP unless the destination IP address belongs to the home subnet. (Frames are only forwarded outbound to end devices that have roamed away from the home subnet.)

Operation

INCA/IP uses IP encapsulation to establish a virtual LAN segment through IP routers. The virtual LAN segment includes the home IP subnet and logically extends to include end devices attached to UAPs on remote IP subnets. An INCA/IP tunnel becomes a branch in the INCA spanning tree. UAPs on remote subnets can be directly connected to an INCA/IP tunnel or indirectly connected through another UAP on a remote subnet.

Tunnel Origination

An INCA/IP remote subnet functions much like a wireless secondary LAN with some notable exceptions:

- Any UAP can provide a wireless link to another UAP. Only the root UAP can originate an INCA/IP tunnel.
- A wireless link can provide a transparent bridge for both wired and wireless devices on a wireless secondary LAN. An INCA/IP tunnel only provides a transparent bridge for end devices (unless explicitly configured to provide connectivity for an NNL gateway on a remote IP subnet).

The number of INCA/IP tunnels the root can originate is practically unlimited. However, the INCA/IP address list can presently contain eight entries. The size of the address list effectively limits the number of tunnels that can be created if unicast and directed broadcast IP addresses are used. However, you can use a single IP multicast address to originate a practically unlimited number of tunnels.

By default, any UAP can attach to an INCA network through an INCA/IP tunnel if it receives INCA/IP hello messages. An INCA/IP tunnel is established when a UAP on a remote subnet attaches to the root UAP on its INCA/IP port.

Note that a non-root UAP can concurrently receive hello messages on its Ethernet port, its radio port(s), and its logical INCA/IP port. However, an INCA UAP uses only one port to attach to the INCA network. UAP port costs are structured so that an Ethernet connection is always selected before an INCA/IP or radio connection. An INCA/IP connection is always selected before a radio connection. The attachment port is its “root port.”

Building the Spanning Tree

UAPs use an election process to determine the root for an INCA network. After the root UAP is elected, it transmits INCA hello messages on all enabled ports. The INCA spanning tree forms as other UAPs receive hello messages and attach to the network on the optimal path to the root. A non-root UAP also transmits hello messages after it is attached to the network.

Each hello message contains the IP subnet ID of the UAP that originated the message. The INCA protocol does not allow wireless links to exist between UAPs that do not have matching subnet IDs.

Establishing and Maintaining Tunnels

If mode is set to originate if root in the root UAP, the root sends hello messages to each IP address contained in its INCA/IP address list. A UAP on a remote IP subnet can automatically establish an INCA/IP tunnel if it receives an INCA/IP hello message from the root UAP. A UAP that attaches through an INCA/IP tunnel transmits hello messages on the remote subnet so that other UAPs on the remote subnet that do not receive INCA/IP hello messages can attach to the INCA network.

If you need to bridge to an INCA/IP remote subnet, you must set the Secondary LAN Bridge Priority parameter to a value greater than 0 in one or more UAPs on the remote subnet. These designated bridge candidates use the bridge priority value in an election procedure (similar to that used to determine the root) to determine a single designated bridge for the secondary LAN.

Redundancy

The root and designated bridge election procedures are repeated if the current root or designated bridge stops sending hellos. If a UAP is unavailable due to a cable or other failure, the remaining UAPs use the election procedure to determine a new root or designated bridge.

Normally one primary and one or two fallback root candidates are sufficient for root redundancy. One primary designated bridge and one fallback are recommended for most remote subnet installations. The number of remote subnets and the redundancy needs on each subnet influence the selection of address types in the INCA/IP Addresses menu. For example, you can use an IP multicast address or multiple unicast addresses to provide redundancy. Multiple UAPs on a remote subnet can receive INCA/IP hello messages; a single unicast IP address does not provide redundancy.

Frame Forwarding

MAC frames originating on the home IP subnet are encapsulated in the root UAP, forwarded through the IP network, deencapsulated by the UAP at the remote end of the INCA/IP tunnel, and forwarded to the appropriate UAP (if necessary) for delivery to the intended end device. For inbound frames, the same process is used in reverse between the UAP at the remote end of an INCA/IP tunnel and the root UAP.

The encapsulation uses the standard IP GRE protocol. Any data packet sent through the tunnel is addressed to the unicast IP address of the UAP at the other end of the tunnel. A UAP at the remote end of the tunnel learns the unicast IP address of the root UAP by listening to INCA/IP hello packets. The root UAP learns the unicast IP address of a remote UAP when the UAP attaches to the INCA network.

Outbound

Data frames are forwarded outbound through an IP tunnel if

- an end device is known to be attached to a UAP on a particular remote subnet.
- the frame type is enabled in the INCA/IP Filter menu.

Unicast frames are not flooded. End devices attach to the root UAP, which maintains entries for these devices in its forwarding database. The database entries indicate the correct subnet for outbound forwarding.

For TCP/IP applications, IP and ARP frames must be forwarded through INCA/IP tunnels. An IP or ARP frame is only forwarded outbound if the destination address identifies an end device on the home subnet. Enabling the ARP server in the root UAP can reduce the number of ARPs forwarded outbound.

Inbound

Only frame types that are specified in the INCA/IP Filter menu are forwarded, and the frames are only forwarded inbound if the source IP address belongs to the home subnet.

Frames transmitted by servers or devices that are wired to an INCA/IP secondary LAN are not forwarded through INCA/IP tunnels if the IP address does not belong to the home subnet of the INCA/IP tunnel. Only frames from radio stations with IP addresses belonging to the home subnet are forwarded inbound.

End Device Mobility

As end devices move through a facility, they roam between UAP coverage areas. In large installations, these UAPs may be on different IP subnets. INCA/IP is designed to support rapid roaming in these environments. A roam requires updates to the forwarding databases in the new UAP, root UAP, previous UAP, and any intermediate UAPs.

An end device initiates a roam when it attaches to a new UAP. The UAP sends an attach message to the root UAP, which in turn forwards a detach message to the previous UAP, allowing each UAP to update its forwarding database. Intermediate UAPs monitor these exchanges and update their forwarding databases.

Mobile IP Comparison

The Internet Engineering Task Force developed RFC 2002, IP Mobility Support, commonly referred to as Mobile IP, to provide mobility for IP hosts. Mobile IP is designed primarily to address the needs of IP end device that may move between geographically separated locations.

INCA/IP is designed primarily to operate in local environments, where hand-held or vehicle-mounted end devices may move rapidly between UAP coverage areas on a subnetted LAN (although it is possible to attach a geographically remote subnet through an INCA/IP tunnel). The two technologies are complimentary and may coexist. Both protocols use similar encapsulation to forward packets to or from end devices that have roamed away from a home IP subnet. The root UAP functions much like a Mobile IP home agent; a UAP attached to the remote end of an INCA/IP tunnel functions much like a Mobile IP foreign agent. The following table summarizes the differences between INCA/IP and Mobile IP.

Issue	Mobile IP	INCA/IP
Software compatibility	Requires a Mobile IP client software stack in IP end devices.	No changes are required to existing IP software stacks in end devices.
Addressing limitations for IP end devices	None.	Requires that IP device addresses belong to the INCA/IP home subnet.
Security	Mobile IP authentication is required for “guest” access to foreign subnets.	Guest addresses are not used. Data link security.
Roaming detection	Foreign agent advertisements.	Data link indications facilitate fast roaming with no added broadcast traffic.
Roaming restrictions	None.	Currently, roaming is limited to a single INCA network that may include multiple IP subnets.
Roaming support for non-IP protocols	None.	Configurable using INCA/IP filters.
Scalability	Has no inherent limitations.	No practical limitations using IGMP.
Special network software	Requires home and foreign agents located on each network or subnetwork.	Standard INCA network feature. No additional network software is required.

Configuring an INCA/IP Tunnel

1. Choose the home subnet. Ideally, you should choose the subnet that contains gateways or servers for end devices; however, these servers may be on other subnets if necessary. Note that you can create a home subnet for end devices. Fixed or variable length subnet masks can be used; subnet addressing is not required. IP addresses for end devices must belong to the home subnet.
2. Select primary and fallback root UAPs on the home subnet. The root UAP should be a UAP that does not otherwise handle a large volume of traffic.
3. Configure all UAPs on the root IP subnet and remote INCA/IP subnets with the same INCA LAN ID. If INCA/IP is not used to attach a remote IP subnet, then UAPs on that subnet should be configured with a different LAN ID.
4. From the Quick Start menu, choose INCA/IP to configure root candidates to the originate if root setting. Configure the IP Addresses table using the appropriate addressing for UAPs on each remote IP subnet. All root candidates should be configured identically.
5. To configure INCA/IP filters, choose Bridge Configuration from the main menu, and then choose Filters. Configure filters in all root UAP candidates and in other UAPs that can attach through an INCA/IP tunnel. INCA/IP output port filters are consistent with Ethernet type and subtype filters.
6. For networks using IP networking on end devices, Intermec recommends that you use the ARP server capability in the UAP.
7. You may need to enable bridging on remote INCA/IP subnets. For example, bridging must be enabled if an Intermec NNL gateway is attached to the remote subnet. If bridging is required, configure one or more designated bridge candidates by setting the Secondary LAN Bridge Priority parameter to a value greater than zero. The designated bridge candidates must have permanent IP addresses and must be able to receive INCA/IP hello messages from the root UAP. A UAP will receive INCA/IP hello messages if the messages are sent to the unicast IP address of the UAP, or to an IP-directed broadcast or IP multicast address. Note that IGMP may be required for IP multicast.

INCA Topologies

The creation of tunnels between the root UAP and remote IP subnets is controlled by three operational parameters:

- The INCA/IP address list in the root UAP, configured through the INCA/IP port
- Secondary LAN bridge priority settings
- Enabling/disabling INCA/IP ports

A tunnel can never be established on a disabled INCA/IP port. The discussion below assumes that INCA/IP ports are enabled, unless noted otherwise.

The INCA/IP address list can contain any combination of IP unicast, IP broadcast, or IP multicast addresses. Only one INCA/IP tunnel can be created for each IP unicast address in the list. A single IP multicast address can be used to create a practically unlimited number of tunnels to multiple remote IP subnets. A single IP directed broadcast address can be used to create a practically unlimited number of tunnels to a single remote IP subnet. (An IP directed broadcast address is typically used to specify all hosts on a single remote subnet.)

By default, bridging to a remote INCA/IP subnet is disabled. In this default case, any UAP on a remote subnet that can receive INCA/IP hello messages can establish an INCA/IP tunnel; therefore, multiple INCA/IP tunnels can exist between the root UAP and a single remote IP subnet.

If INCA/IP hello messages are sent to unicast IP addresses, then some UAPs on a remote subnet will likely not receive hello messages, and, therefore will not be able to establish an INCA/IP tunnel. If bridging is disabled on the subnet, then wireless traffic is forwarded to and from these UAPs through data link tunnels. A data link tunnel is logically concatenated with an INCA/IP tunnel so that wireless traffic can be completely isolated from the remote IP subnet.

If bridging is enabled on an INCA/IP remote subnet, then a single UAP functions as the designated bridge for the INCA/IP secondary LAN. In this case, only the designated bridge can establish an INCA/IP tunnel. Any other UAP on the remote subnet must attach to the network through the designated bridge.

IGMP

IP multicast relies on an IP protocol called Internet Group Management Protocol (IGMP) for multicast packet distribution. An IP router will only forward an IP multicast packet to those IP subnets that have hosts that participate in the respective multicast group. An IP host uses IGMP to notify IP routers that it wants to participate in a multicast group. Intermec UAPs can be enabled to advertise participation in a single multicast group by enabling IGMP and defining a Class D IP multicast address. The Internet Assigned Numbers Authority has allocated a Class D address of 224.0.1.65 for Intermec's INCA inter-access-point protocol. The UAP IGMP feature is structured so that it is independent of INCA/IP; it can be used to facilitate IP multicast for INCA/IP or any other application.

IP multicast provides an ideal way to distribute INCA/IP hello messages. If IP multicast is used, the user must select a single IP multicast address, which is normally Intermec's registered address of 224.0.1.65. The selected address must be configured in the INCA/IP address list in the root AP. (Note that the address list can contain other IP addresses.) Normally, IGMP is enabled and an IGMP address is configured in at least one AP on each remote IP subnet. (Some routers can provide proxy IGMP services for IP hosts.) IP multicast has the following advantages:

- The user does not have to know unicast or directed broadcast IP addresses in advance.
- IP multicast provides better built-in redundancy than IP unicast, because any UAP can potentially establish an INCA/IP tunnel.
- INCA/IP hello messages are only forwarded to those IP subnets and IP hosts (such as INCA UAPs) that participate in the INCA multicast group. Directed broadcast packets are forwarded to all IP hosts on the target subnet.

C

Positioning Antennas

This appendix provides information about positioning the antennas for the UAP. Specific guidelines for antenna separation are provided for those configurations that have multiple antennas.

Antenna Placement Guidelines

Every environment is unique with different obstacles and materials. Therefore, the exact range that you will achieve with your UAP is difficult to determine. Intermec recommends that you allow an Intermec-certified RF specialist to perform a site survey before you install a wireless network. For more information on site surveys, contact your local Intermec representative.

Radio signals may reflect off some obstacles and be absorbed by others. For example, two radios may achieve up to 305 meters (1,000 feet) of range if positioned outdoors within line of sight, with no obstacles between them. However, the same two units may only achieve up to 152 meters (500 feet) of range when the RF signal has to travel through items such as cubicles. If the signal must penetrate office walls, the signal range may decrease to 91 meters (300 feet).

Proper antenna placement can help improve range. If you are interested in antenna options, contact your Intermec representative about antenna kits. Here are some general guidelines for positioning antennas:

- Place the antenna as high as possible. In an office environment, try to place it above cubicle walls.
- Do not place a sheet of metal (such as a filing cabinet) between two antennas.

The following sections provide detailed information about antenna placement for those UAPs that can have more than one antenna.

Positioning the Antennas for a 2.4 GHz OpenAir WAP

Because the 2.4 GHz OpenAir WAP has two radios installed in the device, you need to pay particular attention to the placement of the two antennas. Proper positioning of the antennas is critical for proper functioning of the WAP. You attach antenna cables to the 2110, and then attach the cables to antennas mounted in your work environment.

There are two types of Intermec-recommended antennas you can use:

- Omni
- Directional

You can position the antennas in one of three ways:

- Horizontal. Both antennas are mounted in the same plane (at the same height).
- Stacked. One antenna is mounted directly above the other.
- Angled. The two antennas are mounted some distance apart and at different heights.

You can use either two omni antennas, two directional antennas, or one omni antenna and one directional antenna. The following table shows the MINIMUM distance that must exist between the two antennas.

Position	2 Omni Antennas	2 Directional Antennas	1 Omni, 1 Directional Antenna
Horizontal	3dBi omni, 3 meters (10 feet) 6dBi omni, 6.1 meters (20 feet) 9dBi omni, 12.2 meters (40 feet)	3 meters (10 feet)	6.1 meters (20 feet)
Stacked	.6 meters (2 feet)	(does not apply)	.6 meters (2 feet)
Angled	1.1 meters (3.5 feet) vertically and 7.3 meters (24 feet) horizontally	.6 meters (2 feet) vertically and 3 meters (10 feet) horizontally	.6 meters (2 feet) vertically and 6.1 meters (20 feet) horizontally

Note these additional points about positioning your antennas:

- Intermec recommends that you mount omni antennas so they point down.
- If you are using one omni antenna and one directional antenna, you should mount the directional antenna so that it points away from the omni antenna.
- If you are using one omni antenna and one directional antenna in the stacked position, you must mount the directional antenna above the omni antenna.
- If you are using two directional antennas, you must mount them back-to-back.

Positioning the Antennas for an IEEE 802.11 DS Radio

The IEEE 802.11 DS radio features antenna diversity, which means that each radio has two antennas. One antenna functions as a receive antenna and the other antenna functions as both a transmit and a receive antenna. Note that only one antenna is used at a time in a diversity system.

On an IEEE 802.11 DS radio, the centermost antenna is the antenna that both transmits and receives radio signals. If you attach only one antenna to the IEEE 802.11 DS radio, you should attach it to the centermost antenna connector for that radio card.

If you are using two antennas for your IEEE 802.11 DS UAP, placement of the antennas is critical because each antenna has a particular function. Antennas placed too close together may cause interference with each other. Antennas placed too far apart may not be able to establish two-way communications with other radios. To achieve optimum placement for the two antennas, you must place the transmit/receive antenna so that it is within range of all the radios that the receive-only radio can hear.

Note these important points about antenna placement for an IEEE 802.11 DS radio:

- Use the recommended antenna separation for placement of either omni or directional antennas.
- Position directional antennas so they point in the same direction.
- Follow the recommended antenna separation precisely when using the closest distances. Movement of as little as 3.05 centimeters (1.2 in) may strongly affect performance.
- Position the antennas so that both antennas are within range of the radios they need to communicate with.
- Do not position the two antennas around a corner or so that a wall is between them.

The recommended antenna separation is listed in the following table. You should choose the greatest distance possible within the constraints of your environment.

Location	Recommended Antenna Separation
Highly reflective warehouse environment	.33 m (13 in) or .64 m (25 in)
Moderately reflective warehouse environment	.64 m (25 in), 1.22 m (4 ft), or 1.83 m (6 ft)
Open/Office environment	1.22 m (4 ft) to 3.05 m (10 ft)

D

Upgrading the UAP

This appendix provides instructions for upgrading the UAP firmware.

Upgrading UAP Firmware

For optimal performance, you should ensure that all the UAPs in your network use the most current version of the firmware. Contact your Intermec representative for information about obtaining the latest firmware release. The firmware release is distributed electronically along with release notes that provide additional information.

After you have the firmware release installed on your PC, you can upgrade a UAP using the following methods:

- A serial transfer from a PC to the UAP
- A TFTP transfer from a TFTP server to the UAP
- Through a Web browser from the root UAP to other UAPs

Intermec recommends that you upgrade the root UAP using a serial connection or TFTP, and then use the Upgrade Other UAPs feature available through the Web browser interface to upgrade the remaining UAPs on the network. The upgrade procedures are described in the following sections. Upgrade procedures are also included in a readme.txt file that accompanies the firmware release files. Consult the README.TXT file for the most current procedures.

Note: You must have the firmware release files installed in the directory c:\2100uap on your PC before you begin either a serial transfer or a TFTP transfer.

Performing a Serial Transfer

To perform a serial transfer, you must have the firmware release files on your PC and have an RS-232 null-modem cable connecting the UAP to your PC. Set the serial port terminal communications parameters on your PC to the following values:

Parameter	Setting
Data bits	8
Parity	none
Stop bit	1
Flow control	none

For the most efficient upgrade, you should set the baud rate on both your PC and the UAP to 115,200 bps. For information about changing the baud rate on the UAP, see “Using UAP Monitor Commands” in Chapter 8. The baud rate on your PC must match the baud rate on the UAP.

To perform a serial transfer

1. Reboot the UAP and enter the UAP monitor by pressing any key when asked. The UAP prompt (uap>) appears.
2. To enter service mode, type `srvc` and press **Enter**.
3. Enter the service password. The default password is EV98203S (case sensitive). The service prompt (service>) appears.
4. Type `fd` and press **Enter**. The file directory appears.
5. Scroll up until you see a section similar to the following:

   ```
   Startup Segment:  This startup = 1,  Next startup = 1
      Data Segment:  This startup = 3,  Next startup = 3
   ```

6. Identify the startup and data segments for this startup—these are the current active segments. In the above example, the active startup segment is segment 1 and the active data segment is segment 3.

   You load the new firmware into the inactive segments and then make the segments active. If the active segments are 1 and 3, then the inactive segments are 2 and 4.

7. Erase the inactive startup segment. For example, if the inactive startup segment is segment 2, type:

   `fe 2` and press **Enter**. A ‘P’ appears when the action is complete.

8. Erase the inactive data segment. For example, if the inactive data segment is segment 4, type:

   `fe 4` and press **Enter**. A ‘P’ appears when the action is complete.

9. You must perform these file transfers, in order, to copy files to the inactive startup segment. Use the fx command to start the transfer and then use the Ymodem send command on the PC to transfer the files. Enter these commands:

   Type `fx` *`s`* where *`s`* is the inactive startup segment.
   Copy this file to the startup segment: `c:\2100uap\data\bootchk.dnl`
   Type *`fx s`* where *`s`* is the inactive startup segment.
   Copy the remaining startup files to the startup segment by specifying this directory path: `c:\2100uap\startup\*.dnl`

10. Start the file transfer for the data files. For example, to start the file transfer to segment 4, type:

    fx 4

11. Start the file transfer on the PC using the Ymodem send command. Copy the data files to the inactive data segments by specifying this directory path:

    c:\2100uap\data\*.*

12. Make the inactive segments active. For example, to make segments 2 and 4 active, type:

    `fb 2 4.` A ‘P’ appears when the action is complete.

13. Type `x` to exit the service menu.
14. Restore the original baud rate using the SR command, if needed.
15. To reboot the UAP, type `b` and press **Enter**.

After you complete the upgrade, you must reconfigure the UAP for your installation. Save the configuration and then reboot the UAP to make the configuration active.

Performing a TFTP Transfer

If you have a TFTP server, you can upgrade a UAP over the network from the server. You can perform the upgrade by executing the compiled script file upgrade.dnl that is included with the firmware release. When you execute the script file, a TFTP transfer is performed that copies all the startup and data files to the UAP.

See the procedures in this section and the release notes that accompany the firmware upgrade for more information about using the script file. A sample script file is included in Chapter 8, “Advanced Features.”

You can execute the script file from a serial console or Telnet session. Additionally, if you have UAP code version 2.73 firmware or greater on your UAP, you can execute the script file from a Web browser session. You can determine your current UAP code version by choosing the Maintenance command and then the About Intermec UAP command from the UAP Configuration menu.

This section includes instructions that describe how to perform a TFTP transfer

- via a Telnet session.
- via a Web browser session.

Performing a TFTP Transfer Via a Telnet Session

1. Start the TFTP server.
2. Establish a Telnet session with the UAP. For detailed instructions, see Chapter 6, “Managing the UAP Remotely.”
3. Choose the Maintenance command, and then choose Command Console.

4. Use the sdvars set serveripaddress command to specify the IP address of the TFTP server. (For more information about using sdvars commands, see Chapter 8, “Advanced Features.”) For example, if the server IP address is 151.60.110.241, type:

   ```
   sdvars set serveripaddress 151.60.110.241
   ```

5. Use the sdvars set scriptfilename command to identify the script file. Type:

   ```
   sdvars set scriptfilename c:\2100uap\upgrade.dnl
   ```

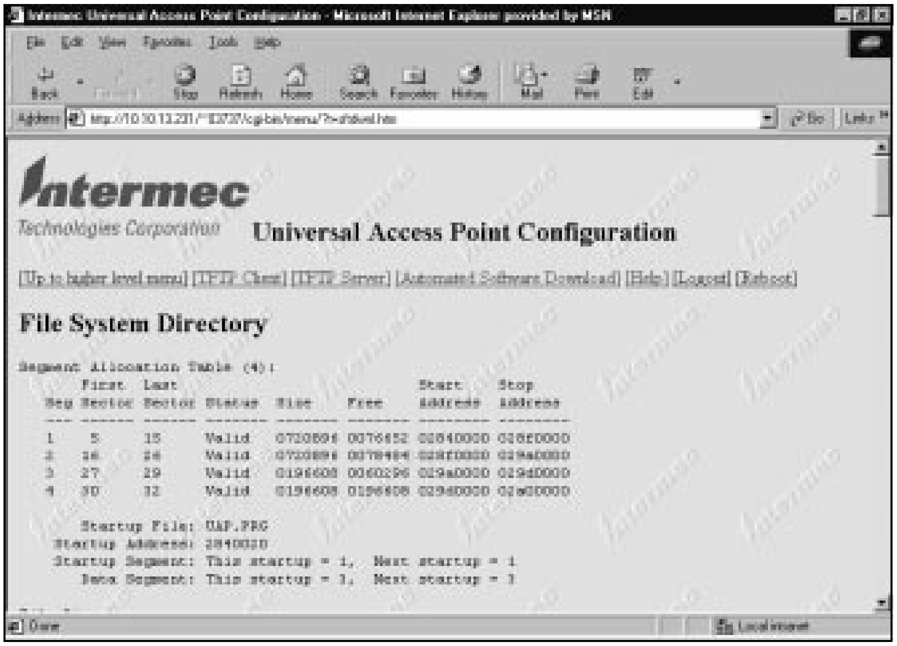
6. Use the sdvars set starttime command to set the start time for the upgrade in dd:hh:mm:ss format. Start time is a countdown timer—when the timer expires, the download begins. You can enter days, hours, minutes, and seconds in the Start Time field. For example, to start the upgrade in two hours and ten minutes, type:

   ```
   sdvars set starttime 00:02:10:00
   ```

   When the starttime counter reaches zero, the upgrade begins. The UAP reboots after the upgrade completes successfully.

Performing a TFTP Transfer Via a Web Browser Session

1. Start the TFTP server.
2. From the Universal Access Point Configuration Web page, choose either the Upgrade Root UAP command or the Software Download command, depending upon the firmware currently on your UAP. For help accessing the Web page, see “Using a Web Browser” in Chapter 6. The following screen appears:



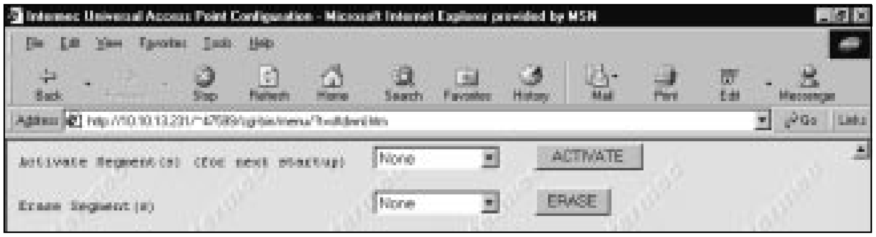
Universal Access Point Configuration

[Up to higher level menu] [TFTP Client] [TFTP Server] [Automated Software Download] [Help] [Logout] [Reboot]

File System Directory

```
Segment Allocation Table (4):
      First  Last                                     Start     Stop
  Seg Sector Sector Status   Size    Free    Address   Address
  --- ------ ------ -------- ------- ------- --------- ---------
   1    5     15    Valid   0720896 0076852 02840000 028f0000
   2   16     26    Valid   0720896 0078484 028f0000 029a0000
   3   27     29    Valid   0196608 0060296 029a0000 029d0000
   4   30     32    Valid   0196608 0196608 029d0000 02a00000

      Startup File: UAP.PRG
   Startup Address: 2840020
   Startup Segment: This startup = 1,  Next startup = 1
      Data Segment: This startup = 3,  Next startup = 3
```

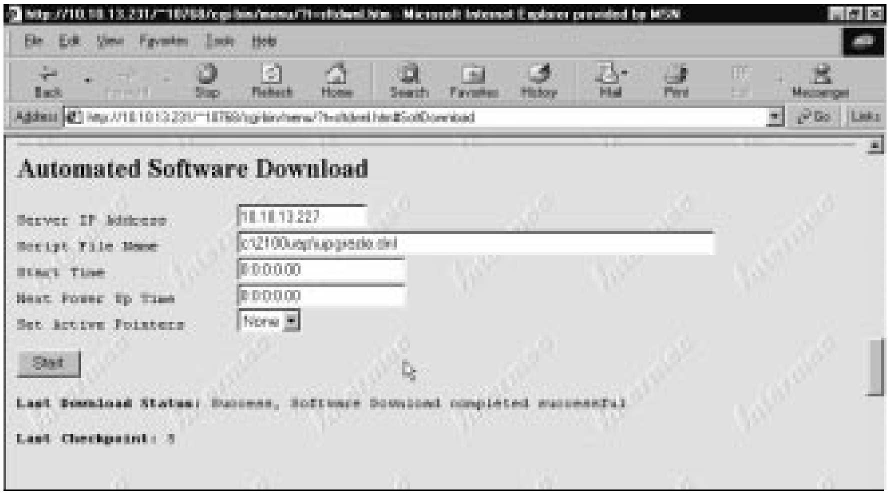
3. Scroll down to the Erase Segments drop-down list box.


Intermec Universal Access Point Configuration - Microsoft Internet Explorer provided by MSN
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Messenger
Address
Go Links
ACTIVATE
ERASE

Activate Segment(s) (for next startup) None

Erase Segment(s) None

4. Select All Inactive.
5. Click the Erase button.
6. Scroll down to the Automated Software Download section.


Microsoft Internet Explorer provided by MSN
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Messenger
Address
Go Links
Start

Automated Software Download

Server IP Address 10.10.13.227
Script File Name c:\2100uap\upgrade.dnl
Start Time 0:0:0:0.00
Next Power Up Time 0:0:0:0.00
Set Active Pointers None

Last Download Status: Success, Software Download completed successful

Last Checkpoint: 5

7. In the Server IP Address field, enter the IP address of the TFTP server where the script file is located. For example, if the server IP address is 151.60.110.241, type:

   `151.60.110.241`

8. In the Script File Name field, enter the directory path to the script file. Type:

   `c:\2100uap\upgrade.dnl`

9. In the Start Time field, you must enter a time for the download to begin. Start time is a countdown timer—when the timer expires, the download begins. You can enter days, hours, minutes, seconds, and partial seconds in the Start Time field. For example, to start the download two hours and ten minutes from now, type:

   `0:2:10:0.00`

10. In the Next Power Up Time field, you must enter a time when the UAP is to reboot. Next power up time is a countdown timer—when the timer expires, the UAP reboots. You can enter days, hours, minutes, seconds, and partial seconds in the Next Power Up Time field. For instance, to reboot the UAP three hours from now, type:

    ```
    0:3:0:0.00.
    ```

    Be sure you allow enough time for the download to complete before the UAP reboots. Intermec recommends that you allow at least ten minutes for the download to complete.

11. In the Set Active Pointers list box, select Both.
12. Click Start.

Upgrading Other UAPs

After you have upgraded the root UAP with UAP code version 3.49 or greater, you can upgrade the other UAPs on the network through a Web browser. For information on establishing a Web browser session with the UAP, see Chapter 6, “Managing the UAP Remotely.” From the Universal Access Point Configuration Web page, you can select the Upgrade Other UAPs command to upgrade the remaining UAPs on the network.

Note: You MUST access the Upgrade Other UAPs function through a browser session with the root UAP to perform this firmware upgrade.

When you use the Upgrade Other UAPs command on the root UAP, the screen displays all 21XX and 6710 access points on the network that have the same LAN ID as the root. The screen also displays the current firmware version of each UAP.

Note: Although the Upgrade Other UAPs screen displays 6710 access points on the network, you can only upgrade 21XX devices using this feature. Also, to upgrade a 21XX that is on a secondary LAN, the UAP must have the same default IP router as the root UAP on the primary LAN.

From the Upgrade Other UAPs screen you can

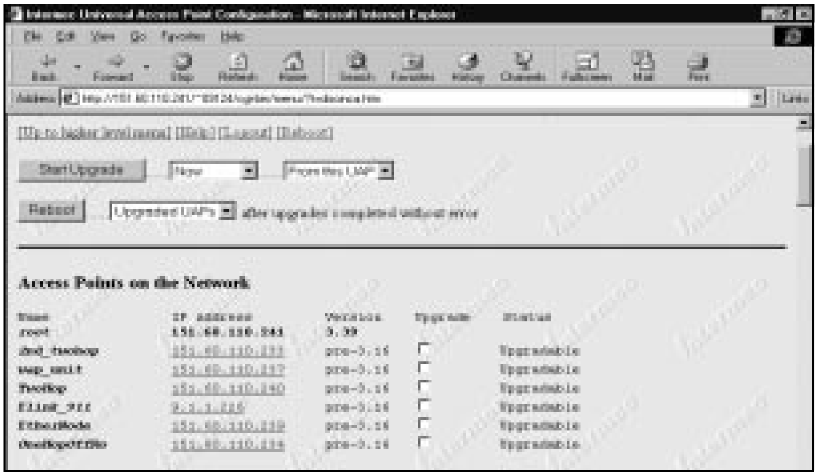
- select the UAPs to upgrade.
- select the source of the upgrade (either the active or inactive segments on the root UAP).
- set the time the upgrade is to begin.
- specify whether to reboot all UAPs or only the upgraded UAPs when the upgrade completes.

When you upgrade multiple UAPs using this feature, one UAP is upgraded at a time during the upgrade process. The amount of time required for the entire upgrade depends upon the number of access points in your network. Each UAP requires at least three or four minutes to upgrade; a two-hop WAP may require up to ten minutes to upgrade. The browser screen automatically refreshes every 30 seconds so you can monitor the progress.

After the UAPs are upgraded, the reboot process requires several additional minutes for the UAPs to boot. If you choose to reboot all UAPs, you must sign in to a new Web browser session after the UAPs boot.

To upgrade other UAPs

1. From the Universal Access Point Configuration Web page on the root UAP, choose the Upgrade Other UAPs command. The following screen appears:


Intermec Universal Access Point Configuration - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address
Links
[Up to higher level menu] [Help] [Logout] [Reboot]
Start Upgrade
Now
From this UAP
Reboot
Upgraded UAPs

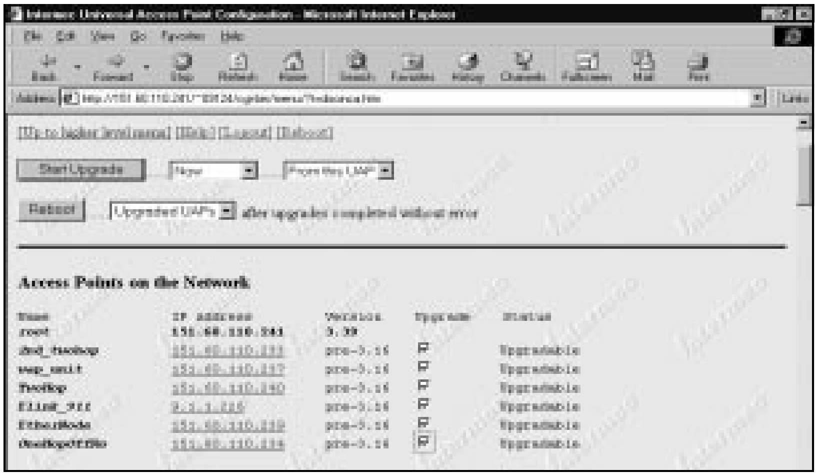
after upgrade is completed without error

Access Points on the Network

Name	IP address	Version	Upgrade	Status
root	151.60.110.241	3.39		
2nd_twohop	151.60.110.233	pre-3.16	□	Upgradable
wap_unit	151.60.110.237	pre-3.16	□	Upgradable
TwoHop	151.60.110.240	pre-3.16	□	Upgradable
Flink_???	9.1.1.216	pre-3.16	□	Upgradable
EtherMode	151.60.110.239	pre-3.16	□	Upgradable
OneHopOffHo	151.60.110.234	pre-3.16	□	Upgradable

2. In the Start Upgrade time drop-down list box, select the start time. You can start the upgrade now or from one to 12 hours from now.
3. In the Start Upgrade source list box, select the source of the upgrade.
   - The “From this UAP” option uses the firmware that is currently in the active boot and data segments in this UAP.
   - The “From backup” option loads the firmware that is currently in the inactive boot and data segments in this UAP.
4. In the Reboot list box, select the UAPs to reboot when the upgrade completes.
   - The “Upgraded UAPs” option boots only those UAPs that were upgraded.
   - The “All UAPs” option boots all UAPs on the network.

5. Select the access points to upgrade.



Intermec Universal Access Point Configuration - Microsoft Internet Explorer

File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address
Links

[Up to higher level menu] [Help] [Logout] [Reboot]

Start Upgrade | Now | From this UAP

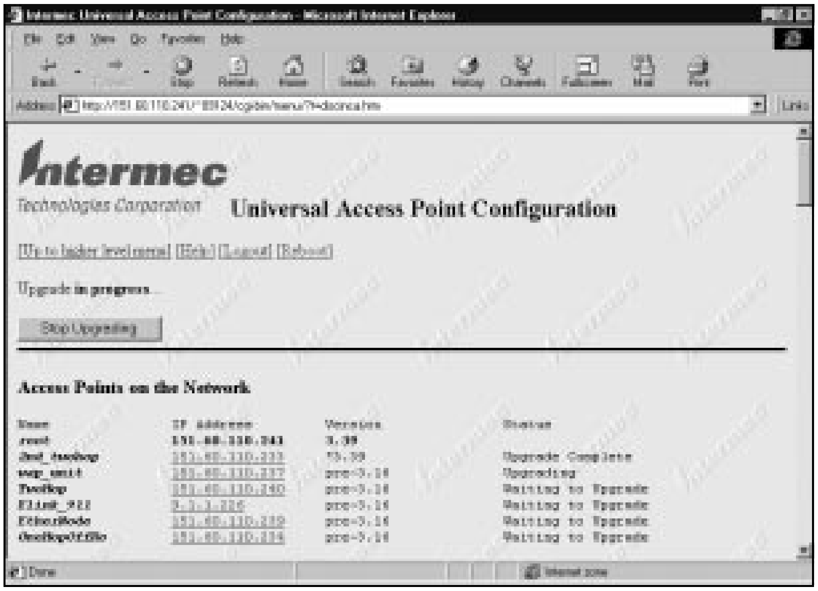
Reboot | Upgraded UAPs | after upgrades completed without error

Access Points on the Network

```
Name            IP Address        Version    Upgrade   Status
root            151.60.110.241    3.39
2nd_twohop      151.60.110.233    pre-3.16   ☑         Upgradable
uap_unit        151.60.110.237    pre-3.16   ☑         Upgradable
TwoHop          151.60.110.240    pre-3.16   ☑         Upgradable
Flink_911       9.1.1.226         pre-3.16   ☑         Upgradable
EtherNode       151.60.110.239    pre-3.16   ☑         Upgradable
OneHopOffNo     151.60.110.234    pre-3.16   ☑         Upgradable
```

6. Click the Start Upgrade button. The upgrade begins at the time you specified in Step 2.

   The screen automatically refreshes during the upgrade so you can monitor the progress. The following screen shows the UAPs during the upgrade process.



Intermec Universal Access Point Configuration - Microsoft Internet Explorer

File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address
Links
Intermec
Technologies Corporation
Done
Internet zone

Universal Access Point Configuration

[Up to higher level menu] [Help] [Logout] [Reboot]

Upgrade **in progress**...

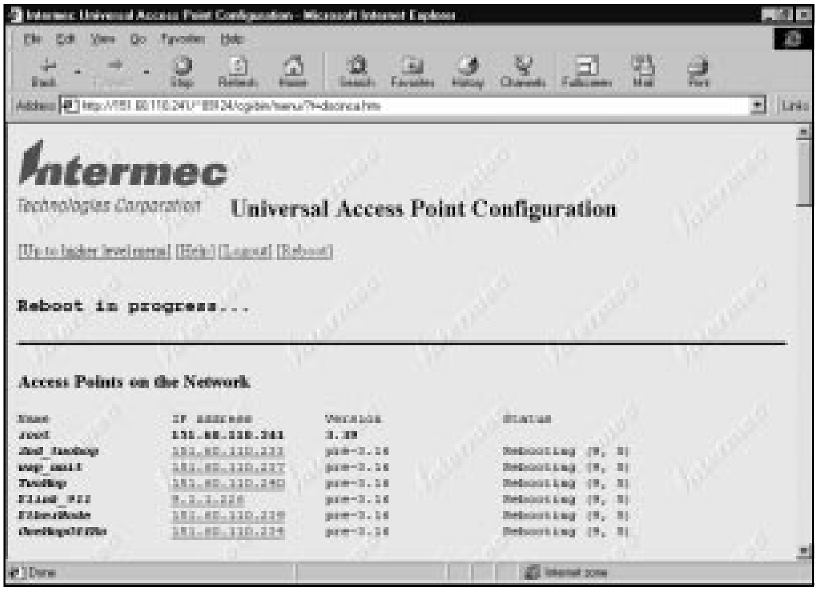
Stop Upgrading

Access Points on the Network

```
Name            IP Address        Version    Status
root            151.60.110.241    3.39
2nd_twohop      151.60.110.233    *3.39      Upgrade Complete
uap_unit        151.60.110.237    pre-3.16   Upgrading
TwoHop          151.60.110.240    pre-3.16   Waiting to Upgrade
Flink_911       9.1.1.226         pre-3.16   Waiting to Upgrade
EtherNode       151.60.110.239    pre-3.16   Waiting to Upgrade
OneHopOffNo     151.60.110.234    pre-3.16   Waiting to Upgrade
```

When the upgrade completes successfully, the UAPs that you specified in Step 4 automatically reboot.

The following screen shows the reboot in process. Note that the status of each UAP is (9, 5), which indicates that the UAP is rebooting and that the UAP completed the upgrade process. The error and status codes and their meanings are listed on the screen in the “Access Points on the Network Help” section.


Intermec Universal Access Point Configuration - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address http://151.60.110.241/~89124/cgi-bin/menu/?t=discinca.htm
Links
Intermec Technologies Corporation
Done
Internet zone

Universal Access Point Configuration

[Up to higher level menu] [Help] [Logout] [Reboot]

Reboot in progress...

Access Points on the Network

Name	IP address	Version	Status
root	151.60.110.241	3.38	
2nd_[illegible]	151.60.110.233	pre-3.16	Rebooting (9, 5)
[illegible]	151.60.110.237	pre-3.16	Rebooting (9, 5)
[illegible]	151.60.110.240	pre-3.16	Rebooting (9, 5)
[illegible]	9.1.1.226	pre-3.16	Rebooting (9, 5)
[illegible]	151.60.110.228	pre-3.16	Rebooting (9, 5)
[illegible]	151.60.110.234	pre-3.16	Rebooting (9, 5)

If a UAP does not upgrade successfully on the first try, select the UAP and start the upgrade again.

If an error occurs during the upgrade process, you must click Reboot to boot the UAPs that upgraded successfully.

G

Glossary

access point

A device that bridges frames between a wired network medium such as Ethernet to a wireless or RF network medium. An access point can also serve as a bridge between two RF networks. Access point in this manual specifically refers to the 21XX Universal Access Point.

ARP (Address Resolution Protocol)

The protocol used by TCP/IP networks to relate IP addresses with the physical network addresses of network interfaces.

BFSK (Binary Frequency Shift Key)

A broadcasting method that lengthens the range but halves the throughput as compared to the QFSK method. In UAPs using an OpenAir radio, the radio can be configured so that it automatically switches to this method when the RF protocol determines that throughput is degrading due to range. The transmit mode parameter determines if BFSK will be used. The default setting for transmit mode is AUTO, which allows this automatic switching to occur.

bridge

A device that expands a local area network by forwarding frames between data link layers associated with two separate physical media types, usually carrying a common protocol. A bridge connects wireless devices to a wired network 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.

channel

The path for transmitting data from a device to the host computer. A port may contain one or more logical channels. In 2.4 GHz RF networks, the channel refers to the frequency hopping sequence the radio follows.

data link tunneling

A UAP encapsulates an Ethernet frame in an INCA data frame and forwards the frame to the next UAP on the path to the final destination. Data link tunneling is used to make mobility transparent to the underlying network, or to isolate the radio traffic from terminals on an Ethernet segment. Data link tunneling occurs automatically when Ethernet bridging is disabled on the root UAP. Ethernet bridging is automatically disabled on a secondary LAN if there is no designated bridge for the secondary LAN. A UAP that has Ethernet bridging disabled forwards a frame inbound on its Ethernet port using data link tunneling. The root UAP or a designated bridge for a secondary LAN uses data link tunneling to forward frames outbound to UAPs on the same Ethernet segment.

designated bridge

A UAP that is assigned the role of bridging frames destined for or received from a secondary LAN. A designated bridge, or secondary LAN bridge, connects a secondary LAN with the primary LAN. In the UAP, the secondary LAN bridge priority parameter determines if the UAP is a candidate to become the designated bridge.

DHCP (Dynamic Host Configuration Protocol)

An Internet standard stack protocol that allows dynamic distribution of IP address and other configuration information to IP hosts on a network. Implementation of the DHCP client in Intermec network devices simplifies installation because the devices automatically receive IP addresses from a DHCP server on the network.

distribution LAN

Any Ethernet LAN attached to UAPs that are bridging between the Ethernet LAN and the INCA radio network. At any given time, only one UAP in a distribution LAN provides access to the Ethernet LAN for a given node in the INCA domain.

DIX

A standardized Ethernet frame format developed by Digital Equipment Corporation, Intel Corporation, and Xerox. Another frame format is 802.3.

flooding

A frame is flooded when the destination location is unknown. The destination location of a multicast frame is never known. Unicast and multicast flooding parameters determine how a flooded frame is forwarded.

home IP subnet

The IP subnet that contains the wired primary LAN and any wireless extensions of the subnet.

inbound frames

Frames moving toward the primary LAN.

IGMP (Internet Group Management Protocol))

IGMP is a protocol that allows the UAP to have more than eight INCA/IP tunnels. IGMP allows a UAP to participate in an IP multicast group without any special router configuration.

INCA (Integrated Network Communications Architecture)

Intermec’s architecture for wireless LANs. INCA is based on the principles of openness and flexibility so that it can accommodate future networking needs. INCA blends network connectivity and wireless LANs into a complete, plug-and-play system.

INCA/IP

The INCA protocol that allows IP tunneling between compatible network components on either side of a router.

IP subnet

A single member of the collection of hardware networks that composes an IP network. Host addresses on a given subnet share an IP network number with hosts on all other subnets of the IP network. The local address is divided into subnet-number and host-number fields to indicate which subnet a host is on.

MAC address

There are 2 types of MAC addresses, unicast and broadcast. Unicast specifies a single Ethernet interface. Multicast specifies a group of Ethernet addresses. Broadcast is a variation of multicast in which a multicast is received by all interfaces.

MIB (Management Information Base)

This repository stores network traffic information that SNMP management programs collect. Your network administrator can use management software interacting with the MIB to obtain information about network activity. Contact your local Intermec representative to learn how to obtain a copy of the MIB for the UAP.

multicast address

A form of broadcast address through which copies of the frame are delivered to a subset of all possible destinations that have a common multicast address.

non-bridging secondary LAN

A secondary LAN that does not have a designated bridge. A non-bridging secondary LAN is used to interconnect UAPs without using wireless hops.

OSI model

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

outbound frames

Frames moving away from the primary LAN.

peer-to-peer network

A type of LAN whose workstations are capable of being both clients and servers.

point-to-point bridge

A wireless link that connects two wired Ethernet segments. Two UAPs can be used to provide a point-to-point bridge between two buildings so that wired and wireless devices in each building can communicate with devices in the other building.

primary bridging

Ethernet bridging on a root port. A UAP uses primary bridging to bridge frames to and from the Ethernet network on its root port. Note that primary bridging is not the same as bridging to the primary LAN.

primary LAN

The Ethernet LAN attached to the UAP that is acting as the INCA root. The primary LAN is typically the LAN on which the servers are located. Primary and secondary LANs are both distribution LANs.

QFSK (Quad Frequency Shift Key)

A broadcasting method that shortens the range but doubles the throughput as compared to the BFSK method. In UAPs using an OpenAir radio, the radio can automatically switch between QFSK and BFSK as needed if the transmit mode is set to AUTO.

remote subnet

An Ethernet segment other than the primary LAN. A remote subnet is a secondary LAN.

remote INCA/IP subnet

A secondary LAN attached to the INCA network through an INCA/IP tunnel.

root

The UAP with the highest root priority becomes the root of the network spanning tree. If the root becomes inactive, the remaining root candidates negotiate to determine which UAP becomes the new root. The root can be used to set system-wide flooding and RF parameters. The root is also the only node in the INCA network that can originate INCA/IP tunnels.

root port

The UAP port that provides the inbound connection to the spanning tree. The root port provides a link to a parent UAP. Note that a root UAP does not have a root port.

root subnet

The Ethernet segment to which the root UAP connects, also known as the primary LAN.

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

secondary bridging
Ethernet bridging on a non-root port. A UAP that is the designated bridge for a secondary LAN uses secondary bridging to bridge frames to and from the secondary LAN on a non-root Ethernet port.

secondary LAN
Any Ethernet LAN that is not the primary LAN. A single UAP functions as the designated bridge for a secondary LAN. The designated bridge attaches the secondary LAN to the INCA network through a radio link or an INCA/IP link. Primary and secondary LANs are both distribution LANs.

SNAP
A protocol extension typically used by Appletalk networks.

SNMP (Simple Network Management Protocol)
SNMP is a popular network management protocol in the TCP/IP and SPX/IPX protocol suite. SNMP allows TCP/IP and SPX/IPX sites to exchange configuration and status information. It uses management programs called “agents” to monitor network traffic. SNMP stores the information it collects in the Management Information Base (MIB). Your network administrator can use management software interacting with the MIB to obtain information about network activity.

spanning tree
A form of network organization in which each device on the network has only one path to the root. The UAPs automatically configure into a self-organized network that provides efficient, loop-free forwarding of frames through the network.

subnet
A single member of the collection of hardware networks that compose an IP network. Host addresses on a given subnet share an IP network number with hosts on all other subnets of that IP network.

triangular routing
The routing logic used for a mobile IP end device that has roamed to a foreign network. Frames destined for a mobile end device are always sent to the home subnet of the end device. If the end device has roamed to another subnet, the frame must be forwarded to the remote subnet where the end device currently resides.

UAP

The 21XX Universal Access Point developed by Intermec Technologies Corporation. The UAP features Radio Independent and Network Independent architecture. The UAP bridges frames between a wired Ethernet network and a wireless RF network. The UAP can also serve as a bridge between two RF networks. In this manual, the term UAP is used as a general term that includes both the 2100 Universal Access Point and the 2101 Universal Office Access Point, unless specifically stated otherwise.

unicast address

A unique Ethernet address assigned to a single device on the network.

WAP

A wireless network device that serves as a repeater. It transmits data between a UAP that is connected to the Ethernet network and end devices.

WEP

Wired Equivalent Privacy, a feature that can be enabled in some IEEE 802.11 DS radios that allows data encryption for wireless communications.

wireless bridging

A wireless link that connects two wired Ethernet segments. Two UAPs can be used to provide a point-to-point or wireless bridge between two buildings, so that wired and wireless devices in each building can communicate with devices in the other building.

I

Index