Technical Reference Manual

P/N 067150-007

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: 1-800-668-7043
Canadian media supplies ordering information: 1-800-268-6936

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

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 S-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.
006	10/00	Revised to support additional features of firmware v1.4 including the IEEE 802.11b High Rate radio, WEP 128, IDRS, and the addition of the Web User Name parameter.
007	02/01	Reorganized and revised to support additional features of firmware 1.50. These features include using the access point as a DHCP server, improved access control, and internet software download support.

Contents

3 Managing the 21XX Remotely

4 Configuring the Radios

5 Configuring Filters and Tunnels

6 Troubleshooting and Maintaining the 21XX UAP

7 Advanced Features

A

Specifications

B

Understanding IP

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 1-800-668-7043. 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.

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, the 2101, and the 2102 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; 5,960,344; 5,696,903; 5,740,366; 5,790,536; 5,862,171; 5,940,771.

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

Getting Started

The chapter introduces and explains the 2100, 2101, and 2102 access points.

Understanding the 21XX Universal Access Point

The Intermec 21XX Universal Access Point™ (UAP) family consists of the following high-performance, wireless local area network (LAN) access points:

- 2100 Industrial Access Point
- 2101 Access Point
- 2102 Corporate Access Point

Each UAP is designed to be powerful and easy to use, and each 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 and is often used to provide wireless communications in locations where running cable is difficult, such as across roads or between buildings.

The UAP can also be configured as a repeater or wireless access point (WAP). A WAP does not require an Ethernet connection; it receives data from end devices and forwards it to an access point. A WAP is useful in areas that do not support a wired network connection.

Note: This manual supports the 1.50 Enterprise software for the 21XX access point.

The 2100 UAP

The 2100 access point accommodates dual radios and is a transparent bridge that enables your wireless end devices to communicate with devices on your wired network. The 2100 features a sealed case that meets IP 54 standards for protection from wind and dust and is designed for harsh indoor or outdoor environments. An integrated heater option is available for use in environments that experience temperatures below -25°C (-13°F).

You can configure the 2100 as a

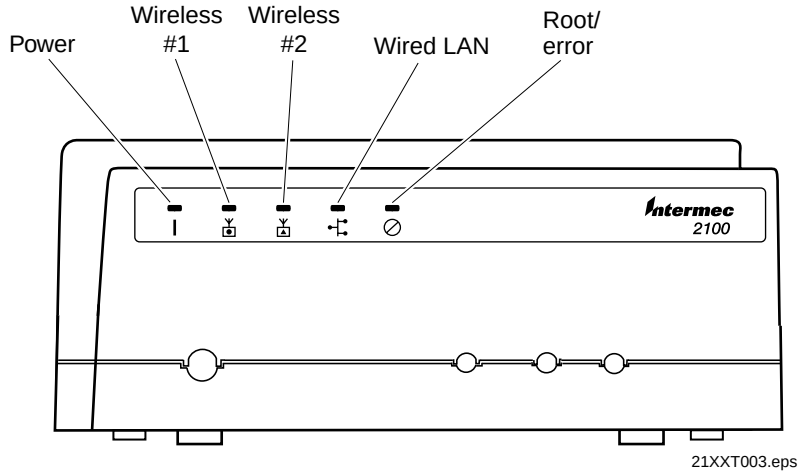
- standard access point.
- point-to-point bridge, which connects two wired networks, such as between buildings.
- repeater or WAP, which extends the range of your wireless devices.

The 2100 ships with these items:

- Power cord
- Safety information

Understanding the 2100 LEDs

The following illustration identifies the five LEDs on the 2100.

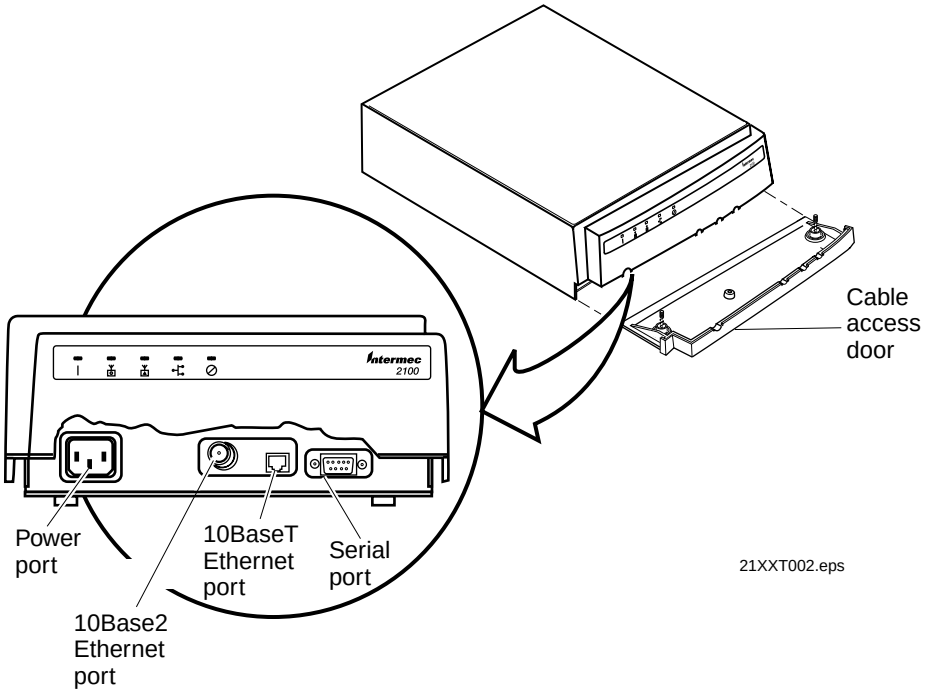


The following table describes the LEDs on the 2100.

LED	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 radio slot 1.
Wireless #2	Flashes when a frame is transmitted or received on the radio port for the radio installed in radio slot 2 (if a second radio is installed).
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. May also remain on if an error is detected.

Understanding the 2100 Ports

The following illustration identifies the ports on the 2100.



The following table describes the ports on the 2100.

Port	Description
Power port	Used with an appropriate power cable, the power port connects the access point to an AC power source.
Serial port	Used with a null-modem cable, the serial port connects the access point to a terminal or PC to perform initial configuration.
10BaseT port	Used with an appropriate cable, the 10BaseT port connects the access point to your Ethernet network.
10Base2 port	Used with an appropriate cable, the 10Base2 port connects the 2100 to your Ethernet network.

To access the ports 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 the door off.

The 2101 UAP

The 2101 access point accommodates dual radios and is a general-purpose access point suitable for use in most environments. You can configure the 2101 as a

- standard access point.
- WAP.
- point-to-point bridge.

The 2101 with an 802.11b HR radio installed is Wi-Fi™ certified for interoperability with other 802.11b HR wireless LAN devices.

The 2101 ships with these items:

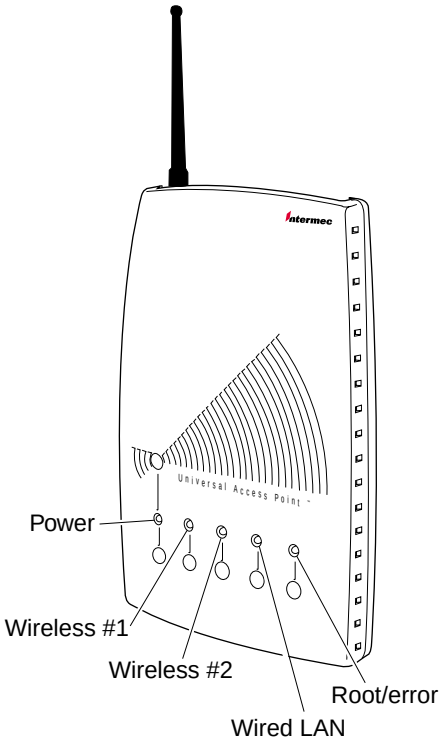
- Power supply (Part No. 3-304029-01) and AC power cord
- Antenna
- Mounting bracket
- Mounting screws (4)
- Safety information

Caution
You must use the appropriate Intermec power supply with these devices or equipment damage may occur.

Conseil
Vous devez utiliser la source d'alimentation Intermec adéquate avec cet appareil sinon vous risquez d'endommager l'équipement.

Understanding the 2101 LEDs

The following illustration identifies the five LEDs on the 2101.



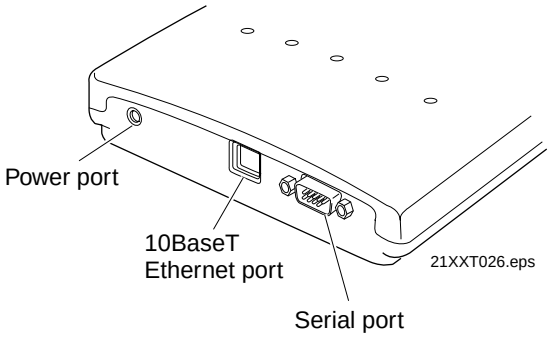
21XXT018.eps

The following table describes the LEDs on the 2101.

LED	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 radio slot 1.
Wireless #2	Flashes when a frame is transmitted or received on the radio port for the radio installed in radio slot 2 (if a second radio is installed).
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. May also remain on if an error is detected.

Understanding the 2101 Ports

The following illustration identifies the ports on the 2101.



The following table describes the ports on the 2101.

Port	Description
Power port	Used with an appropriate power cable, the power port connects the access point to an AC power source.
Serial port	Used with a null-modem cable, the serial port connects the access point to a terminal or PC to perform initial configuration.
10BaseT port	Used with an appropriate cable, the 10BaseT port connects the access point to your Ethernet network.

The 2102 UAP

The 2102 access point accommodates only one radio (either an 802.11b HR radio or a 2.4 GHz OpenAir radio) but has much of the same functionality as the 2100 and 2101. The 2102 is ideal for locations that do not require dual radios.

The 2102 can only be configured as a standard access point.

The 2102 with an 802.11b HR radio installed is Wi-Fi™ certified for interoperability with other 802.11b HR wireless LAN devices.

The 2102 ships with these items:

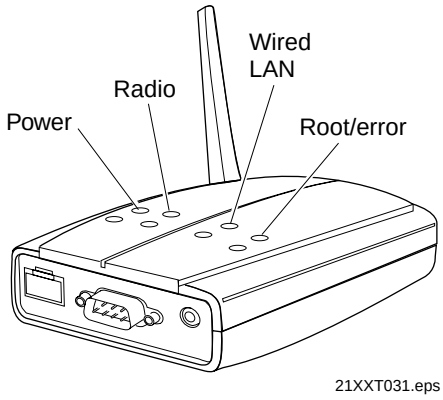
- Power supply (Part No. 3-304029-01) and AC power cord
- Mounting bracket
- Safety information
- Antenna

Caution
You must use the appropriate Intermec power supply with these devices or equipment damage may occur.

Conseil
Vous devez utiliser la source d'alimentation Intermec adéquate avec cet appareil sinon vous risquez d'endommager l'équipement.

Understanding the 2102 LEDs

The following illustration identifies the four LEDs on the 2102.

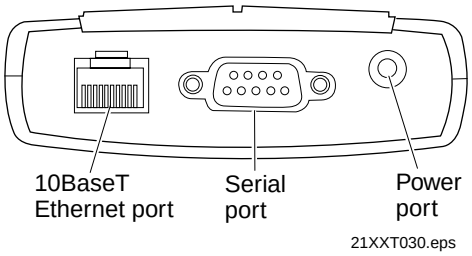


The following table describes the LEDs on the 2102.

LED	Description
Power	Remains on when power is applied.
Radio	Flashes when a frame is transmitted or received on the radio port.
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. May also remain on if an error is detected.

Understanding the 2102 Ports

The following illustration identifies the ports on the 2102.



The following table describes the ports on the 2102.

Port	Description
Power port	Used with an appropriate power cable, the power port connects the access point to an AC power source.
Serial port	Used with a null-modem cable, the serial port connects the access point to a terminal or PC to perform initial configuration.
10BaseT port	Used with an appropriate cable, the 10BaseT port connects the access point to your Ethernet network.

Configuring the 21XX UAP

Although the 21XX UAP will work directly out of the box, you must assign it an IP address and define other basic parameters before you can manage it remotely. To perform these initial configurations, you must use a serial connection and a terminal or a communications program (such as HyperTerminal). This manual assumes that you are using a communications program for your initial configuration and performing all other configurations remotely using the Web interface.

Configuring the 2100 UAP

To perform a basic configuration for the 2100 using the default settings, you need

- a power cable.
- an RS-232 null-modem cable. This 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.
- a terminal or PC with an open serial port.

If you are using the UAP as a UAP or a point-to-point bridge, you also need

- an Ethernet cable drop and cable.

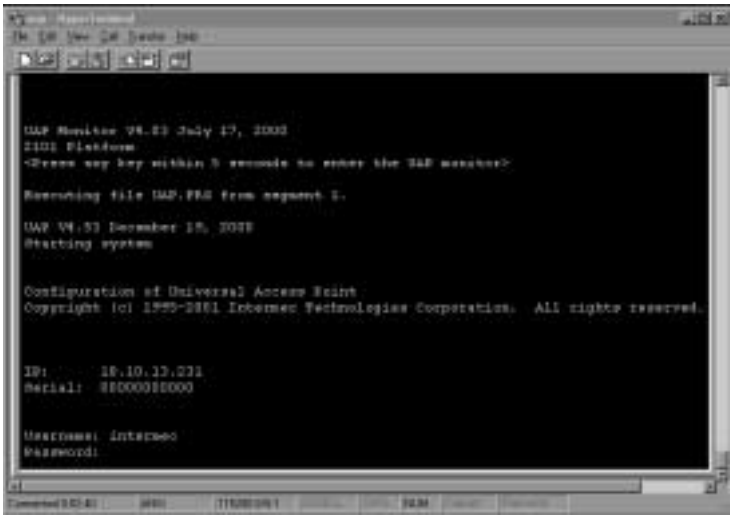
The following steps explain how to configure the basic parameters using a serial connection; however, you can use a remote connection to configure all the parameters shown here except those shown in Step 7.

To configure the 2100

1. Use the RS-232 null-modem cable to connect the serial port on the UAP to a serial port on your PC.
2. Open your communications program and configure the serial communications parameters on your PC to:

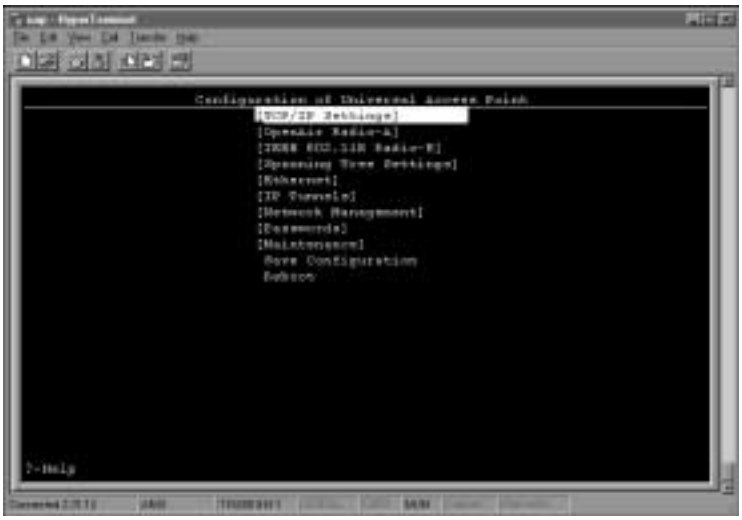
Baud	9600
Data bits	8
Parity	no
Stop bit	1
Flow control	no

3. Connect the power cable to the UAP and to a power source. The 2100 has no On/Off switch, so it boots as soon as you apply power.
4. Press **Enter** when the message "`Starting system`" appears on your PC screen. The login screen appears.



5. Type the default username `Intermec` and press **Enter**. The username is not case sensitive.

6. Type the default password `Intermec` and press **Enter**. The password is not case sensitive. The Configuration menu appears.



7. In the TCP/IP Settings menu, configure these parameters:

Parameter	Description
IP Address	A unique IP address.
IP Subnet Mask	The subnet mask that matches the other devices in your network.
IP Router (Gateway) if the UAP will communicate with devices on another subnetwork	The address of the router that will forward frames if the 2101 will communicate with devices on a subnetwork.

8. In the Spanning Tree Settings menu, configure LAN ID (Domain). For more information about the LAN ID (Domain), see "Configuring the LAN ID (Domain)" on page 3-12.
9. Configure the radio parameters.

   802.11b HR radios If you are using 802.11b HR radios, configure these parameters in the IEEE 802.11b Radio menu:

(SSID) Network Name	The network name. All 802.11b HR radios must have the same network name to communicate.
Frequency	The frequency appropriate for your installation. Frequencies range from 2.4 to 2.5 GHz and depend on the specific country.

2.4 GHz OpenAir radios If you are using OpenAir radios, first configure the LAN ID (Domain) in the Spanning Tree Settings menu. The LAN ID (Domain) is a number between 0 and 15. All OpenAir devices on the same network must have the same LAN ID to communicate.

After you have configured the LAN ID, configure these parameters in the OpenAir Radio menu:

Channel	A number from 1 to 15.
Subchannel	A number from 1 to 15.
Security ID	An identification up to 20 alphanumeric characters long. All OpenAir radios must have the same security ID to communicate.

Note: Intermec recommends that you set the Security ID parameter to a value other than null (the default value) to prevent unauthorized access to your network.

900 MHz radios If you are using 900 MHz radios, configure Mode-Channel in the 900 MHz Radio menu.

UHF radios If you are using UHF radios in the United States and you are required to transmit a call sign, configure Call Sign in the S-UHF Radio menu.

10. Save the configuration.
11. Disconnect the null-modem and power cables.

You are now ready to install the 2100 in your network. See page 2-11, “Installing the 2100 UAP.”

Configuring the 2101 or 2102 UAP

To perform a basic configuration of the 2101 or 2102 using the default settings, you need

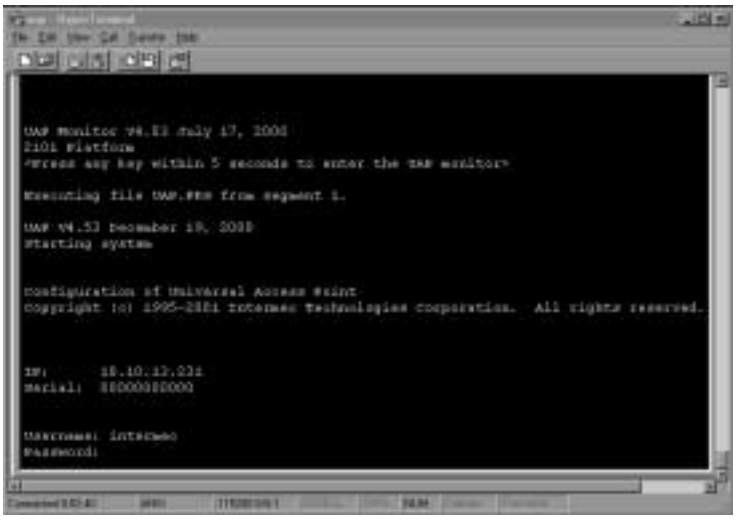
- an RS-232 null-modem cable.
- a terminal or PC with an open serial port.

To configure the 2101 or 2102

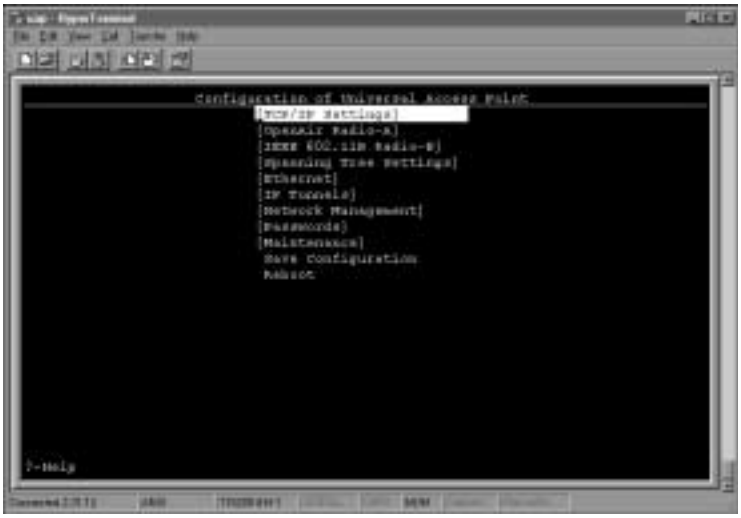
1. Use the RS-232 null-modem cable to connect the serial port on the UAP to a serial port on your PC.
2. Open your communications program and configure the serial communications parameters on your PC to:

Baud	9600
Data bits	8
Parity	no
Stop bit	1
Flow control	no

3. Connect the power cable to the UAP and to a power source. The UAPs have no On/Off switch, so each UAP boots as soon as you apply power.
4. Press **Enter** when the message "`Starting system`" appears on your PC screen. The login screen appears.



5. Type the default username `Intermec` and press **Enter**, and then type the default password `Intermec` and press **Enter**. The Configuration menu appears.



6. To use DHCP to automatically assign an IP address, configure the following parameters in the TCP/IP Settings menu:

DHCP Mode	Set to <Enabled, if IP Address is zero>.
DHCP Server Name	The name of the DHCP server that the 2102 is to access for automatic address assignment. If no server name is specified, the 2101 responds to offers from any server.

To assign an IP address manually, configure these parameters in the TCP/IP Settings menu:

IP Address	A unique IP address.
IP Subnet Mask	The subnet mask that matches the other devices in your network.
IP Router (Gateway)	The address of the router that will forward frames if the 2101 will communicate with devices on a subnetwork.

7. Configure the radio parameters.

802.11b HR radios If you are using 802.11b HR radios, configure these parameters in the IEEE 802.11b Radio menu:

(SSID) Network Name	The network name. All 802.11b HR radios must have the same network name to communicate.
Frequency	The frequency appropriate for your installation. Frequencies range from 2.4 to 2.5 GHz and are country-dependent.

2.4 GHz Open Air radios If you are using OpenAir radios, first configure the LAN ID (Domain) in the Spanning Tree Settings menu. The LAN ID (Domain) is a number between 0 and 15. All OpenAir devices on the same network must have the same LAN ID to communicate.

After you have configured the LAN ID, configure these parameters in the OpenAir Radio menu:

Channel	A number from 1 to 15.
Subchannel	A number from 1 to 15.
Security ID	An identification up to 20 alphanumeric characters long. All OpenAir radios must have the same security ID to communicate.

Note: Intermec recommends that you set the Security ID parameter to a value other than null (the default value) to prevent unauthorized access to your network.

If you are configuring a 2101, you must configure Node Type in the Wireless Bridging menu in the OpenAir Radio menu. Configure Node Type as Master if this radio will communicate with end devices; configure it as Station if you are configuring a WAP and this radio will communicate with a UAP on the wired network. For more information, see "Configuring Node Type" on page 4-15.

8. Save the configuration.
9. Disconnect the null-modem and power cables.

For optimal performance, you may need to set additional parameters. For more information, see Chapter 3, "Managing the 21XX Remotely."

You are now ready to install the 2101 or 2102 in your network. See "Installing the 2101 UAP" on page 2-12 or "Installing the 2102 UAP" on page 2-16.

2

Installing the 21XX UAP

This chapter explains how the 21XX functions in a network and how to install the 21XX UAP. This chapter also explains bridging and how to establish a Web browser session.

Using the 21XX UAP in a Wireless Network

In general, the 21XX UAP forwards data between end devices and the wired network. Use the 21XX in the following locations and environments.

2100 Use in locations where a UAP is exposed to extreme environments.

2101 Use in most environments.

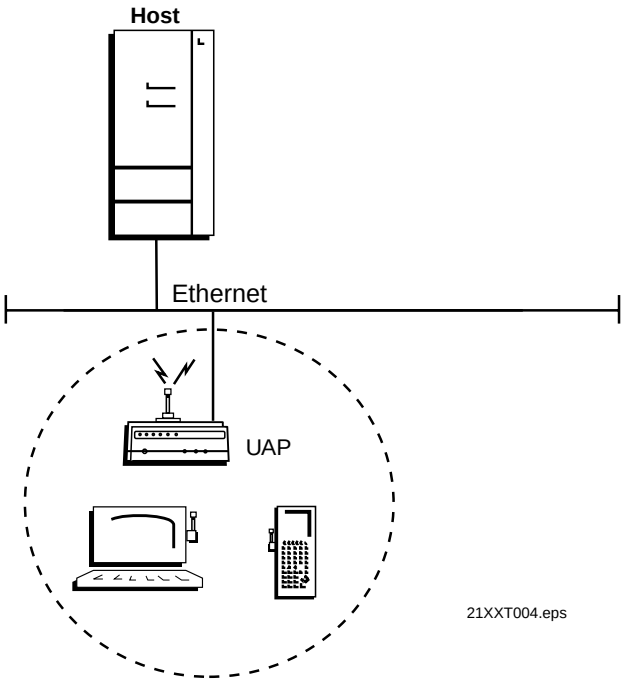
2102 Use when you do not need mixed radios or the 2102 is configured as a station at the remote end of a wireless hop to a secondary LAN.

The 21XX UAP supports a variety of network configurations. These configurations are explained in this section.

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 a network that functions as a wireless extension of the wired LAN.

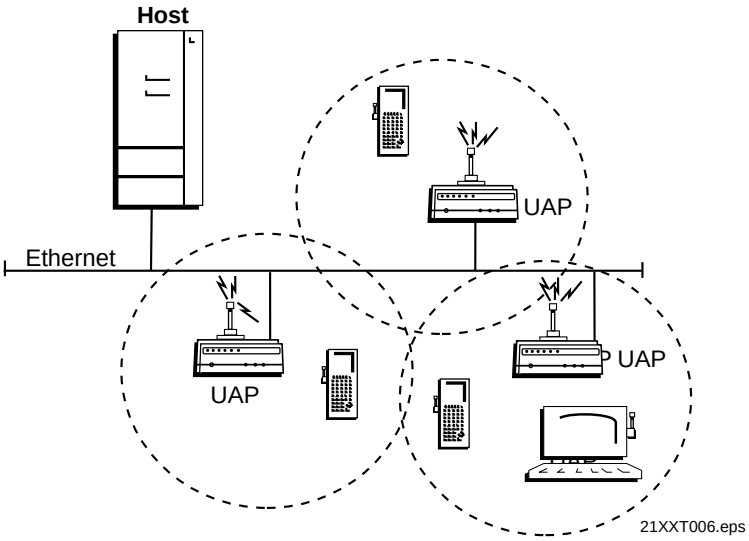
In a simple wireless network, a single UAP on the wired network serves as a transparent bridge between the wired network and end devices. The end devices communicate exclusively with devices on the wired network; they do not communicate with other end devices.



Using Multiple UAPs and Roaming End Devices

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



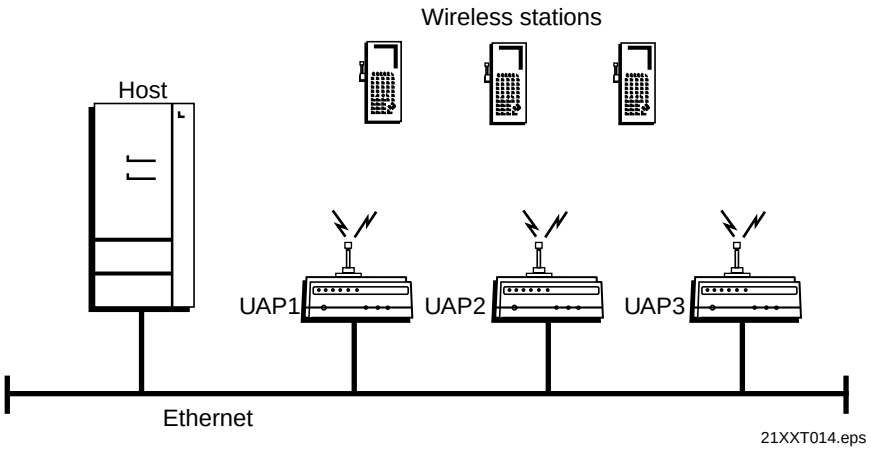
Using UAPs with Dual Radios for Redundancy

To provide redundancy for your network, you can use UAPs with two 802.11b HR radios or two 2.4 GHz OpenAir radios installed. Configure one radio as a master to communicate with end devices, which are stations by definition. The second radio in the UAP, configured as a station, provides backup transmission if the Ethernet network fails.

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

For more information about configuring wireless UAPs, see Chapter 4, “Configuring the Radios.”

Using UAPs with Dual Radios for Redundancy



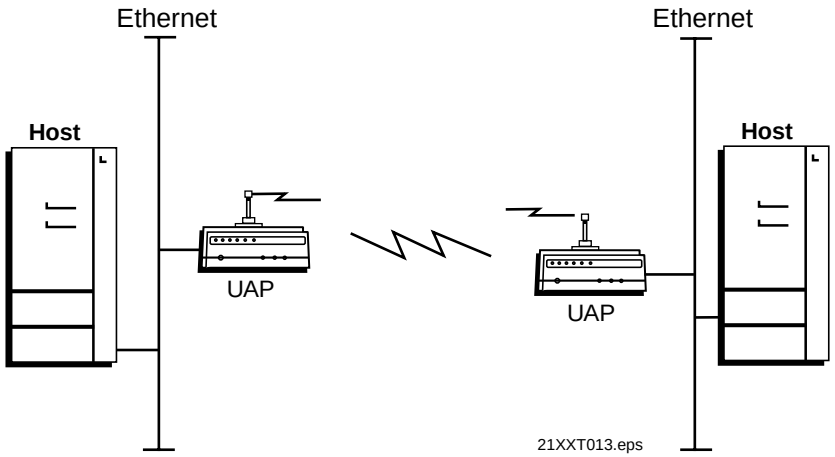
In the above example, UAP3 might be located on a loading dock or other remote location. It has dual radios for redundancy. During normal operations, UAP3 functions as a wired bridge, transmitting to and from the host on the Ethernet network. If the Ethernet connection is disrupted, however, UAP3 functions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

Note: In the above example, UAP2 must have the wireless hops parameter enabled, and UAP3 must be within range of UAP2. For information about configuring wireless hops, see Chapter 3, “Managing the 21XX Remotely.”

Using UAPs to Bridge Between Wired LANs

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 a campus environment where pavement or other objects prevent installation of a wired link. For information about configuring UAPs for point-to-point bridging, see Chapter 4, “Configuring the Radios.”

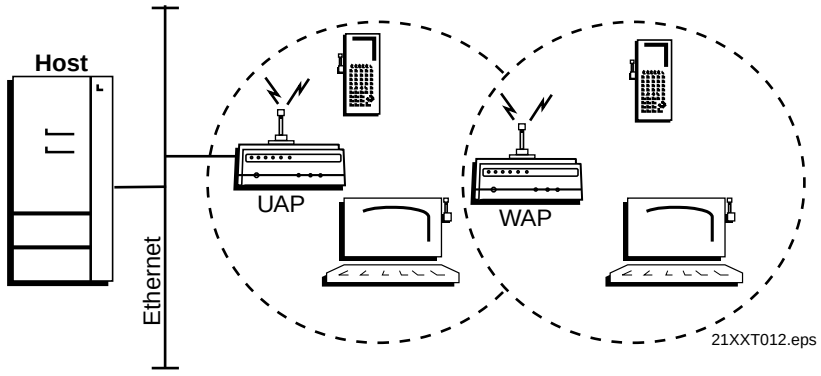
Using UAPs to Bridge Between Wired LANs



Note: You can configure UAPs for point-to-point bridging if the UAPs that form the bridge each have two 802.11b HR radios, two 2.4 GHz OpenAir radios, or one 900 MHz radio. Only one radio is required if there are no wireless terminals that need to connect in this area.

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 UAP (WAP) or repeater. You can position the WAP in a strategic location so 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 4, "Configuring the Radios."

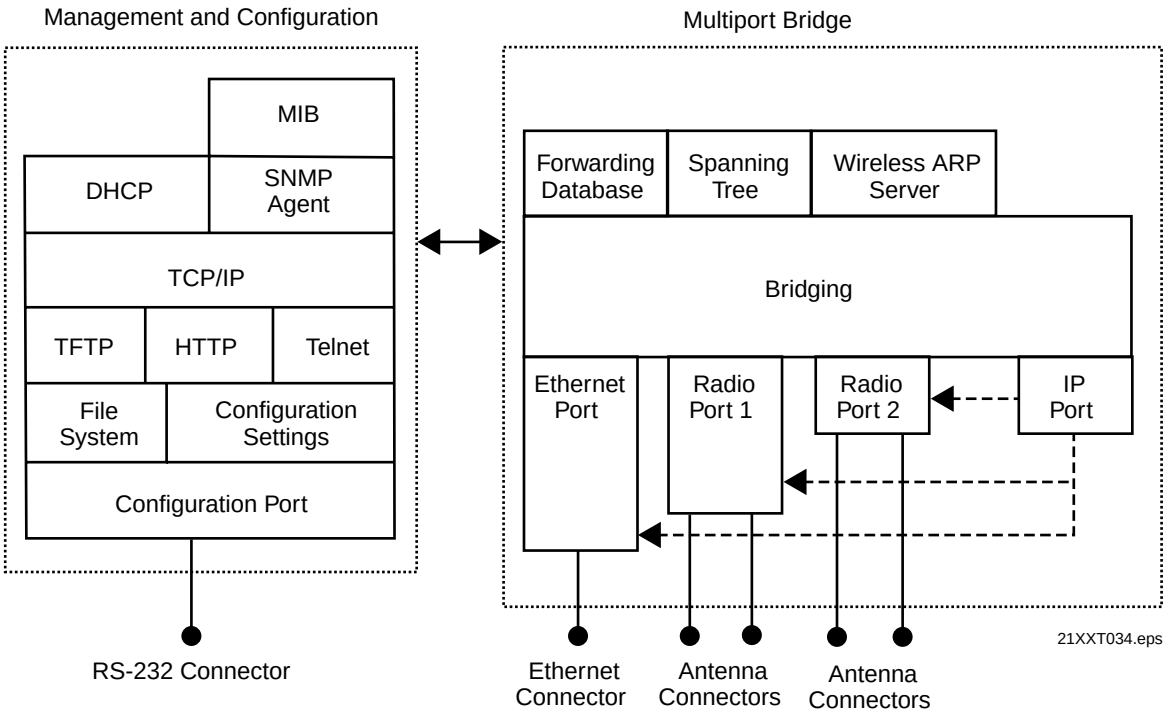


Note: You can configure the UAP as a repeater if it has two 802.11b HR radios, two 2.4 GHz OpenAir radios, or one 900 MHz radio.

Understanding Bridging and the UAP Ports

The UAPs consist of a group of multiport Ethernet-to-wireless bridges. The UAPs support IP for installations where wireless end devices roam across IP router subnets. Unlike the Ethernet and radio ports, the IP port does not have its own output connector. Instead, it is a logical port that provides Generic Router Encapsulation (GRE) for data that requires tunneling through routers. The IP port forwards encapsulated data through the Ethernet and radio ports as required to reach the intended end device.

The following illustration shows the general architecture of the 2100, 2101, and 2102.



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 explained in the next table.

Bridging Layer Functions Table

Function	Explanation
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 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. End devices can optionally participate in the 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 hands-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 leaning), by receiving explicit 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. For more information, see "Configuring Global Flooding" on page 3-17.
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.

Bridging Layer Functions Table (continued)

Function	Explanation
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. For more information, see Chapter 5, "Configuring Filters and Tunnels."

Configuring Ethernet Bridging

Ethernet bridging determines how wireless frames are converted to Ethernet frames and vice versa. With Ethernet bridging enabled, frames are forwarded directly to the Ethernet network. With Ethernet bridging disabled, data link tunneling occurs; that is, the UAP forwards frames on the Ethernet link encapsulated in data frames. Data link tunnels 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 set to Enabled on the root UAP even if you set it to Disabled.

To configure Ethernet bridging

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click Spanning Tree Settings. The Spanning Tree Settings screen appears.
3. Click the Ethernet Bridging down arrow and choose Enabled or Disabled. When you are finished, click Submit Changes to save your changes.

Configuring Secondary LAN Bridge Priority

A secondary Ethernet LAN can be bridging or non-bridging. A bridging secondary Ethernet LAN

- interconnects UAPs.
- provides a wireless connection for wired Ethernet hosts.
- has a UAP that is the designated bridge to the primary LAN.

A non-bridging secondary LAN interconnects UAPs but has no designated bridge.

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. The Secondary LAN bridging option only appears if you have a Secondary LAN Bridge Priority. If you have wired hosts on the secondary LAN, you must enable bridging to the secondary LAN.

You should enable bridging on a secondary LAN unless the inbound path is through an 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 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 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 zero prohibits the UAP from becoming the designated bridge. If all UAPs connected to a secondary LAN have a bridge priority of zero, then a non-bridging secondary LAN exists and bridging to the secondary LAN is automatically disabled.

Note: If a switch fails, the 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 the Secondary LAN Bridge Priority to zero in this case.

To configure secondary LAN bridge priority

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Spanning Tree Settings. The Spanning Tree Settings screen appears.
3. Set the Secondary LAN Bridge Priority parameter to a value greater than zero. When you are finished, click Submit Changes to save your changes.

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.
- Use an uninterruptible power supply when the AC power system is not reliable.

For information about antenna placement and accessories, see Appendix C, "Using External Antennas."

Decreasing Interference

Microwave ovens operate in the same frequency band as 802.11b HR and 2.4 GHz OpenAir radios; therefore, if you use a microwave within range of your Intermec RF network, you may notice network performance degradation. Both your microwave and your RF network will continue to function, but you may want to consider relocating your microwave out of range of your UAP.

The UAP features an advanced configuration parameter for the 802.11b HR radio called microwave oven robustness. You can enable this parameter to minimize potential interference between your microwave oven and your RF network.

Access points configured for the frequency in the same coverage area may interfere with each other and decrease throughput. You can reduce the chance of interference by configuring your UAPs so they are configured 5 channels apart, such as Channels 1, 6, and 11. For more information about microwave oven robustness, see "Configuring Advanced 802.11b Radio Parameters" on page 4-6.

If you have a 900 MHz or 2.4 GHz OpenAir radio in your UAP, the radio may experience interference from some cordless telephones. For optimal performance, consider operating 900 MHz and 2.4 GHz cordless telephones out of range of your UAP.

Installing the 21XX UAP

Follow these steps to install the UAP in your network.

1. Mount the UAP.
2. Attach the antenna(s).
3. Connect the UAP to the Ethernet network (unless you are using it as a wireless UAP) and power source.

Installing the 2100 UAP

The 2100 is designed to be placed horizontally or vertically on a desk or counter. You can also mount it vertically to a wall or beam using an optional Intermec mounting bracket specially designed for the 2100. You must mount the 2100 in either the horizontal or vertical position to maintain the IP 54 environmental rating.

Mounting the 2100

You can mount the 2100 to a wall or beam using an Intermec mounting bracket kit. Contact your Intermec representative to order one of these mounting kits:

- Mounting bracket kit (Part No. 068918)
- Rotating mounting bracket kit (Part No. 068751)

After the 2100 is mounted, it is ready to begin transmitting data packets between your end devices and your wired network.

Attaching an Antenna

A variety of external antenna options are available for the 2100 UAP. Contact your local Intermec representative for information about the various antenna options, including higher gain and directional antennas. The optional antennas ship with installation and mounting instructions. For more information about antennas, antenna accessories, and antenna placement, see Appendix C, "Using External Antennas."

Connecting the 2100

Unless you are using the UAP as a wireless UAP, you need to connect the UAP to your Ethernet network. You can use either a 10BaseT or 10Base2 Ethernet connector.

To connect the 2100

1. Attach one end of the 10BaseT (or 10Base2) cable to the appropriate port on the UAP, and attach the other end to your Ethernet network.
2. Plug one end of the power cord into the power port on the UAP, and plug the other end into an AC power outlet. The 2100 has no On/Off switch, so it boots as soon as you apply power.

Your 2100 is now ready to begin transmitting data packets between your end devices and your wired network.

Installing the 2101 UAP

You can install the 2101 horizontally on a desk or counter, or you can install it vertically to a wall using the wall bracket that ships with it. To mount the 2101 on a wall, follow the instructions that ship with the bracket and UAP.

Additional mounting options for the 2101 include a desk bracket that allows you to mount the 2101 upright on a desk or counter, and a cubicle bracket that allows you to mount the 2101 on a cubicle wall. A locking bracket is also available; use this bracket in conjunction with the wall bracket to secure the 2101 on a wall or ceiling.

These optional mounting brackets and accessories are available for the 2101:

- Desk bracket kit (Part No. 069657)
- Cubicle bracket kit (Part No. 069926)

- Locking bracket kit (Part No. 070184)
- Power supply holder kit (Part No. 069893)
- Dual antenna bracket kit (Part No. 069888)

For more information about mounting options, contact your Intermec representative.

Mounting the 2101

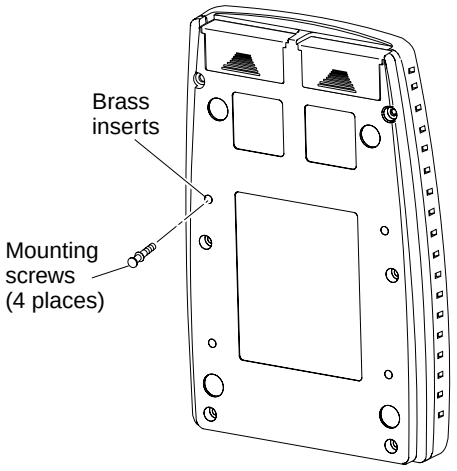
The 2101 ships with a mounting bracket and four mounting screws. The following instructions explain how to mount the UAP using the mounting bracket that ships with the 2101.

Install the mounting bracket and 2101 on a sturdy surface in accordance with local building codes. To install the bracket, you need these tools and materials:

- Drill and drill bit appropriate for the mounting screws
- Screwdriver

To mount the UAP vertically to a wall or beam

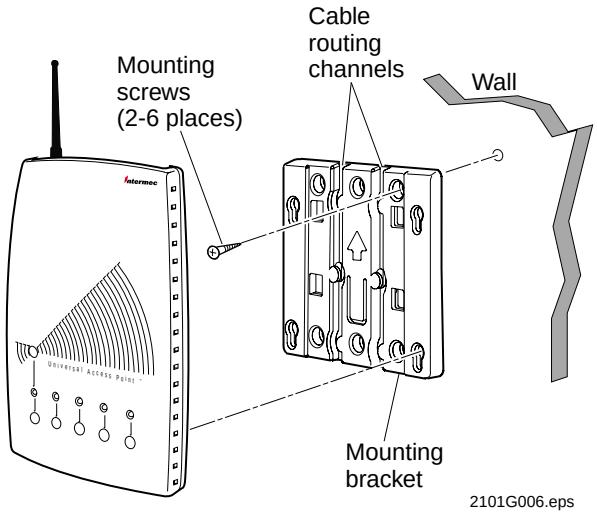
1. Insert one mounting screw into each of the threaded brass inserts on the back of the 2101 and tighten securely.



2101G004.eps

2. Use the mounting bracket as a template to mark the location of the mounting holes on the mounting surface.
3. Drill the mounting holes.

4. Position the bracket on the wall so the arrow points up.



5. Using the screws you provided, secure the bracket to the wall.
6. Route the power and Ethernet cables through the cable routing channels in the mounting bracket, if desired.
7. Mount the 2101 in the bracket by inserting the shoulder screws into the keyhole slots in the bracket. Slide the 2101 down until it is firmly seated in the bracket.

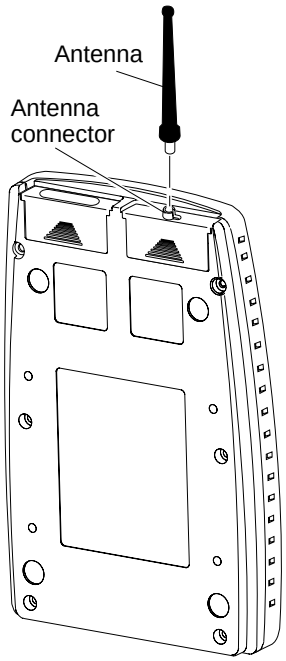
Attaching an Antenna

Intermec offers a variety of antennas and antenna accessories. For information about antenna options, contact your local Intermec representative. For the recommended antenna separation for UAPs with multiple antennas, see Appendix C, "Using External Antennas."

To attach an antenna to the 2101

1. Align the antenna with the antenna connector on the radio card in the 2101.

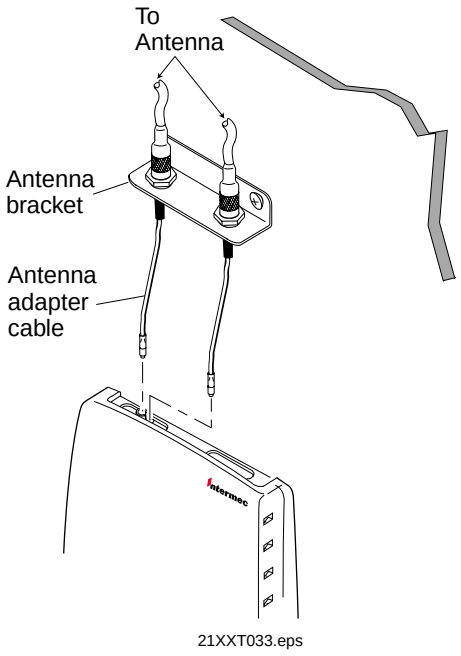
2. Insert the antenna into the antenna connector until you feel the antenna click into place.



2101G020.eps

The 802.11b HR radio features antenna diversity, which allows you to attach two antennas to a single radio. One antenna port sends and receives data, while the other antenna port only receives data. If you attach only one antenna to the 802.11b HR radio, you must attach it to the | (send/receive) port. The port is marked on the radio card. For more information about antenna diversity and the send/receive port, see Appendix C, “Using External Antennas.”

The following illustration shows how the optional dual antenna bracket kit (Part No. 069888) can be used to mount antennas or antenna cables to a wall.



Connecting the 2101

Unless you are using the UAP as a wireless UAP, you must connect the UAP to your Ethernet network using a 10BaseT Ethernet connector.

To connect the 2101

1. Attach one end of the 10BaseT cable to the 10BaseT port on the UAP, and attach the other end to your Ethernet network.
2. Plug one end of the power cord into the power port on the UAP, and plug the other end into an AC power outlet. The 2101 has no On/Off switch, so it boots as soon as you apply power.

Your 2101 is now ready to begin transmitting data packets between your end devices and your wired network.

Installing the 2102 UAP

You can install the 2102 horizontally on a desk or counter, or you can install it vertically to a wall using the wall bracket that ships with it. Follow the instructions that ship with the bracket and UAP. An optional cubicle bracket is also available for mounting the 2102 on a cubicle wall.

These optional mounting bracket kits and accessories are available for the 2102:

- Cubicle bracket kit (Part No. 070440)
- Power supply holder kit (Part No. 069893)
- Dual antenna bracket kit (Part No. 069888)

Contact your Intermec representative for more information about ordering UAP accessories.

Mounting the 2102

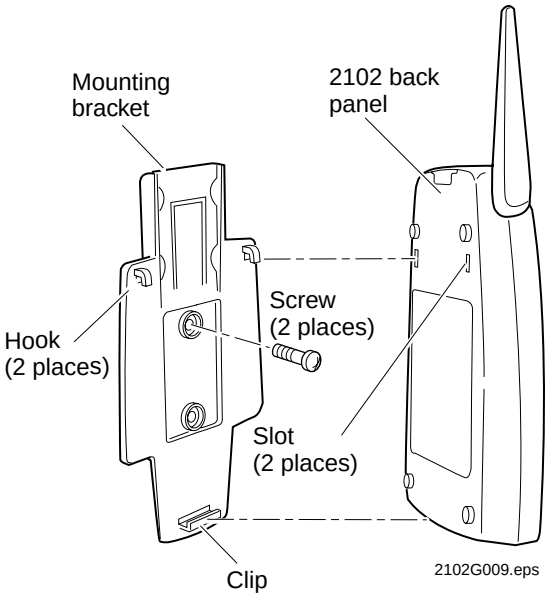
The following instructions explain how to mount the 2102 using the mounting bracket that ships with it.

Install the mounting bracket and 2102 on a sturdy surface in accordance with local building codes. You need the following tools and materials to install the bracket:

- Two #5 or M3 screws. The screws should be appropriate for the surface on which you are mounting the bracket.
- Drill and drill bit appropriate for the mounting screws
- Screwdriver

To mount the 2102

1. Use the mounting bracket as a template to mark the location of the mounting holes on the mounting surface.
2. Drill the mounting holes.
3. Position the bracket on the mounting surface.

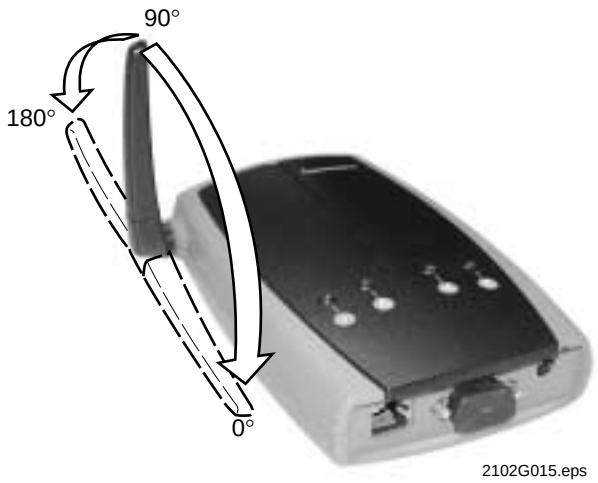


4. Using the screws you provided, secure the bracket to the wall.
5. Fit the slots on the back of the 2102 over the hooks on the mounting bracket.
6. Slide the 2102 up slightly, and then press the base of the 2102 until it clicks into the clip at the bottom of the mounting bracket.

Positioning the Antenna

The 2102 features a built-in antenna that rotates 180° as shown in the next illustration. Use the following guidelines when positioning the antenna.

- Place the antenna at 0° when storing the 2102.
- Place the antenna at 90° when using the 2102 horizontally; for instance, when the 2102 is positioned on a desk or counter.
- Place the antenna at 180° when using the 2102 vertically; for instance, when the 2102 is mounted on a wall or cubicle.



Note: Do not force the antenna past the hard stop at 0° or 180° or you may break the antenna connector.

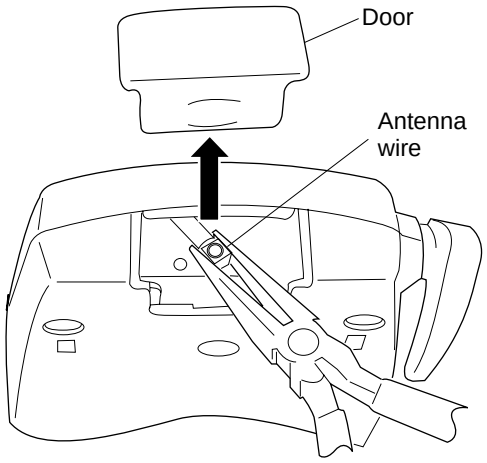
Attaching an External Antenna

You can attach an external antenna to the 2102. To attach an external antenna, you must disconnect the built-in antenna and attach an antenna cable directly to the radio card in the UAP. The following steps explain how to attach an antenna cable to the 2102.

For more information about antenna options, contact your local Intermec representative.

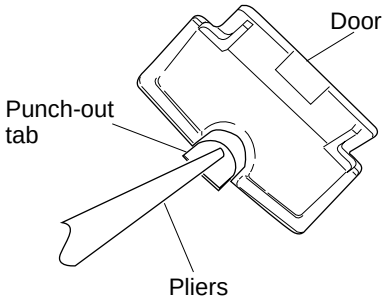
To attach an external antenna to the 2102

1. Remove the radio card door.
2. Pull straight up on the antenna wire to disconnect it from the radio card.



21XXT010.eps

3. Tuck the antenna wire inside the UAP housing.
4. Remove the punch-out tab from the door.



21XXT009.eps

5. Attach the antenna cable to the radio by inserting the cable connector into the radio card.
6. Replace the door.

For information about installing diversity antennas on the 802.11b HR radio, see Appendix C, “Using External Antennas.”

Connecting the 2102

Unless you are using the UAP as a wireless UAP, you must connect the UAP to your Ethernet network using a 10BaseT Ethernet connector.

To connect the 2102

1. Attach one end of the 10BaseT cable to the 10BaseT port on the UAP, and attach the other end to your Ethernet network.
2. Plug one end of the power cord into the power port on the UAP, and plug the other end into an AC power outlet. The 2102 has no On/Off switch, so it boots as soon as you apply power.

Your 2102 is now ready to begin transmitting data packets between your end devices and your wired network.

Establishing a Web Browser Session

After you have configured the IP address and other basic network parameters, you can access your UAP from a remote location.

Note: Although you can manage the device remotely using either a Telnet session or a Web browser, this manual assumes you are using a Web browser.

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.

To access the UAP remotely, you must first establish a Web browser session. When using the Web to establish remote access to your UAP, keep the following points in mind:

- Your session terminates if you do not use it for 15 minutes.
- Console Command mode is not available.

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

Note: If you access the Internet using a proxy server, you must add the IP address of the UAP to your Exceptions list. The Exceptions list contains the addresses that you do not want to use with a proxy server.

To establish a Web browser session with the UAP

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, and press **Enter**.
   - Choose Open from the File menu. In the Open field, enter the IP address of the UAP and press **Enter**.

   The Universal Access Point Login screen appears.

4. Type `Intermec` in both the Username and Password fields. You can change the user name and password after you have established your remote session. For help, see “Changing the User Name and Password” on page 3-3.
5. Click Login. The TCP/IP Settings screen appears.

The TCP/IP Settings Screen

Your Web browser session is established.

3

Managing the 21XX Remotely

This chapter explains how to configure and manage the 21XX remotely using a Web browser.

Configuring the 21XX Universal Access Point Parameters

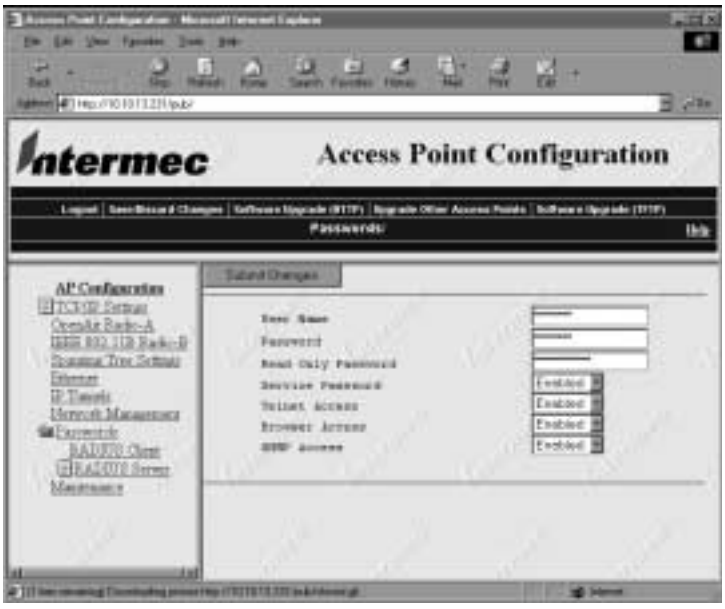
The UAP interface uses common menus to accomplish common tasks and does not make distinctions between specific UAPs except regarding the individual radio(s) installed. The following sections explain those common tasks.

Changing the User Name and Password

To ensure security to your UAP, you can make changes to your UAP security parameters after you establish a Web browser session.

To change the user name and password

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Passwords. The Passwords screen appears.



3. Type a user name in the User Name field and a password in the Password field. The User Name and Password can be 0 to 16 characters long. When you are finished, click Submit Changes to save your changes. The new user name and password are saved, and you must enter these new values each time you establish a Web session for this UAP.

This table explains the Password parameters.

Parameter	Description
Read Only Password	Gives read only access to the UAP. If you sign in with the read only password, you are able to view the configuration and execute diagnostics, but you cannot take any action that affects the operation of the access point such as changing configuration options, rebooting, or downloading software. Delete the password to disable it.
Service Password	Gives read only access to the UAP. For information on activating the UAP using the service password, see the next section, "Logging In Using the Service Password." To disable this password, click the Service Password down arrow and choose Disabled.
Telnet Access	Enables/disables the ability to Telnet to the access point.
Browser Access	Enables/disables the ability to Browse to the access point.
SNMP Access	Enables/disables SNMP access.

Understanding RADIUS Support

You can use RADIUS (Remote Authorization Dial-In User Services) to authorize configuration users. When you enter a user name and password when RADIUS is enabled, the User Name and Password is sent to a RADIUS server for authentication. If the server returns an access-accept packet, you are logged into the access point with read/write privileges.

If no RADIUS server is available when the RADIUS client is enabled, the RADIUS client times out on RADIUS access requests. In this case, because the Service password is checked after the read/write password, each failed Service Password login attempt may take up to eight seconds.

RADIUS Server

You can also configure the access point to act as a RADIUS server for itself and other access points. You can enter up to 70 username/passwords into the UAP RADIUS server database.

To configure the RADIUS server

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.

2. Click Passwords, and then click RADIUS Server. The RADIUS Server screen appears.

3. Click the Server down arrow and choose Enabled or Disabled. When you are finished, click Submit Changes to save your changes.
4. In the RADIUS Server you must enter in the secret key that is going to authenticate RADIUS clients.
5. In the RADIUS Server you must enter User Name and Password that are going to be used by the RADIUS Clients.

RADIUS Client

Use the RADIUS client to administer passwords for all access points at a central location (a RADIUS server). When you enable the RADIUS client, the normal passwords for the access point are disabled. The username and password information that you enter is sent to the RADIUS server; the RADIUS server then validates them and returns a response to the access point indicating whether or not the user should be logged in.

For example, when a user without access attempts to log in with the username “apusername” and the password “appassword,” the access point sends “apusername, appassword wants to log in” to the RADIUS server. The RADIUS server looks up “apusername, appassword” in its database and doesn't find it. The RADIUS server tells the access point not to let that user in, and the access point prompts the user for another username and password.

When a user with access attempts to log in with the username “apusername” and the password “appassword,” however, the access point sends “apusername, appassword wants to log in” to the RADIUS server. The RADIUS server looks up and finds “apusername, appassword” in its database and sends “let this user have access, they are approved” back to the access point. The access point then logs the user in.

To configure the RADIUS Client

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Passwords, and then click RADIUS Client. The RADIUS Client screen appears.

3. Set Configuration access to enabled.
4. Configure the Servers. There is a Primary Server (Server 1) and a Secondary Server (Server 2). The Primary server will always be sent the Authentication first. If the Primary Server is not on the network, the Authentication request will then go to the Secondary Server.

   You must enter in the IP Address of the server you want to authenticate with and you must enter in the Secret Key that is used by the Server.

Setting the Hello Period

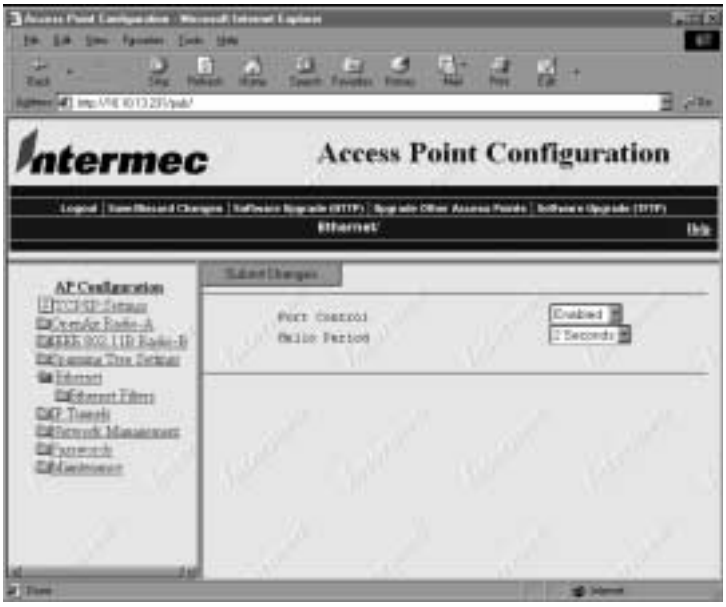
You can set the following types of Hello periods:

- Ethernet Hello Period, which describes how often Hellos are sent on the Ethernet.
- IP Tunnel Hello Period, which describes how often Hellos are sent through the tunnel.
- Radio Hello Period, which describes how often Hellos are sent out the radio when a wireless hop is formed.

The following sections explain how to set each type of Hello period.

To set the Ethernet Hello Period

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Ethernet. The Ethernet screen appears.

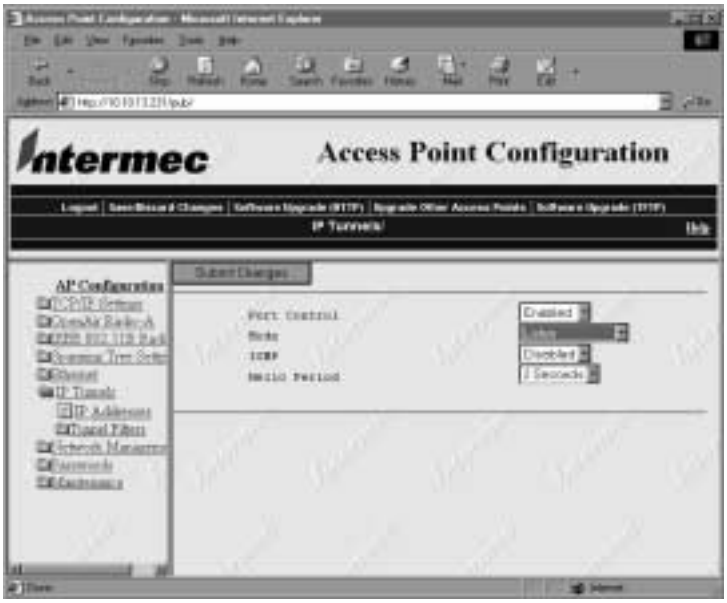


3. Click the Hello Period down arrow, and choose a hello period. When you are finished, click Submit Changes to save your changes.

To configure the IP Tunnel Hello period

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IP Tunnels. The IP Tunnels screen appears.

The IP Tunnels Screen

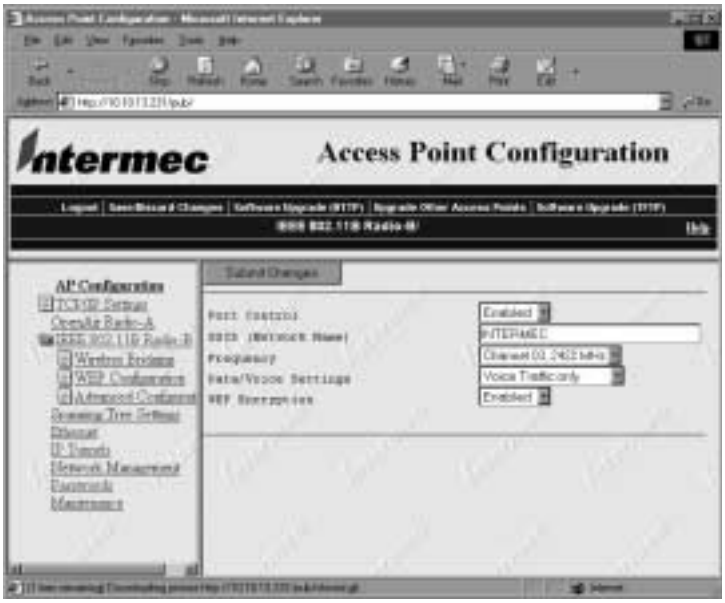


3. Click the Hello Period down arrow, and choose a hello period. When you are finished, click Submit Changes to save your changes.

To configure the 802.11b HR radio Hello period

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears.

The IEEE 802.11b Radio Screen

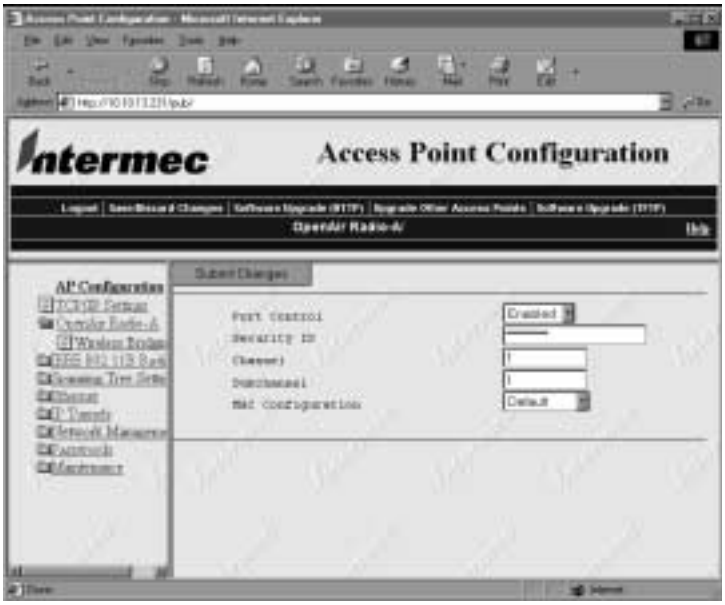


3. Click Wireless Bridging. The Wireless Bridging screen appears.

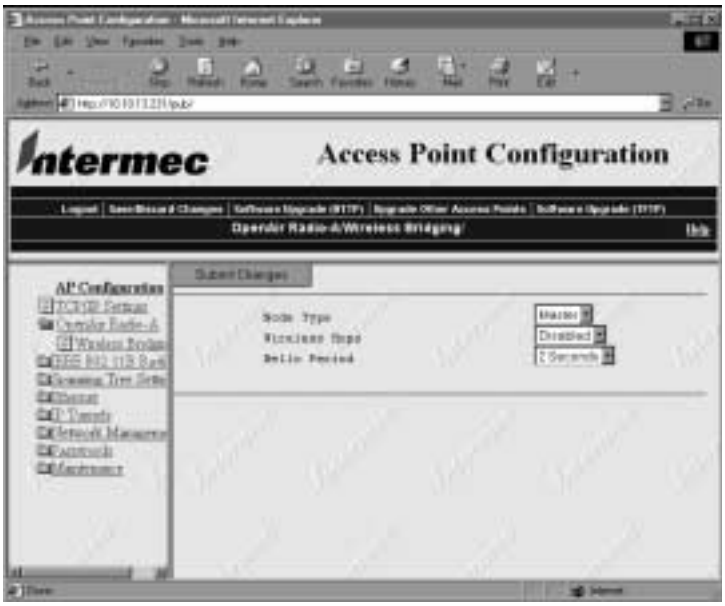
4. Click the Hello Period down arrow, and choose a hello period. When you are finished, click Submit Changes to save your changes.

To configure the OpenAir radio Hello period

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click OpenAir Radio. The OpenAir Radio screen appears.



3. Click Wireless Bridging. The Wireless Bridging screen appears.



4. Click the Hello Period down arrow, and choose a hello period. When you are finished, click Submit Changes to save your changes.

Configuring Ethernet or IP Tunnel Port Control

This section explains how to enable and disable port control for the Ethernet network and for IP Tunnels. For information about configuring port control for a specific radio, see Chapter 4, "Configuring the Radios."

To configure port control

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click Ethernet or IP Tunnels from the Configuration screen menu. The appropriate screen appears.
3. Click the Port Control down arrow and choose Enabled or Disabled. When you are finished, click Submit Changes to save your changes.

Setting 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.

To set ARP minutes

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click TCP/IP Settings. The TCP/IP Settings screen appears.
3. Type a time period in the Auto ARP Minutes field. The range is from 1 to 120 minutes. Set the time period to 0 to disable 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 would expire from the router ARP table. If the IP address expires, the network management program must 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.

Configuring the LAN ID (Domain)

All UAPs must have the same LAN ID or domain to participate in the same spanning tree. Additionally, all non-802.11b HR devices in a network must have the same LAN ID to be able to communicate.

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

To configure the LAN ID (Domain)

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Spanning Tree Settings. The Spanning Tree Settings screen appears.
3. Enter the LAN ID (Domain) in the LAN ID (Domain) field. The LAN ID (Domain) can be from 0 to 254. When you are finished, click Submit Changes to save your changes.

Setting Root Priority

The root priority determines whether a particular UAP is a candidate to become the root of the spanning tree. 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.

To set root priority

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Spanning Tree Settings. The Spanning Tree Settings screen appears.

The Spanning Tree Settings Screen

3. Type a root priority in the Root Priority field. The root priority can be a value from 0 to 7, but UAPs with a root priority of 0 cannot become the root. When you are finished, click Submit Changes to save your changes.

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

Configuring the AP Name

The AP name is a unique name that identifies a given UAP in the network. The AP name is also used by the OpenAir master to distinguish the radios in a given UAP from other radios in the network. Only the first 11 characters are used for the OpenAir master name.

To configure the AP name

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Spanning Tree Settings. The Spanning Tree Settings screen appears.
3. Type an AP name in the AP Name field. The AP name can be from 1 to 16 characters long. When you are finished, click Submit Changes to save your changes.

Configuring the 21XX UAP as a DHCP Server

The 21XX UAP contains a simple DHCP server that you can use to provide DHCP server functions for small installations where no other DHCP server is available. The DHCP server will offer IP addresses to any DHCP client it hears as long as a pool of unallocated IP addresses is available. These clients may include other UAPs, wireless clients, wired hosts on the distribution LAN, or wired hosts on secondary LANs.

Note: This DHCP server is not intended to replace a general purpose, configurable DHCP server, and it makes no provisions for synchronizing DHCP policy between itself and other DHCP servers. Customers with complex DHCP policy requirements should use other DHCP server software.

To avoid a single point of failure, the DHCP server may be enabled in more than one UAP; however, UAPs do not share DHCP client databases. Each DHCP server UAP should be configured with a different DHCP address pool from which to allocate client addresses.

You must configure a UAP acting as a DHCP server with a static IP address. You cannot configure the UAP as both a DHCP server and a DHCP client.

To configure the 21XX UAP as a DHCP server

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Enter an IP address and a subnet mask for the UAP.
   a. Click TCP/IP Settings.
   b. Enter a static IP address in the IP Address field, and enter a subnet mask in the IP Subnet Mask field. When you are finished, click Submit Changes to save your changes.
3. Enable the server.
   - In the TCP/IP Settings screen, click the DHCP Mode down arrow and choose This AP is a DHCP Server. When you are finished, click Submit Changes to save your changes.
4. Configure the DHCP server.
   a. Click DHCP Server Setup. The DHCP Server Setup screen appears.

The DHCP Server Setup Screen

b. Configure the DHCP server. When you are finished, click Submit Changes to save your changes.

The following table explains each parameter.

Parameter	Explanation
Low Address	Specifies the low IP address in the range of IP addresses available to the DHCP server for distribution to DHCP clients. If these addresses are not on the same subnet as the UAP, the UAP will perform Network Address Translation (NAT) for the devices to which it grants IP addresses.
High Address	Specifies the high IP address in the range of IP addresses available to the DHCP server for distribution to DHCP clients. If these addresses are not on the same subnet as the UAP, the UAP will perform Network Address Translation (NAT) for the devices to which it grants IP addresses.
DNS Address 1	Specifies the IP address of a Domain Name Server that will be distributed to DHCP clients. You can enter up to two DNS addresses to be delivered to DHCP clients.
DNS Address 2	Specifies the IP address of a Domain Name Server that will be distributed to DHCP clients. You can enter up to two DNS addresses to be delivered to DHCP clients.
IP Subnet Mask	Indicates how many host bits of the IP address represent a subnet number. Use IP subnets to partition traffic and to connect routers. The IP subnet mask must represent contiguous ones (1) from the left and contiguous zeros (0) from the right.

DHCP Server Parameters Table (continued)

Parameter	Explanation
IP Router (Gateway)	Specifies what IP router DHCP will be offering to clients. If NAT has been automatically enabled, the UAP will use the lowest DHCP address to provide an IP router that performs NAT.
NAT (Network Address Translation) Status	Specifies if DHCP has been properly configured and if the range has automatically enabled NAT. When a station uses the UAP as an IP router, the UAP replaces the MAC address, IP source address, and TCP/UDP port with its own. You can configure the DHCP to indicate that the UAP is the IP router when it allocates the address to a station. Special consideration is given to changing the FTP data connection TCP port number, which is in the body of the TCP frame. After the frame source is modified, it is forwarded to the proper subnet. If the destination subnet is not the same subnet as the UAP's Ethernet, the destination MAC address is changed to the IP router that has been configured for the access point. If the access point belongs to the subnet, the AP converts the MAC address to the MAC address that belongs to the destination IP address. This may involve the operation of the ARP protocol for MAC address discovery. When the access point receives a frame with its IP address, it identifies the need for address translation by inspecting the destination port number. If the port number is within the pool reserved for NAT operation, it looks up the original MAC address, IP address, and port number. The frame is then modified and forwarded to the station. You can disable or enable NAT operation. You must configure the access point with two IP addresses; the normal address already has a configuration method. The access point must also have an address on the subnet for which it is acting as a NAT gateway. This second address only supports ARP translation for stations configured for NAT. It cannot access any AP menus. NAT operation is disabled or enabled automatically depending on the continuous range of addresses you enter into the DHCP Server. NAT is disabled if the range of addresses to be given to DHCP Clients is on the same subnet as the access point. If the range of addresses to be given out by the DHCP server is not on the same subnet as the access point, you are creating a virtual network and the DHCP server will also perform NAT translation.

Supported DHCP Options

The DHCP server issues IP address leases to configure the following fields and options:

IP broadcast address This address, along with the subnet mask and default router, will contain the same values as configured for the UAP.

Lease duration The lease duration is always twenty minutes.

Unsupported DHCP Options

The DHCP server implemented in the 21XX UAP does not support any DHCP options other than those listed. The DHCP server disregards any DHCP options that are not explicitly required by the DHCP specification. The DHCP server ignores all packets with a non-zero giaddr (gateway IP address). The server only responds to requests emanating from it's own subnet.

Configuring the 21XX UAP as a NAT Server

You can enable the access point as a NAT server.

To enable the access point as a NAT server

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Choose the TCP/IP Settings menu and configure the following parameters:
   a. subnet mask
   b. static IP address
3. Choose This AP is a DHCP Server in the DHCP Mode field.
4. Click DHCP Server Setup and enter a contiguous range of IP addresses that are not on the same subnet as the access point for the DHCP address pool. Click Submit Changes when you are finished.
5. Configure any optional parameters.
   a. Enter up to two DNS addresses to be delivered to DHCP clients.

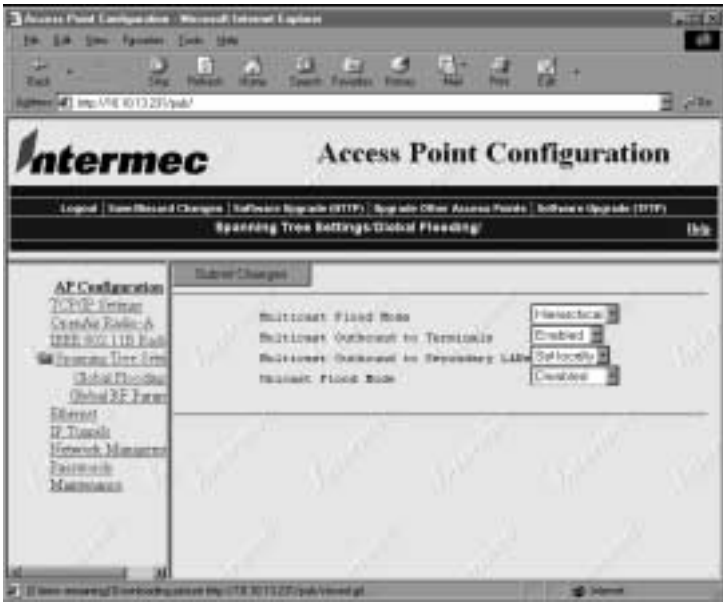
Configuring Global Flooding

Use global flooding to determine how a UAP handles a frame with an unknown address. The global flooding settings are sent throughout the network from the root UAP. Access points try to forward frames to the port with the shortest path to the destination address. When the UAP has not learned the direction of the shortest path, you can configure it to flood the frames in certain directions to try to locate the destination address.

Global flooding parameters you set will override parameters that you set in UAPs acting as designated bridges.

To configure global flooding

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Spanning Tree Settings. The Spanning Tree Settings screen appears.
3. Click Global Flooding. The Global Flooding screen appears.



4. Configure the Global Flooding parameters. When you are finished, click Submit Changes to save your changes.

The following table explains each parameter.

Parameter	Explanation
Multicast Flood Mode	Determines the flooding structure for multicast frames with unknown destination addresses.
	Universal Allows any node to communicate with any other node.
	Hierarchical Allows nodes in the wireless network to communicate with nodes on the primary LAN but not with other wireless devices.
	Disabled Prevents flooding.
Multicast Outbound to Terminals	Determines if outbound multicast frames with unknown destination addresses are flooded toward wireless stations. Only applies to 2.4 GHz OpenAir and 802.11b HR radios.
	Enabled Outbound multicast frames with unknown destination addresses are flooded toward wireless stations.
	Disabled Outbound multicast frames with unknown destination addresses are not flooded toward wireless stations.
Multicast Outbound to Secondary LANs	Determines whether outbound multicast frames with unknown destination addresses are flooded toward secondary LAN segments.
	Enabled Causes the root access point to control flooding for all access points serving as designated bridges for the secondary LANs.
	Set locally Allows designated bridges on secondary LANs to control flooding on their LANs.
Unicast Flood Mode	Determines the flooding structure for inbound unicast frames with unknown destination addresses.
	Universal Allows any node to communicate with any other node.
	Hierarchical Allows nodes in the wireless network to communicate with nodes on the primary LAN but not with other wireless devices.
	Disabled Prevents flooding.

Configuring Global RF Parameters

You can 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 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.

To configure global RF parameters

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Spanning Tree Settings. The Spanning Tree Settings screen appears.
3. Click Global RF Parameters. The Global RF Parameters screen appears.

4. Configure the Global RF Parameters. When you are finished, click Submit Changes to save your changes.

The following table explains each parameter.

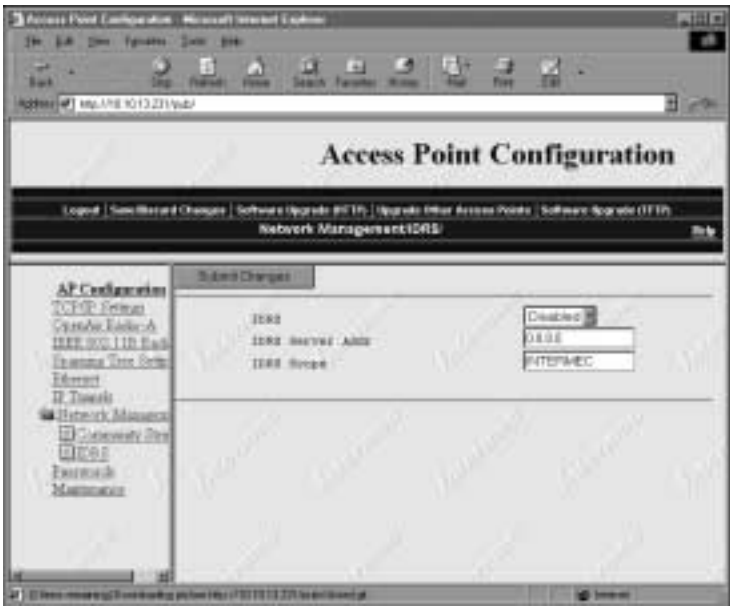
Parameter	Explanation
RFC1042/DIX Conversion	Determines how the access point will handle the conversion of RFC1042/DIX frames that are received on its 802.11b HR radio ports. **Enabled** Causes frames received on an 802.11b HR port with a protocol type equal to a value in the "RFC1042 types to pass through" list to be forwarded without conversion. Frames with protocol types not found in the list will be converted to DIX format before they are forwarded. **Disabled** Causes frames received on a radio port to be forwarded without translation from RFC10472 format to DIX; that is, when a SNAP frame is received from an 802.11b HR radio with an OUI (Organizationally Unique Identifier) equal to 000000, it will be forwarded without conversion.
S-UHF Rfp Threshold	Determines the largest data packet that can be transmitted without reserving air time. Air time is normally reserved to help prevent collisions with other transmitters; however, when the amount of data is small enough, sending the data may be more effective than creating the reservation.
S-UHF Frag Size	Determines the largest data packet that can be transmitted without fragmentation. On certain radios, the fragmentation does not occur unless the radio detects interference. Larger packet sizes can improve throughput on a reliable connection, while smaller packet sizes can improve throughput on a poor connection.
900 MHz Frag Size	Determines the largest data packet that can be transmitted without fragmentation. On certain radios, fragmentation does not occur unless the radio detects interference. Larger packet sizes can improve throughput on a reliable connection, while smaller packet sizes can improve throughput on a poor connection.
S-UHF/900 MHz Awake Time	Specifies the amount of time that a wireless station stays awake when radios are inactive. A sleeping station is less responsive to radio activity; however, the longer a station is kept fully awake, the larger the drain on the battery. You should set a station to stay awake long enough to receive an expected reply to a transmission and short enough to reduce power consumption. The awake time can be set to a number from 0 to 250 tenths of a second. This parameter applies only to S-UHF and 900 MHz radios.
RFC1042 Types to Pass Through	Determines values for protocol types that are to be passed without conversion. The list includes the Apply Talk protocol type, value 80F3. This parameter only appears when RFC1042/DIX conversion is Enabled. Values entered in this parameter represent the protocol types of frames that will be passed without conversion to DIX format.

Configuring IDRS

IDRS (Intermec Device Registration Service) is part of an overall network management strategy. Typically, a network management station polls each possible IP address to discover the active devices on a network. This discovery process is time-consuming and uses valuable network bandwidth. When you use IDRS, however, each Intermec device automatically registers with an IDRS server on startup; the IDRS server then maintains a database of all registered devices. To retrieve information, a management station can query the IDRS server rather than poll each individual address, easing the burden on the management station and reducing network traffic. For more information about IDRS servers, contact your Intermec representative.

To configure IDRS

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Network Management, and then click IDRS. The IDRS screen appears.



3. Configure the IDRS parameters. When you are finished, click Submit Changes to save your changes.

The following table explains the IDRS parameters.

Parameter	Explanation
IDRS	Enables or disables IDRS. If you enable IDRS and specify a valid IDRS server using the IDRS Server Address parameter, the UAP registers with the IDRS server when it boots.
IDRS Server Addr	Specifies the IP address of the IDRS server. If you specify a non-zero IP address in this field, the UAP will attempt to discover an IDRS server to register when it boots.
IDRS Scope	Specifies a logical name for a group of devices. You can use the scope field to define different groups of devices. The scope can be no more than 15 characters.

4

Configuring the Radios

This chapter explains how to configure the radios.

About the Radios

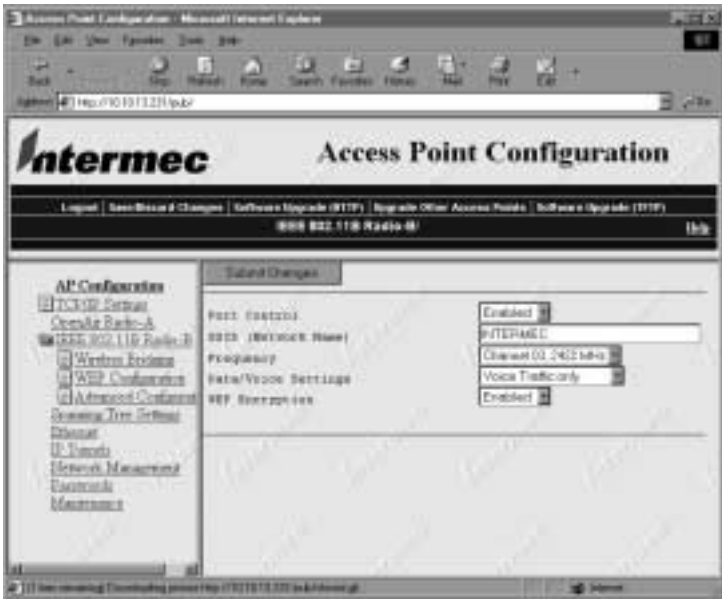
Access points consist of a group of multiport Ethernet bridges. The 2102 supports only one radio port; otherwise, the three UAPs are identical. The 2100 supports the following radios:

- 802.11b HR
- 2.4 GHz OpenAir
- 900 MHz
- S-UHF

The 2101 and 2102 support the 802.11b HR and 2.4 GHz OpenAir radios.

Configuring the 802.11b HR Radio

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears.



3. Configure the parameters for the radio. When you have finished, click Submit Changes to save your changes.

   The following table explains each parameter.

Parameter	Explanation
Port Control	Enables or disables the Ethernet port.
SSID (Network Name)	The 802.11b HR radio communicates with other 802.11b HR radios with the same network name. Use this parameter to 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 SSID (Network Name) can be no more than 32 alphanumeric characters. The default SSID (Network Name) is INTERMEC (case-sensitive).
Frequency	The frequency is the particular frequency within the 2.4 to 2.5 GHz range that the UAP uses to transmit and receive packets. The available frequencies are country-dependent and are determined by the radio. Configure all UAPs used in Spain, France, or Japan to a common frequency. For all other countries, you can configure all UAPs to a common frequency, or you can select up to three frequencies that are at least three channels (or 25 MHz) apart. You could select 2412 MHz, 2437 MHz, and 2462 MHz, for example. 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 or multiple microwave ovens are in use in the area. For optimal performance of UAPs that are within range of each other, you should configure their frequencies to be five channels apart. You could configure the UAPs to use channels 1, 6, and 11, for example.
Data/Voice Settings	Set to Data Traffic Only if the UAP will transmit only data traffic. Set to Data and Voice Traffic if the UAP will transmit both data and voice traffic. Set to Voice Traffic Only if the UAP will transmit only voice traffic.
WEP Encryption	Use this option to enable or disable WEP Encryption. This option appears on your menu only if your 802.11b HR radio supports WEP data encryption for wireless communication.

Worldwide Frequencies for the 802.11b HR Radio

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

FCC countries include the United States, Canada, China, Taiwan, India, Thailand, Indonesia, Malaysia, Hong Kong, and most South American countries.

ETSI countries include all European Union countries except France. It also includes Switzerland, Iceland, Norway, Czech Republic, Slovenia, Slovakia, Turkey, Russia, and the United Arab Emirates.

Mexico and Singapore use the same channels as France.

The 802.11b channels that are allowed in a given country may change without notice. Be sure you use only those frequencies that are permissible in the given country.

Configuring Voice Over IP

You can specify what type of traffic can be delivered to your 802.11b HR port. You can use a single 802.11b HR radio to support both voice and data communications over the same radio.

To configure Voice over IP

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.

2. Configure the following parameters on your 802.11b HR radio:
   - Multicast rate to 1 Mbits/Sec if you are using a 1 Mbit/sec telephone
   - Multicast rate to 2 Mbits/Sec if you are using a 2 Mbit/sec telephone
   - Transmit Rate Fallback to Enabled
3. Click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears.
4. Click the Data/Voice Settings down arrow and choose a setting. When you are finished, click Submit Changes to save your changes.

   Data Traffic only Specifies that the port will be used for data traffic only. No special filtering.

   Data and Voice Traffic Specifies that the port will be used for both data and voice traffic. All MobileLAN™voice 2 handset packets are sent in the high priority queue. Packets in the high priority queue are sent ahead of packets in the normal priority queue. No special filtering.

   Voice Traffic only Specifies that the port will be used for voice traffic only. All MobileLAN™voice 2 handset IP packets are sent with a priority setting. All other multicast/broadcast packets will be dropped.

Note: To specify which terminals/telephones attach to which radio in a dual access point, you should use a different Network Name for each radio. You also must enter the Network Name on each telephone.

Configuring Advanced 802.11b HR Radio Parameters

You can configure other parameters for the 802.11b HR radio, such as Data Rate, Medium Reservation, and Microwave Oven Robustness. Click Advanced Configuration to configure these and other parameters.

To configure advanced parameters

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Advanced Configuration in the IEEE 802.11b Radio menu. The Advanced Configuration screen appears.

The Advanced Configuration Screen

3. Configure the advanced parameters. When you are finished, click Submit Changes to save your changes.

   Use the following table to configure advanced parameters.

Parameter	Description
Data Rate	Use Data Rate to choose the rate at which the UAP transmits data.
Data Rate Fallback	Disable this parameter to prevent the radio from dropping to a slower transmission bit rate when it has trouble communicating with another station. This parameter also limits your range to the Data Rate selected above.
Basic Rate	Use this parameter to choose the UAP's basic and multicast transmission rate. Under most circumstances this parameter should be left at the default 2 Mbit setting.
Medium Reservation	Use this parameter to enable or disable a reservation threshold. **Enabled** Allows you to set a threshold value using the Reservation Threshold parameter. **Disabled** May improve network response time in installations that primarily send very small frames or that have no hidden stations.

The Advanced Parameters Configuration Table (continued)

Parameter	Description
Distance Between APs	Use this parameter to control the roaming sensitivity of your end devices. The setting on your UAP should match the setting on your end devices. You can use this parameter to virtually reduce the range of your UAP. Using the Small or Medium setting does not reduce the absolute range of your radio, but it does modify the collision detection mechanism to allow significant overlap of the wireless cells. Although setting this parameter to Small or Medium creates a higher performance radio network, more UAPs are needed to cover a given area.
Microwave Oven Robustness	Enable this parameter to activate a modified algorithm for automatic rate fallback, which prevents the UAP from falling back to 1 Mbits when trying to retransmit radio packets when 2.4 GHz interference is present.
Network Name Security	Use this parameter to determine if terminals with an SSID (Network Name) setting of ANY or NULL will associate with any access point. **802.11 Compliant** Allows terminals with an SSID setting of ANY or NULL to associate with the access point. This setting is 802.11b HR compliant. **Network Name 'ANY' Not Allowed** Prevents terminals with an SSID setting of ANY or NULL from associating with the access point. This setting is not 802.11b HR compliant.
DTIM Period	Use this parameter to specify 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 increase response time. You can set the DTIM period to a value from 1 to 65535.

Configuring WEP

Click WEP Configuration under the IEEE 802.11b Radio menu to set WEP configuration parameters. This option appears only if your 802.11b HR radio supports WEP encryption and you enabled WEP Encryption.

To set WEP configuration parameters

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Choose IEEE 802.11b Radio and enable WEP Encryption.
3. Click WEP Configuration in the IEEE 802.11b Radio menu. The WEP Configuration screen appears.

The WEP Configuration Screen

4. Set the parameters for WEP configuration. When you are finished, click Submit Changes to save your changes.

   The following table explains each parameter.

Parameter	Explanation
WEP Receive Data	Use this parameter to determine if the UAP will receive transmissions from end devices that are not using WEP. **Unencryption Allowed** Allows transmissions from end devices that are not using WEP. **Encryption Required** Prevents transmissions from end devices that are not using WEP.
WEP Transmit Key	Use this parameter to determine which of the four default WEP keys this UAP uses to transmit data. The default is 1, which means that the UAP uses WEP key 1 to transmit data.
WEP Key 1	Your own WEP code.
WEP Key 2	Your own WEP code.
WEP Key 3	Your own WEP code.
WEP Key 4	Your own WEP code.

   To ensure maximum security, you should configure each WEP key with a different WEP code.

Configuring Wireless Hops

A hop occurs when data from an end device moves from one access point to another via the radio ports. At least two access points must be configured for wireless hops: one as a master and the other as a station. Station access points attach to master access points. Wireless hops must be enabled on the master access point for IAPP Hello packets to be transmitted via the master's radio port. This setting allows the wireless access points to attach to the IAPP spanning tree in the same way that a wired access point does.

You can enable or disable wireless hops on any master UAP. If you enable wireless hops, the UAP honors connections from UAPs that are configured as stations.

If you have a 2.4 GHz OpenAir radio in your station access point, the LAN ID, security ID, channel, and subchannel must match those of the master access point.

If you have an 802.11b radio in your station access point, the LAN ID and Network Name must match those of the master access point; in addition, the station and master must be on the same IP subnet.

You must enable wireless hops on the master UAP for

- point-to-point bridging.
- a master access point that will communicate with a WAP.

To form a wireless hops (Ethernet access point)

1. Establish a Web browser session on the wired access point if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click the menu corresponding to the radio you are configuring (i.e., IEEE 802.11b Radio).
3. Click Wireless Bridging.
4. Click the Node Type down arrow and choose master.
5. Click the Wireless Hops down arrow and choose Enabled. Click Submit Changes before leaving the Wireless Bridging screen.

To form a wireless hops (Wireless access point)

1. Establish a Web browser session on the wireless access point if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click the menu corresponding to the radio you are configuring (i.e., IEEE 802.11b Radio).
3. Click Wireless Bridging.

4. Click the Node Type down arrow and choose station. Click Submit Changes before leaving the Wireless Bridging screen.

Configuration Example 1: Dual 802.11b HR Radios Without WEP

Following is an example of how you might configure a wireless hop in which a terminal is able to roam between the wired LAN and the wireless access point. In general, this is the easiest wireless hop configuration to set up. The advantages and disadvantages of using this configuration are listed below.

Advantages	Disadvantages
Does not require WEP keys.	A second 802.11b HR radio is required on the root LAN/distribution LAN access point.
Terminals can roam between access points forming the wireless hop.	Limited to a single wireless hop if terminals are to roam.

To configure wireless hops using dual 802.11b HR radios and not using WEP

1. Configure the root LAN segment access point.
   a. Be sure the access point is configured with two master radios (see "Configuring Node Type" on page 4-15).
   b. Set Wireless Hops on radio B to Enabled (see "Configuring Wireless Hops" on page 4-10).
   c. Be sure the SSID (Network Name) of the root LAN access point master radio A matches the SSID (Network name) of master radio A on the wireless access point (see "Configuring Node Type" on page 4-15).
   d. Be sure the SSID (Network Name) of master radio B on the root LAN access point matches the SSID (Network Name) of station radio A on the wireless access point.
   e. Wireless terminals are station radios by definition and should be configured with the <Choice 1> network name.
2. Configure the wireless access point.
   a. Be sure the access point is configured with one Master radio and one Station radio.
   b. Set the AP Root Priority to zero (see "Setting Root Priority" on page 3-12).
   c. Be sure the SSID (Network Name) of each radio is set so that <Choice 1> and <Choice 2> do not match.

Configuration Example 2: Single Radio on Remote LAN Segment

Following is an example of how you might configure a wireless hop using a single radio on the remote LAN segment. The advantages and disadvantages of using this configuration are listed below.

Advantages	Disadvantages
Does not require WEP keys.	Wireless clients are not supported on the wireless access point because the wireless access point is configured with only one station radio.
Designed to support wired terminals on the secondary LAN segment.	

To configure wireless hops using a single radio on the remote LAN segment

1. Set up the access point on the remote LAN segment.
   a. Be sure the radio in the primary LAN segment is configured as a Master.
   b. Enable wireless hops on the master access point (see “Configuring Wireless Hops” on page 4-10).
   c. Be sure the SSID (Network Name) of the master radio on the root LAN segment matches the SSID (Network Name) of the station radio in the secondary LAN segment.
2. Set up the wireless access point on the secondary LAN segment.
   a. Be sure the radio is configured as a Station.
   b. Set the Root Priority to zero (see “Setting Root Priority” on page 3-12).
   c. Set the secondary LAN bridge priority to a value other than zero (see “Configuring Secondary LAN Bridge Priority” on page 2-9). Setting this parameter to 1 will satisfy most standard configurations.
   d. Enable secondary LAN flooding.
   e. Be sure the SSID (Network Name) of the master radio of the root LAN segment matches the SSID (Network Name) of the station radio of the secondary LAN segment.

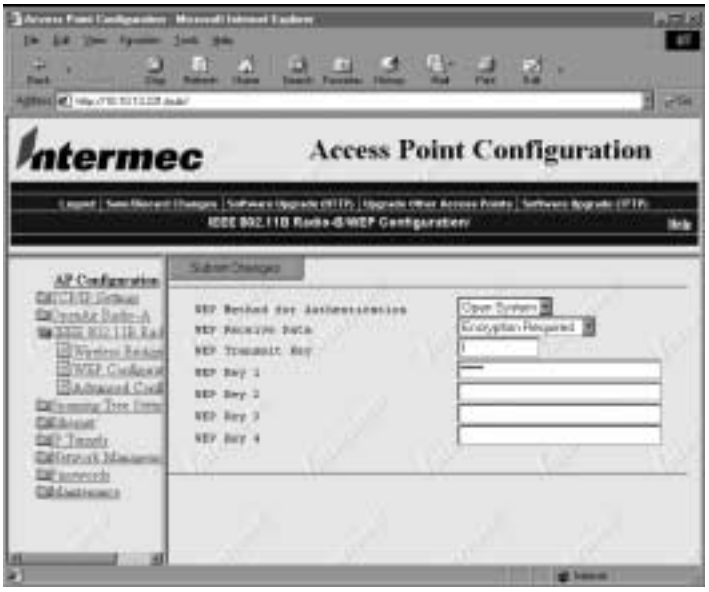
Configuration Example 3: Dual 802.11b HR Radios Using WEP

Following is an example of how you might configure a wireless hop using dual 802.11b HR radios and using WEP.

To configure wireless hops using dual 802.11b HR radios and WEP

1. Configure the root LAN segment access point.
    a. Be sure the access point is configured with two master radios (see "Configuring Node Type" on page 4-15).
    b. Set Wireless Hops on radio B to Enabled (see "Configuring Wireless Hops" on page 4-10).
    c. Be sure the SSID (Network Name) of the root LAN access point master radio A matches the SSID (Network name) of master radio A on the wireless access point (see "Configuring Node Type" on page 4-15).
    d. Be sure the SSID (Network Name) of master radio B on the root LAN access point matches the SSID (Network Name) of station radio A on the wireless access point.
    e. Wireless terminals are station radios by definition and should be configured with the <Choice 1> network name.
    f. Click IEEE 802.11b Radio, and then click WEP Configuration. The WEP Configuration screen appears. For more information, see "Configuring WEP" on page 4-8.
2. Configure the wireless access point.
    a. Be sure the access point is configured with one Master radio and one Station radio.
    b. Set the AP Root Priority to zero (see "Setting Root Priority" on page 3-12).
    c. Be sure the SSID (Network Name) of each radio is set so that <Choice 1> and <Choice 2> do not match.
    d. Click IEEE 802.11b Radio, and then click WEP Configuration. The WEP Configuration screen appears. For more information, see "Configuring WEP" on page 4-8.

The WEP Configuration Screen



3. Click the WEP Method for Authentication down arrow and choose Open System or Shared Key.

   Open System A WAP using encryption will not use WEP to authenticate the WEP key, allowing a WAP to attach to a master access point without the same key. The wireless hop will be formed, but no communication will be possible.

   Shared Key A WAP will use WEP to authenticate the WEP key, preventing a WAP from attaching to an access point with an incorrect WEP key.

If you have a secondary LAN and plan to use an access point to roam, you must enter the MAC address of every Ethernet client on the secondary LAN into the Ethernet Address Table of the secondary LAN bridge access point. For more information, see “Configuring the Ethernet Address Table” on page 5-3. You must enter the MAC address when the Ethernet client on the secondary LAN does not **always** initiate communication.

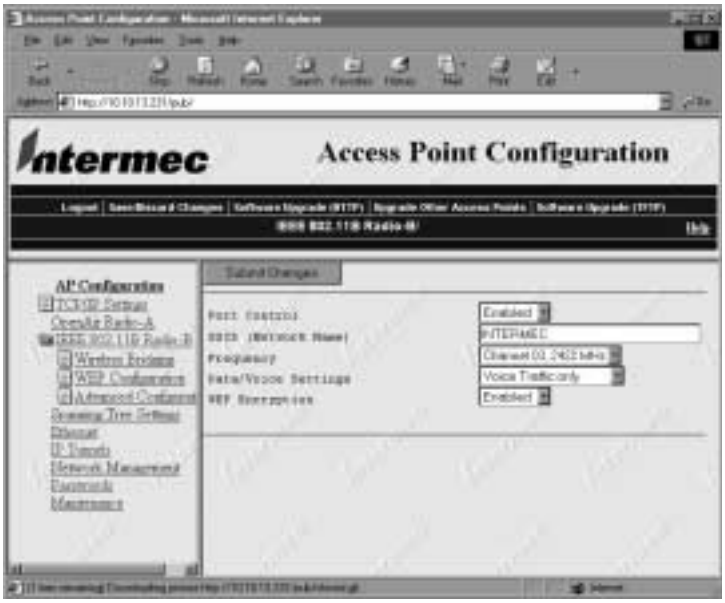
Terminals that roam using WEP can have up to two hops; terminals that roam without using WEP can have only one hop. Because the previous example configuration uses the same network name to allow terminals to roam, you must use WEP to prevent your master radio from connecting to your station radio in the same access point.

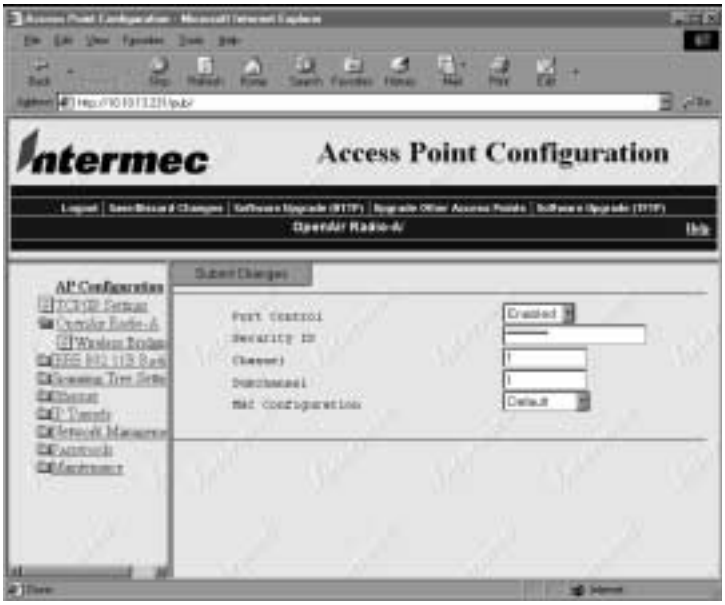
Configuring Node Type

Use the node type parameter to configure a radio as a Master or Station. You can configure node type only when wireless hops is enabled.

To configure node type

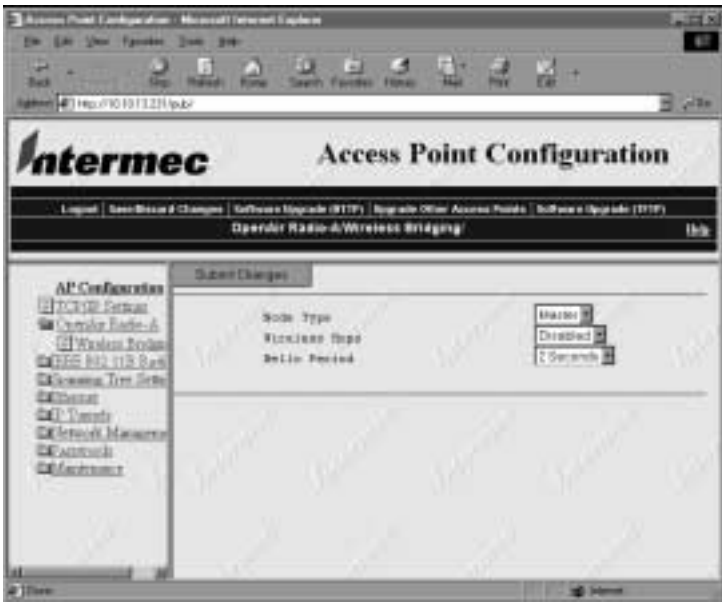
1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IEEE 802.11b Radio or 2.4 GHz OpenAir Radio. The appropriate screen appears.





3. Click Wireless Bridging. The Wireless Bridging screen appears.

The OpenAir Wireless Bridging Screen



4. Change node type to “station.” When you are finished, click Submit Changes to save your changes.

Configuring OpenAir UAPs for Bridging

To use OpenAir radios for wireless bridging, you must configure one UAP as a master and the second as a station.

For wireless bridging, both OpenAir radios must have the same

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

To configure OpenAir UAPs to bridge between Ethernet LANs

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Configure the LAN ID (Domain). For more information, see “Configuring the LAN ID (Domain)” on page 3-12.
3. Configure the Security ID, Channel, and Subchannel. For more information see “Configuring the 2.4 GHz OpenAir Radio” on page 4-19.

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

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

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

You may need to adjust the global flooding parameters for wireless bridging. Follow these recommendations when configuring the global flooding parameters for a point-to-point bridge:

- If all gateways and servers are on the primary LAN, set the Multicast Flood Mode to Hierarchical.
- If end devices must communicate with gateways or servers on a secondary LAN, set Multicast Flood Mode to Universal.
- If end devices on a secondary LAN communicate with end devices on another secondary LAN, set Multicast Flood Mode to Universal.

For more information about global flooding, see “Configuring Global Flooding” on page 3-17.

Configuring the 2.4 GHz OpenAir Radio

Click the 2.4 GHz OpenAir Radio menu to configure the 2.4 GHz OpenAir radio.

To configure the 2.4 GHz OpenAir radio

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click 2.4 GHz OpenAir Radio from the Configuration screen menu. The 2.4 GHz OpenAir screen appears.
3. Configure the parameters for the radio. When you are finished, click Submit Changes to save your changes.

   The following table explains what information is needed in each parameter.

Parameter	Explanation
Port Control	Use this parameter to enable or disable the OpenAir port.
Security ID	Use this parameter to set a security identification value. All UAPs and end devices that use OpenAir radios in the same network must have the same security ID to communicate with each other. Setting a security ID value prevents unauthorized radios from communicating with the UAP. Security ID values can be from 0 to 20 characters in length.

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

CAUTION

Caution
Intermec recommends that you set the security ID for your OpenAir network to a value other than null. Failure to change the default setting could expose your network to a security breach by an unauthorized wireless device.

Conseil
Intermec vous recommande de régler l'ID de sécurité de votre réseau OpenAir de 2,4 GHz sur une valeur autre que Nul. Si le paramètre par défaut n'est pas modifié, vous risquez d'exposer votre réseau à une brèche de sécurité par un périphérique sans fil non autorisé.

Channel	Use this parameter to set the hopping sequence for the radio. The Channel value can be any number from 1 to 15. The Channel parameter only applies if the radio is set to master. If you are using OpenAir radios and you have more than one UAP in the same coverage area, you must configure each UAP with a unique channel.

2.4 GHz OpenAir Radio Parameters Table (continued)

Subchannel	Use this parameter to enable UAPs to share the same channel while having a unique subchannel. This configuration prevents the UAP from receiving frames intended for another UAP. Two UAPs on different subchannels share the same hopping sequence, but behave as if they were on different channels. The Subchannel parameter only applies if the radio is set to master.
MAC Configuration	Use this parameter to adjust the MAC Configuration parameter, which may enhance the performance of your OpenAir radio. **Note:** An inefficient MAC Configuration setting can adversely affect the performance of your open wireless LAN. Change the MAC Configuration setting only under the direction of Intermec Technical Support. **Default** Uses the factory settings for the radio protocol. You should use this setting for normal operations. **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 Manual MAC Parms command. To adjust these parameters, see "Setting Manual MAC Parameters" in the next section.

Configuring MAC Configuration

The MAC configuration determines the type of MAC configuration parameters the access point will use to enhance performance.

To configure MAC configuration

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click 2.4 GHz OpenAir. The 2.4 GHz OpenAir screen appears.
3. Click the MAC Configuration down arrow and choose a configuration.

The following table explains each configuration.

Parameter	Description
Default	Uses the factory default settings for the radio protocol.
Interference	Optimizes performance in high interference or multipath environments.
Throughput	Optimizes file transfer operations in low interference environments, such as office areas.
Manual	Allows you to adjust the MAC parameters individually. To configure MAC parameters individually, see "Setting Manual MAC Parameters" in the next section.

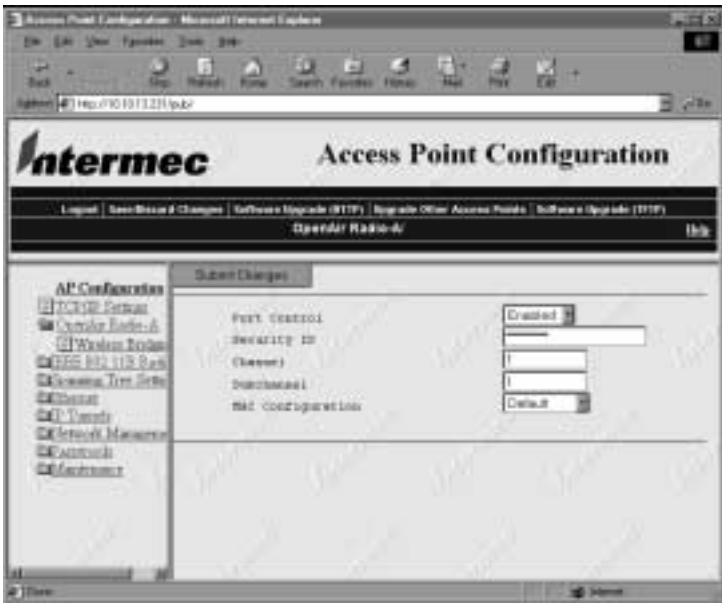
Setting Manual MAC Parameters

Occasionally, you may need to fine-tune your OpenAir radio MAC parameters. To configure MAC settings manually, click Manual MAC Parms.

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.

To set manual MAC parameters

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click 2.4 GHz OpenAir Radio from the Configuration screen menu. The OpenAir Radio screen appears.



3. Click the MAC Configuration down arrow, and choose Manual MAC Parms. Click Submit Changes.
4. Click Manual MAC Parms. The Manual MAC Parms screen appears.

Note: This is a master radio menu. A station radio menu will have fewer options.

5. Configure the radio parameters. When you finish, click Submit Changes to save your changes.

   The following table explains each 2.4 GHz OpenAir manual MAC parameter.

Parameter	Explanation
Hop Period	Determines how long the radio stays on a frequency in the hopping sequence before stepping to the next frequency. You can set Hop Period to 100, 200, or 400 milliseconds. Longer time periods result in better throughput while shorter time periods result in faster roaming response and immunity from interference.
Beacon Frequency	Shows the number of hops between beacons (the UAP periodically transmits a beacon to allow stations to quickly scan each frequency to find a master UAP). You can set Beacon Frequency to a value from 1 to 7.
Deferral Slot	Works with the Fairness Slot to determine the average back-off time when the channel is busy. You can set Deferral Slot to 1, 3, 7, or default. You may want to reduce the number of slots on lightly-loaded networks to increase throughput or increase the number of slots to help prevent repeated collisions under a heavy load.

2.4 GHz OpenAir Manual MAC Parameter Table (continued)

Parameter	Explanation
Fairness Slot	Works with the Deferral Slot to determine the average back-off time when the channel is busy. You can set Fairness Slot to 1, 3, 7, or 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	Determines the maximum fragment size that can be sent over the radio during interference (fragments are created when errors occur in transmission). 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.
Transmit Mode	Modulates the transmit signal and sets the bits per second. **BFSK (Binary Frequency Shift Keying)** Transmits at 0.8 Mbps. Data is transmitted by shifting between two frequencies to represent one 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 two bits of 0 or 1. QFSK has better throughput than BFSK at the expense of range. **AUTO** Automatically adapts the bit rate to the error conditions. The transmit mode is automatically selected for the best range and throughput.
Norm Ack Retry	Controls the number of times an unfragmented frame is resent unsuccessfully before fragmenting. You can set the parameter 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.
Norm QFSK Retry	Controls the number of times that an unfragmented QFSK frame is resent unsuccessfully before switching to BFSK. Set this parameter to a value from 1 to 255. This parameter only applies when Transmit Mode is set to AUTO.
Frag QFSK Retry	Controls the number of times a fragmented QFSK frame is resent unsuccessfully before switching to BFSK. You can set this parameter to a value from 1 to 255. This parameter only applies when Transmit Mode is set to AUTO.

Configuring an OpenAir Wireless Access Point

To configure an OpenAir UAP as a WAP, the UAP must have two OpenAir radios installed. One radio must be configured as a master and the other one as a station. The master radio communicates with end devices that are configured as stations, and the station radio communicates with an OpenAir radio in another 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.

To configure an OpenAir wireless access point

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Configure the LAN ID (Domain). For more information, see "Configuring the LAN ID (Domain)" on page 3-12.
3. Configure the Security ID, Channel, and Subchannel. For more information see "Configuring the 2.4 GHz OpenAir Radio" on page 4-19.

The following table is an example of how you might configure the single radio in the UAP and the dual radios in the WAP.

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

In this example, the OpenAir-A radio in the UAP is configured as a master and has the same channel and subchannel as the OpenAir-B radio in the WAP, which is configured as a station. The end devices must be configured as stations to communicate with the OpenAir-A master radio in the WAP. Instructions for setting these parameters are included earlier in this chapter.

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 Chapter 6, "Troubleshooting and Maintaining the 21XX UAP."

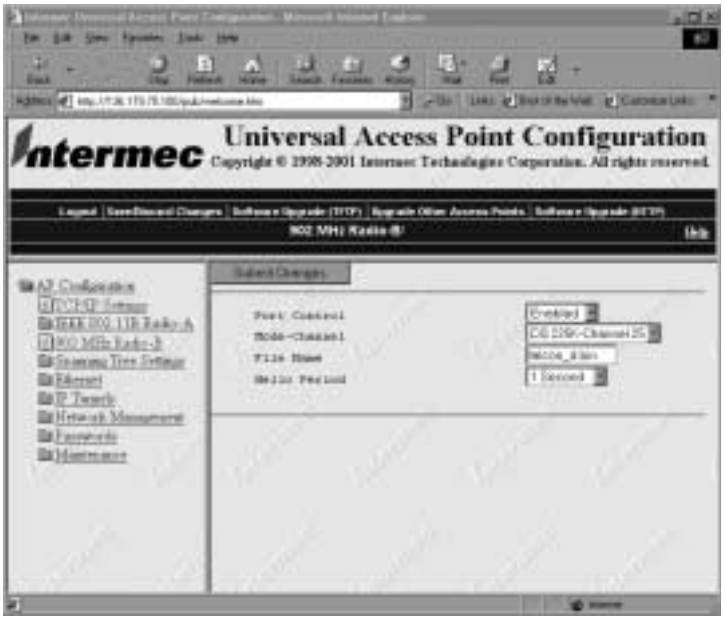
Configuring the 900 MHz Radio

Click 900 MHz Radio to configure the 900 MHz radio. The 900 MHz radio will communicate with other 900 MHz radios that have the same

- LAN ID.
- Mode-Channel.

To configure the 900 MHz port

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click 900 MHz Radio. The 900 MHz Radio screen appears.



3. Configure the parameters for the radio. When you are finished, click Submit Changes to save your changes.

The following table explains each 900 MHz radio parameter.

Parameter	Explanation
Port Control	Enables or disables the 900 MHz port.
Mode-Channel	Sets the bit rate option for the 900 MHz radio. Generally, the higher the bit rate, the lower the range of the UAP. Mode-Channel defines a frequency range that is a small portion of the available bandwidth. Mode-Channel displays the list of mode and channel combinations available on your UAP. Mode-Channel options are country-dependent. 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: **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 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-sequence channel at 450,000 bits per second. This one high-speed channel uses all available bandwidth.
File Name	Specifies the name of the radio's driver software. The default file name is falcon_d. You should change this name only when directed to do so by Intermec Technical Support.
Hello Period	Controls how frequently the UAP broadcasts hello packets on the 900 MHz radio port. Use hello packets on wireless links between UAPs to maintain the spanning tree. Hello packets also serve as beacon messages to synchronize communications with power-managed stations.

Configuring a 900 MHz Wireless Access Point

A 900 MHz wireless access point (WAP) communicates with other 900 MHz radios that have the same

- LAN ID (Domain).
- Mode-Channel.

Note: You can position your 900 MHz 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.

To configure your 900 MHz radio as a wireless access point

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Configure the LAN ID (Domain). For more information, see “Configuring the LAN ID (Domain)” on page 3-12.
3. Configure the Mode-Channel.

Intermec recommends that you install no more than two wireless access points for each UAP that is wired to the Ethernet network.

Configuring 900 MHz UAPs to Bridge Between Ethernet LANs

To use 900 MHz UAPs as a wireless bridge, you must configure the LAN ID (Domain) in both UAPs to the same value and set bridging parameters.

To configure 900 MHz UAPs to bridge between Ethernet LANs

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Configure the LAN ID (Domain). For more information, see “Configuring the LAN ID (Domain)” on page 3-12. The LAN ID in both UAPs must match. Click Submit Changes to save your changes.

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

Parameter	UAP on Primary LAN	UAP on Secondary LAN
LAN ID (Domain)	1	1
Root Priority	5	0
Secondary LAN Bridge Priority	0	5
Secondary LAN Flooding	Disabled	Disabled
Mode-Channel	DS 225K-Channel 25	DS 225K-Channel 25

You may need to adjust the global flooding parameters for wireless bridging. Follow these recommendations when configuring the global flooding parameters for a point-to-point bridge:

- If all gateways and servers are on the primary LAN, set the Multicast Flood Mode to Hierarchical.
- If end devices must communicate with gateways or servers on a secondary LAN, set Multicast Flood Mode to Universal.
- If end devices on a secondary LAN communicate with end devices on another secondary LAN, set Multicast Flood Mode to Universal.

For more information about global flooding, see “Configuring Global Flooding” on page 3-17.

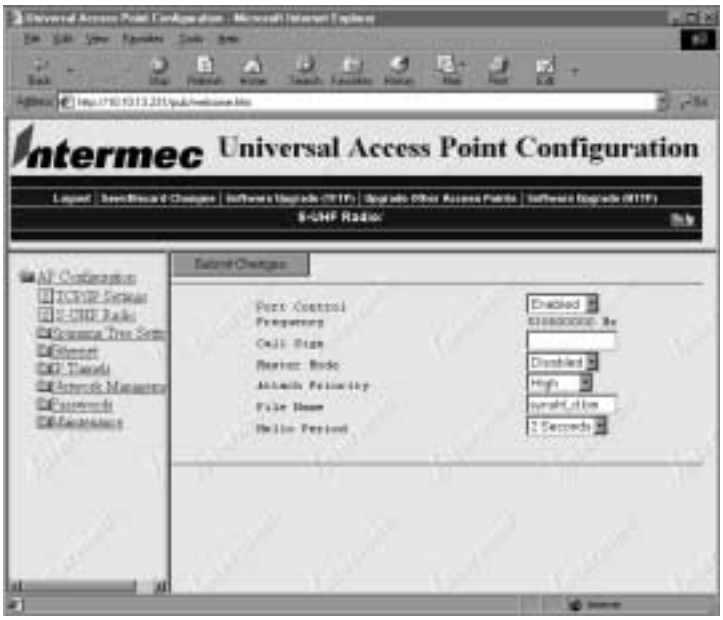
Configuring the S-UHF Radio

Click S-UHF Radio to configure the S-UHF radio.

To configure the S-UHF port

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.

2. Click S-UHF Radio. The S-UHF Radio screen appears.



3. Configure the S-UHF radio. When you are finished, click Submit Changes to save your changes.

The following table explains each S-UHF radio parameter.

Parameter	Explanation
MAC Address	Displays the MAC address of this port.
Port Control	Enables or disables the S-UHF port.
Hello Period	Controls how frequently the UAP broadcasts hello packets on the S-UHF port. Hello packets are used to maintain the spanning tree and serve as beacon messages to synchronize communications with power-managed stations.
File Name	Specifies the name of the radio's driver software. The default file name is synuhf_d.bin. Change this name only when directed to do so by Intermec Technical Support.
Call Sign	Specifies the call sign of the radio. Agencies that allocate S-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. The call sign can be from 0 to 12 characters long. The call sign parameter only applies to radios in the United States. Ignore this parameter if you are outside the United States.

The S-UHF Radio Parameters Table (continued)

Parameter	Explanation
Frequency	Displays the frequencies available on your UAP. Some radios have multiple frequencies. 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	Determines how channel access is controlled. **Enable** Sets the UAP to control channel access for end devices in its coverage area, and end devices automatically operate as slaves. Enabling may improve performance in some environments, but you should only enable Master Mode if the UAP radio coverage area does not overlap other access points operating in the same area. **Disable** Causes all radios in the network to cooperate as peers, and UAPs and end devices coordinate channel access as each radio bids for time. Disabling Master Mode often provides quicker access times on lightly- to moderately-loaded systems. Disabling overlaps coverage areas with access points on the same or different frequencies.
Attach Priority	Determines the likelihood that the UAP will obtain media access. This parameter only appears when Master Mode is Disabled. **High** Causes the radio to be more likely than an end device to obtain transmit time. **Medium** Causes the radio to be equally likely as an end device to obtain transmit time. **Low** Causes the radio to be less likely than an end device to obtain transmit time. Set Attach Priority 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 in the same coverage area. You should position the antenna at least 3 meters (10 feet) away from the UAP to achieve the specified performance for the S-UHF radio.

5

Configuring Filters and IP Tunnels

This chapter explains how to configure filters and tunnels.

Configuring Ethernet Filters

You can set both Ethernet and IP tunnel filters, and you can create protocol filters for both predefined and user-defined protocol types. In addition, you can define arbitrary frame filters based on frame content.

For help configuring IP filters, see “Configuring IP Tunnel Filters” on page 5-15.

Configuring the Ethernet Address Table

Use the Ethernet address table to enter the MAC address of a station attached to this UAP’s Ethernet. The address is entered as 6 hex pairs separated by spaces, colons, or hyphens. The default address is 00:00:00:00:00:00.

To configure the Ethernet address table

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Ethernet Filters from the Ethernet menu.
3. Click Address Table. The Address Table screen appears.

4. Enter up to 20 MAC addresses. When you are finished, click Submit Changes to save your changes.

Using Frame Type Filters

You can establish filters for common networking protocols such as IP, Novell IPX, and 802.2 LLC. You can also set filters to pass only those Ethernet frame types found on your network.

You can set the default action for general and specific frame types. For example, you can set the DIX-Other EtherTypes frame parameter to drop, and then use the subtype menus to pass only those specific DIX types that are used in your radio network.

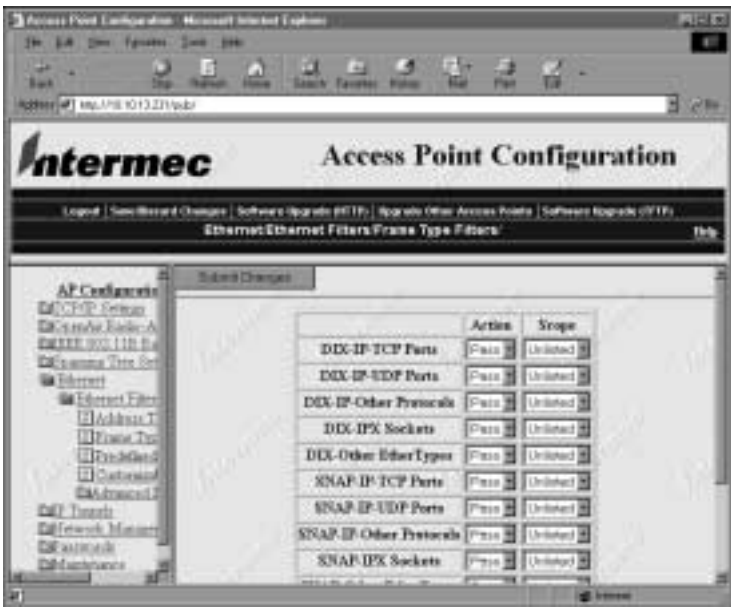
You can also set the scope for general and specific frame types. For example, you can set the action to Drop and the scope to All for DIX-IP-TCP Ports, and then all IP packets with the TCP protocol type will be dropped even if specific TCP parts are set to pass in the subtype menus.

Action Set the action so the UAP will either Pass or drop all frames of a specified type.

Scope Can be set to Unlisted or All. If you select All, then all frames of that type are unconditionally passed or dropped, depending on 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.

To set frame type filters

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Ethernet, and then click Ethernet Filters. The Ethernet screen appears.
3. Click Frame Type Filters. The Ethernet Frame Type Filters screen appears.



4. Set the action and scope for any particular frames. When you are finished, click Submit Changes to save your changes.

   The following table explains various frame types.

Frame Type	Explanation
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.
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 subtree rooted at the local UAP.

Using Predefined Subtype Filters

You can set filters on certain frame subtypes by setting the action, subtype, and Value of the filter.

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.

To set predefined subtype filters

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Ethernet, and then click Ethernet Filters. The Ethernet screen appears.
3. Click Predefined Subtype Filters. The Ethernet Predefined Subtype Filters screen appears.

The Ethernet Predefined Subtype Filters Screen

4. Set the action for any filters you want to change. When you are finished, click Submit Changes to save your changes.

Using Customizable Subtype Filters

You can define the action, subtype, and Value parameters in customized filters.

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

Subtype Selects the frame subtype you wish to filter.

Value Refer to the following table for the value for a specific subtype. The value must be two hex pairs. You must enter port values as decimals; for example enter “23.” for port 23. The UAP displays the hexadecimal equivalent in the value 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.
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.

To set customized subtype filters

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Ethernet, and then click Ethernet Filters. The Ethernet screen appears.
3. Click Customizable Subtype Filters. The Ethernet Customizable Subtype Filters screen appears.

The Ethernet Customizable Subtype Filters Screen

4. Configure each parameter to the desired values. When you are finished, click Submit Changes to save your changes.

Configuring Advanced Filters

You can use advanced filters if you need more flexibility in your filtering. 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 earlier filters dropped the frame, 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 filters if you have an extensive understanding of network frames and their contents. You should use other existing filters whenever possible.

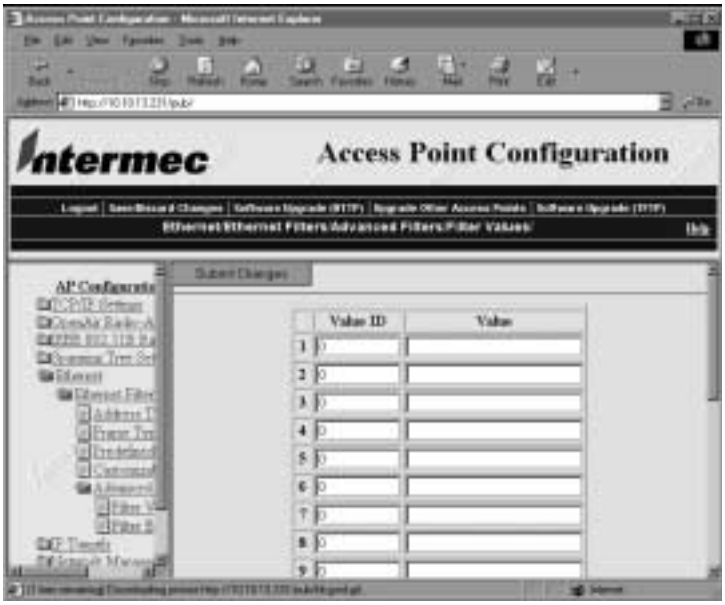
Setting Filter Values

You can associate an ID with a pattern value by selecting a filter and then entering an ID and a value. All values with the same value ID belong to the same list.

To set the value ID and value

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Ethernet, and then click Ethernet Filters. The Ethernet screen appears.

3. Click Advanced Filters, and then click Filter Values. The Filter Values screen appears.



4. Enter up to 22 value IDs and values. When you are finished, click Submit Changes to save your changes.

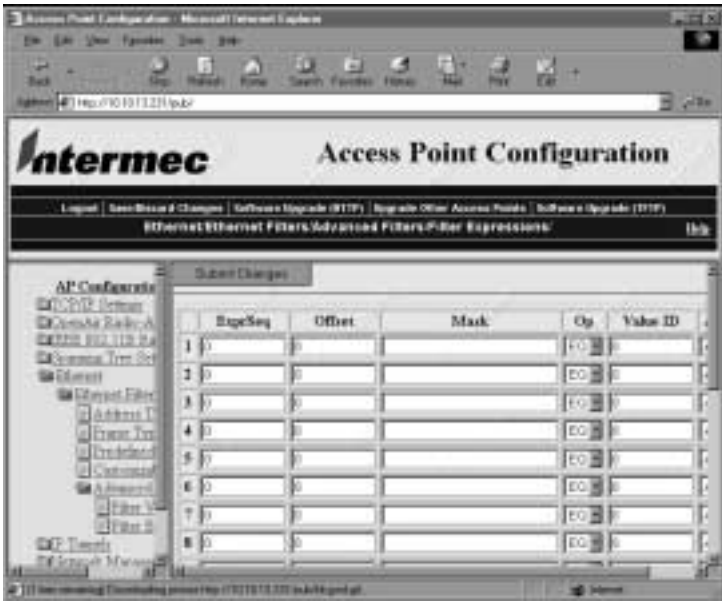
Setting Filter Expressions

You can set filter expressions by specifying parameters for packet filters. You can also create a filter expression, which is executed in ascending order based on the ExprSeq values until the UAP determines whether to pass or drop the frame.

To set filter expressions

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Ethernet, and then click Ethernet Filters. The Ethernet Filters screen appears.
3. Click Advanced Filters, and then click Filter Expressions. The Filter Expressions screen appears.

The Filter Expressions Screen



4. Configure the Filter Expressions parameters. When you are finished, click Submit Changes to save your changes.

   The next table explains each parameter.

Parameter	Explanation
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 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 Offset to identify a point inside a bracket where testing for the expression is to start. Offset values 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 specific 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.

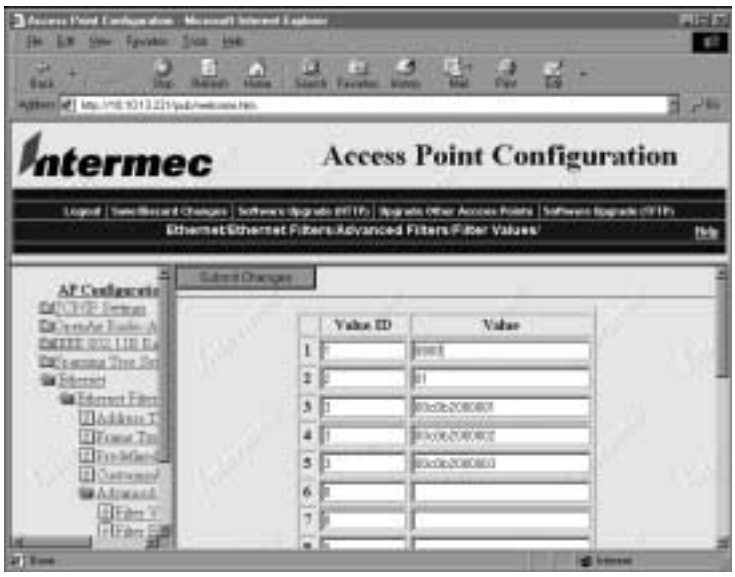
The ExprSeq Parameters Table (continued)

Parameter	Explanation
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, the filter expression with the next highest sequence is applied.

Ethernet Advanced Filter Example

The following example shows how to use Ethernet Advanced Filters to discard all DIX IP multicast frames except those from a selected list of Ethernet stations.

Set the following filter values for this example.

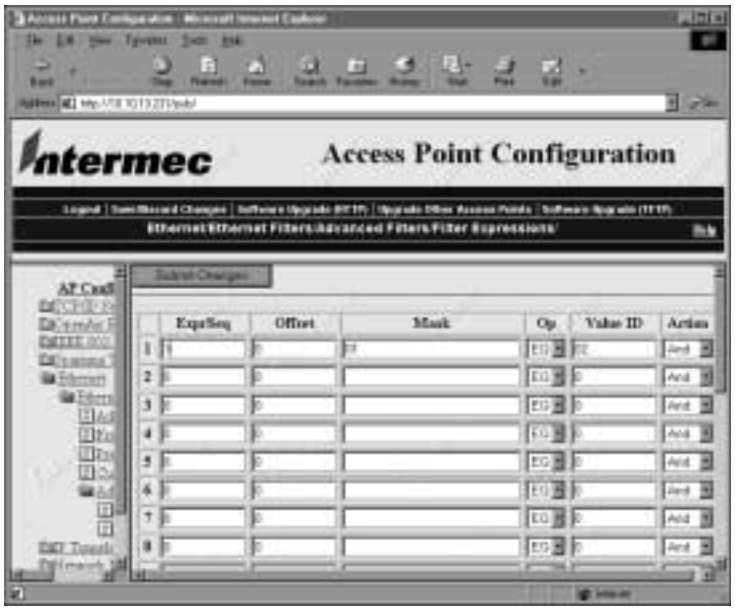


Three value entries have the same value ID of 3 to demonstrate how to enter a list. All entries with the same value ID belong to the same list.

The following table explains the values used in the Filter Values.

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.

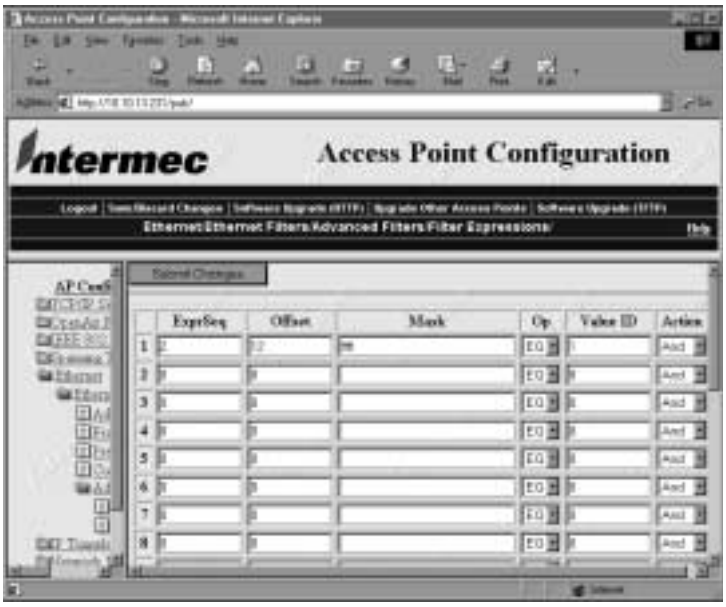
Set the first filter expression as shown below.



The following table explains the values used in 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.

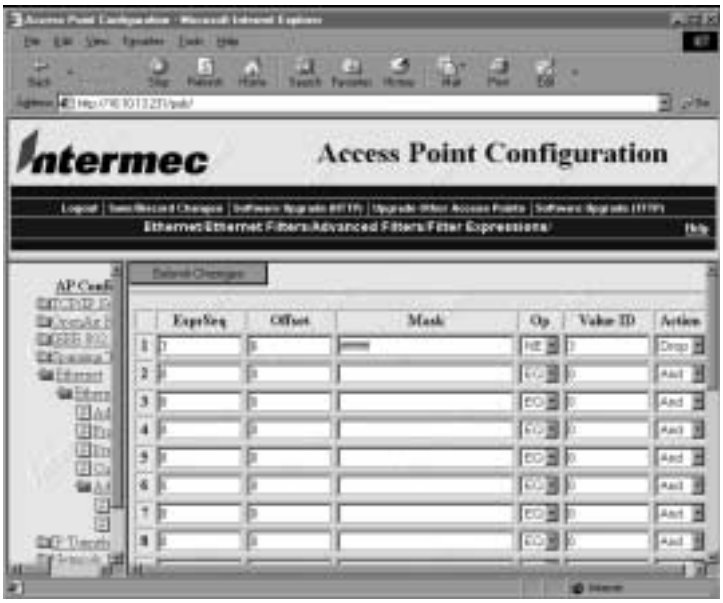
Set the second filter expression as shown below.



The following table explains the values used in the second filter expression.

Parameter	Value	Explanation
ExprSeq	2	This is the second expression.
Offset	12	The data for this express 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 on 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.

Set the third filter expression as shown below.



The following table explains the values used in 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.

Configuring IP Tunnel Filters

You can set both Ethernet and IP tunnel filters, and you can create protocol filters for both predefined and user-defined protocol types. In addition, you can define arbitrary frame filters based on frame content.

Configuring IP Multicast

Configure IP Multicast to determine if the root will send IP multicast packets through its IP tunnels. You can set IP Multicast to either pass or drop IP multicast packets.

To configure IP Multicast

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IP Tunnels, and then click Tunnel Filters. The Tunnel Filters screen appears.

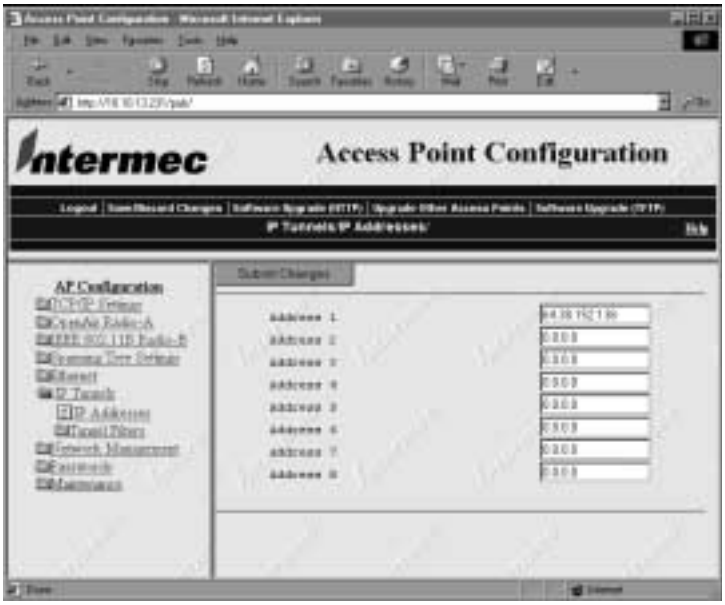
3. Click the IP Multicast down arrow and choose Drop or Pass. When you are finished, click Submit Changes to save your changes.

Configuring IP Addresses

You can define an IP address for which the access point can originate tunnels if it is functioning as the root for the network. The tunnel can be configured using a class D multicast IP address. Intermec's default is 224.0.1.65.

To configure IP addresses

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IP Tunnels, and then click IP Addresses. The IP Addresses screen appears.



3. Enter up to 8 IP addresses. When you are finished, click Submit Changes to save your changes.

Using Frame Type Filters

Permanent IP output port filters prevent unwanted frame forwarding through an 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
- 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 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 IP tunnel unless the destination belongs to the home subnet.

You can set action and scope.

Action Passes or drops that type of frame.

Scope Sets the scope of the filter.

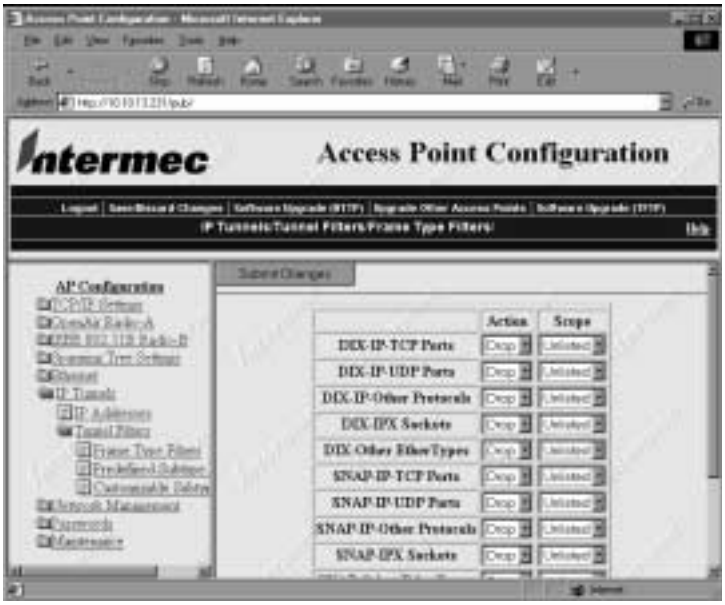
All All frames of that type are filtered.

Unlisted Frames of that type are filtered only if they are not in the predefined or customizable IP tables.

To set frame type filters

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IP Tunnels, and then click Tunnel Filters. The Tunnel Filters screen appears.
3. Click Frame Type Filters. The Frame Type Filters screen appears.

The Frame Type Filters Screen



4. Set the action and scope for any particular frames. When you are finished, click Submit Changes to save your changes.

Using Predefined Subtype Filters

You can set filters on certain frame subtypes by setting the action, subtype, and value of the filter.

Action Passes or drops all frames of that type.

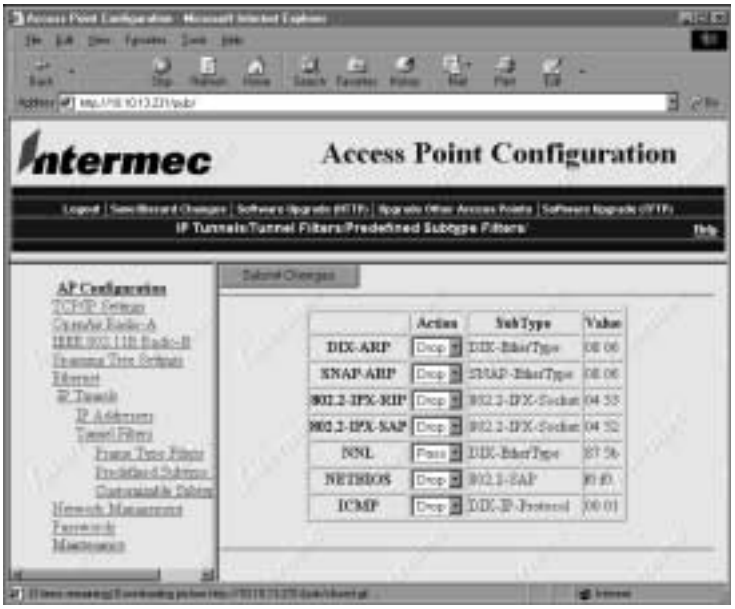
Subtype Displays the frame subtype.

Value Provides information about the subtype value.

To set predefined subtype filters

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IP Tunnels, and then click Tunnel Filters. The Tunnel Filters screen appears.
3. Click Predefined Subtype Filters. The Predefined Subtype Filters screen appears.

The Predefined Subtype Filters Screen



4. Set the action for any filters you want to change. When you are finished, click Submit Changes to save your changes.

Using Customizable Subtype Filters

You can define the action, subtype, and value parameters in customized filters.

Action Passes or drops all frames of that type.

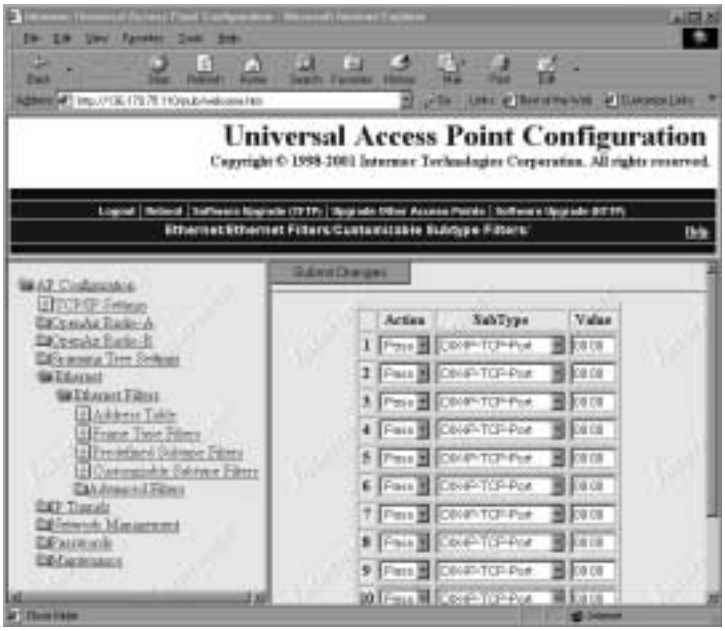
Subtype Selects the frame subtype you wish to filter.

Value Specifies the value of the subtype. Refer to the following table for the value for a specific subtype. The value must be two hex pairs. You must enter port values as decimals; for example enter “23.” for port 23. The UAP displays the hexadecimal equivalent in the Value field on the menu. When a match is found between frame subtype and value, the specified action is taken.

To set customized subtype filters

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IP Tunnels, and then click Tunnel Filters. The IP Tunnels/Tunnel Filters screen appears.
3. Click Customizable Subtype Filters. The Customizable Subtype Filters screen appears.

The Customizable Subtype Filters Screen



4. Configure each parameter to the desired values. When you are finished, click Submit Changes to save your changes.

   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.
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.

Creating IP Tunnels

For more information, see Appendix B, “Understanding IP.”

To create an IP tunnel

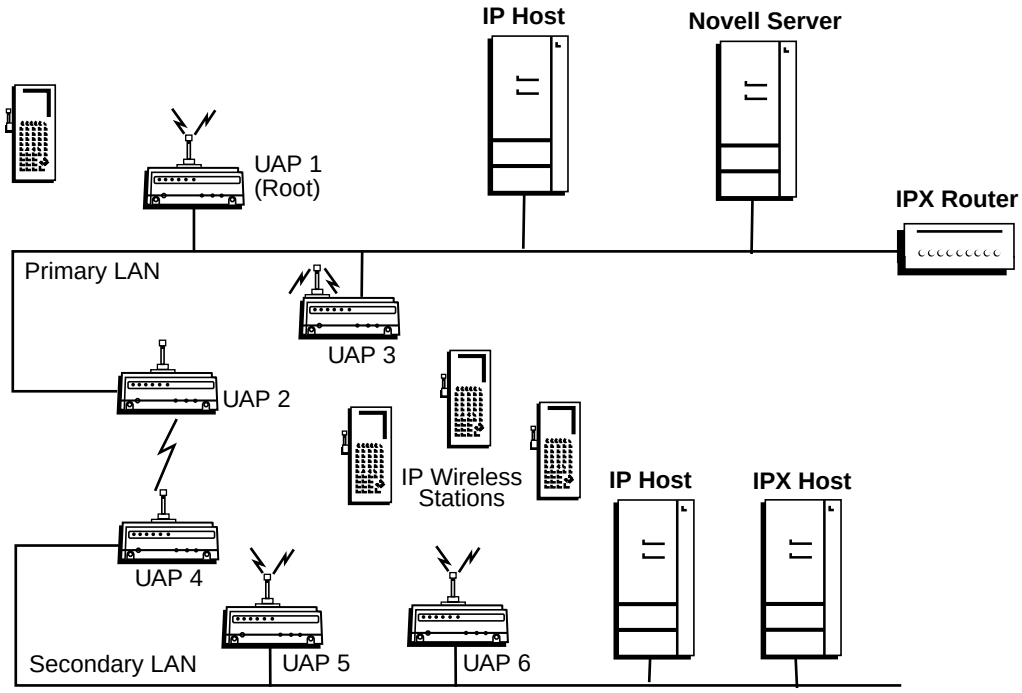
1. Configure the root UAP to originate the tunnel.
2. Specify the IP addresses of the UAPs that will listen at the other end of each tunnel.

IP Tunnel Filter Examples

The next examples 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.



21XXT027.eps

Example 1

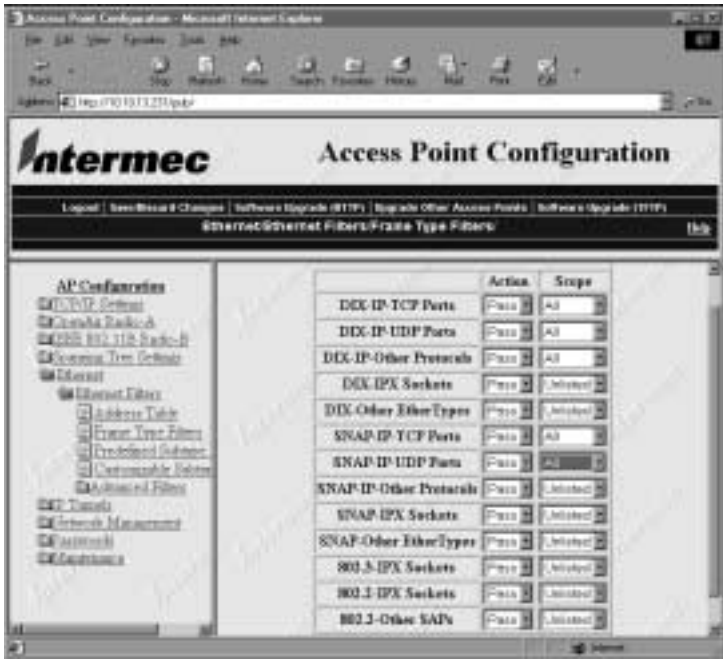
UAPs 1, 3, 5, and 6 service only IP end devices. These UAPs need to pass IP traffic, but eliminate IPX traffic that does not need to be forwarded to the primary or secondary LAN. Filter the IPX frames in the Ethernet Frame Type Filter table. No subtype filters are needed.

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.

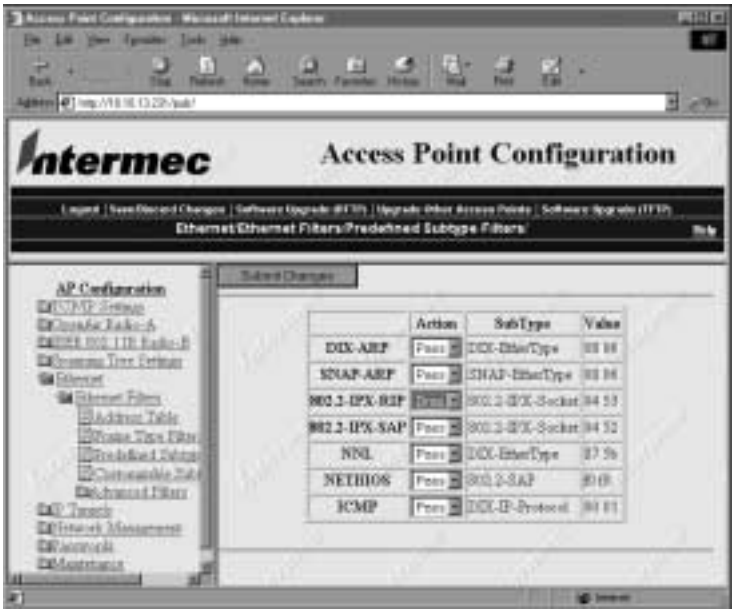
To filter the IPX RIP frames, you need to configure subtype filters. This example sets filters for three different cases: DIX, 802.2, and 802.3 SNAP frames. In many actual networks, only one type of filter is required because all stations are configured using one of the three options.

For this example, set the following options in the Ethernet Frame Type Filters screen.

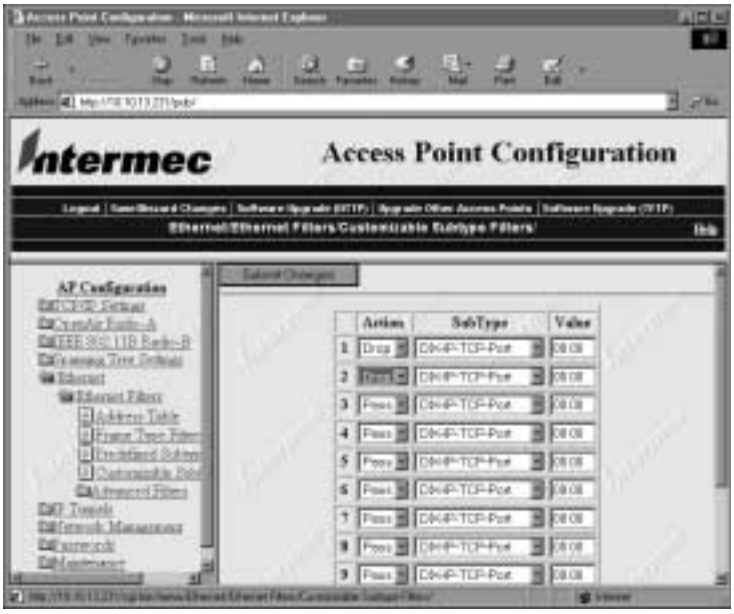


You need to use subtype filters to drop IPX RIP for 802.2, DIX, and 802.3 frames. Use the settings shown next on the Ethernet Predefined Subtype Filter table to filter IPX RIP for 802.2 frames.

Settings for Ethernet Filter Example 2



Use the settings shown next on the Ethernet Customizable Subtype Filter table to filter DIX-IPX for 802.3 IPX.



Example 3

If you have a Windows NT server and want to use DHCP for automatic address assignment for an end device on a remote subnet, you need to set the following filters to allow for the necessary IP tunneling. See "Configuring Ethernet Filters" and "Configuring IP Tunnel Filters" for information about how to configure these settings.

1. On the UAP that originates the tunnel, set
   - IP Multicast to Pass.
   - DIX-IP-UDP Ports to Pass All in the IP Tunnel Frame Type Filter table.
2. On the UAP that terminates the tunnel, set
   - DIX-IP-UDP Ports to Pass All in the IP Tunnel Frame Type Filter table.

Example 4

If you have a Linux or Unix DHCP server and want to use DHCP for automatic address assignment for an end device on a remote subnet, set DIX-IP-UDP Port to Pass All in the IP Tunnel Frame Type Filter table.

Configuring Mode

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

To configure Mode

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click IP Tunnels. The IP Tunnels screen appears.
3. Click the Mode down arrow and choose Listen or Originate If Root.

   Listen 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 IP tunnels if it is functioning as the root for the network.

   When you are finished, click Submit Changes to save your changes.

Configuring IGMP

Internet Group Management Protocol (IGMP) lets you establish multiple IP tunnels using a single multicast IP address. If you enable IGMP, the root UAP uses a Class D IP multicast address to send IP Hello packets through routers to UAPs on other IP subnets.

Enabling IGMP on remote IP subnets causes intermediate IP routers to forward the IP hello packets to those subnets. Using IP multicast and IGMP for IP Hello packets has these advantages:

- Allows you to establish multiple tunnels with a single address.
- Causes IP Hello packets to be forwarded only to those IP subnets that participate in the multicast group.
- Increases redundancy because multiple UAPs on a remote subnet can receive IP Hello packets.

To configure IGMP

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click IP Tunnels. The IP Tunnels screen appears.
3. Click the IGMP down arrow and choose Enabled or Disabled.

   Enabled Causes the root UAP to use a Class D IP multicast address to send IP Hello packets through routers to UAPs on other IP subnets.

   Disabled Causes the root UAP not to use a Class D IP multicast address to send IP Hello packets through routers to UAPs on other IP subnets.

   When you are finished, click Submit Changes to save your changes.

6

Troubleshooting and Maintaining the 21XX UAP

This chapter explains how to upgrade the 21XX UAP firmware. This chapter also explains how to troubleshoot and maintain the 21XX UAP.

Analyzing the 21XX UAP

You can view different parameters configured for the 21XX UAP, including port statistics, connections, and a configuration summary. The information on these screens may be needed when you call Intermec Technical Support.

Viewing AP Connections

AP Connections shows information about the devices in the spanning subtree.

To view AP connections

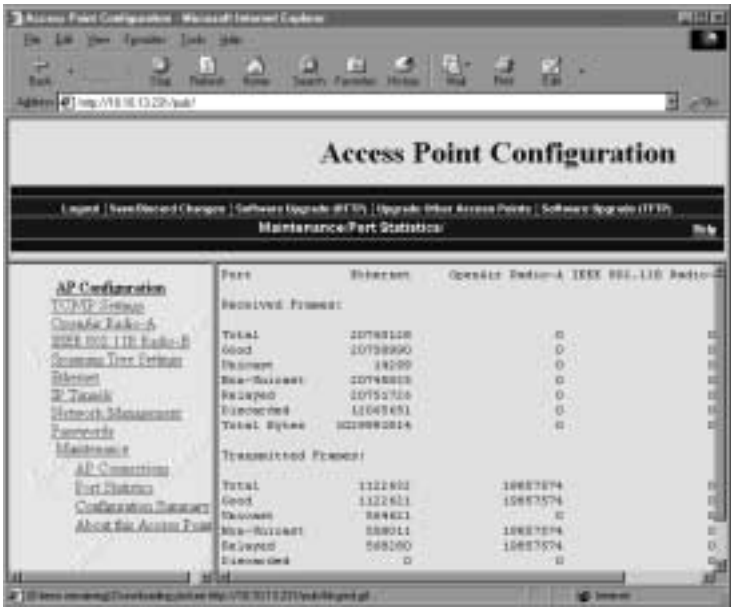
1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Maintenance.
3. Click AP Connections. The read-only AP Connections screen appears.

Viewing Port Statistics

The Port Statistics screen shows the total number of frames and bytes that the access point has transmitted and received since it was last booted.

To view port statistics

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Maintenance.
3. Click Port Statistics. The read-only Port Statistics screen appears.



Viewing the Configuration Summary

Configuration Summary summarizes the major configuration settings and installed hardware for the access point.

To view the configuration summary

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Maintenance.
3. Click Configuration Summary. The read-only Configuration Summary screen appears listing each parameter in the access point and its current configuration.

The Configuration Summary Screen

Viewing Information About the UAP

About this Access Point shows information about the UAP including software versions, radio versions, and MAC addresses.

To view About this Access Point

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Maintenance.
3. Click About this Access Point. The read-only About this Access Point screen appears.

The About this Access Point Screen

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.

Power	Wireless #1	Wireless #2	Wired LAN	Root/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	Monitor loading 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 the UAP is configured as the root

Upgrading the 21XX UAP Firmware

For optimal performance, you should install the most current firmware version on all the UAPs in your network. Firmware releases are available from the Product Support Page on the Intermec Web site.

You can install the firmware release using

- a Web browser session. For more information, see "Using a Web Browser," in the next section.
- a serial connection. For more information, see "Using a Serial Connection" on page 6-10.
- a TFTP transfer via a Telnet session. For more information, see "Using a TFTP Transfer" on page 6-12.

Using a Web Browser

To upgrade the firmware using a Web browser session, you must first install the firmware release on your PC, and then upload the release to your UAP. For more information, see the release notes that accompany the firmware release.

To install the firmware release on your PC

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Navigate to http://corp.intermec.com/prodsupp/dloadsndex.htm and click Software: Applications and Examples.
3. Choose the latest firmware release from the list of available software downloads.

After you have the installed the firmware release on your PC, use the Web browser interface to upload the file from your PC to the access point.

You can choose to upload the file using one of the following Web methods:

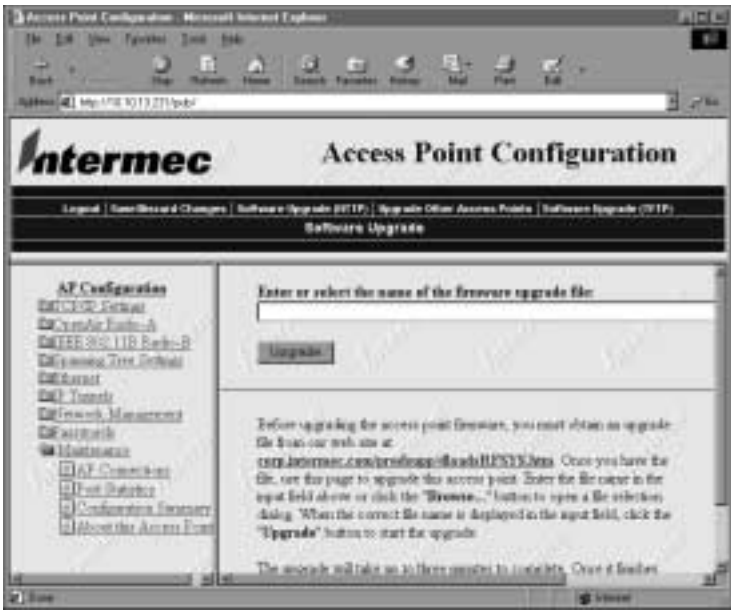
- HTTP
- TFTP

You must have a TFTP server installed to use the TFTP upgrade option.

In addition, you can upload the files using a communications program.

To upload the firmware release using HTTP

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click Software Upgrade (HTTP). The Software Upgrade screen appears.



3. Enter the name of the upgrade file, or click the Browse button to find the file.
4. Click Upgrade to start the upgrade. The upgrade may take up to three minutes to complete.
5. When the upgrade is complete, reboot the access point to activate the new firmware.

To upload the firmware release using TFTP

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click Software Upgrade (TFTP). The Software Upgrade screen appears.

The Software Upgrade Screen

3. Click Automated Software Download. The Automated Software Download screen appears.

4. Configure the following parameters:

Server IP Address	The IP address of your TFTP server.
Script File Name	The location of the upgrade script file on the TFTP server.
Start Time	The time the upgrade should start.

5. Click Start. The upgrade will start when the Start Time expires. The UAP reboots when the upgrade is complete.

   If the upgrade is unsuccessful, the TFTP server prints an error message. When you have corrected the problem, repeat steps 2 through 5.

6. Click Maintenance, and then click About this Access Point to verify the new firmware versions.

Using a Serial Connection

To upgrade the firmware using a serial connection, you must have the firmware release files on your PC and have an RS-232 null-modem cable connecting the UAP to your PC. For more information, see the release notes that accompany the firmware upgrade.

To upgrade the firmware using a serial connection

1. Configure the following communications parameters on your PC:

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

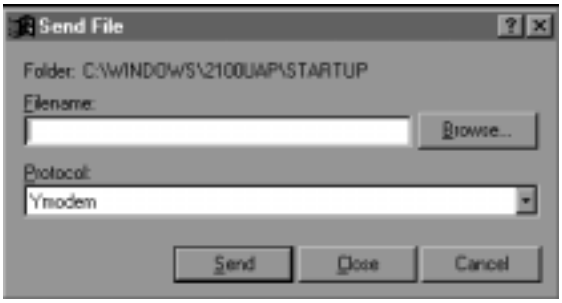
2. Reboot the UAP and enter the UAP monitor by pressing any key when asked. The UAP prompt (uap>) appears.
3. Type `srvc` and press **Enter**.
4. Type the service password. The default password is `EV98203S` (case-sensitive). The service prompt (service>) appears.
5. Type `fd` and press **Enter**. The file directory appears.
6. 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

7. Identify the startup and data segments for this startup—these are the current segments. In this example, the active startup segment is 1, and the active data segment is 3.

You will first erase the inactive segments, and then you will load the new firmware into the inactive segments and make those segments active. In this example, the inactive segments are 2 and 4.

8. Erase the inactive startup segment. Type `fe 2` at the service prompt and press **Enter**. A 'P' appears when the segment is erased.
9. Erase the inactive data segment. Type `fe 4` at the service prompt and press **Enter**. A 'P' appears when the segment is erased.
10. Transfer the startup files to the inactive startup segment.
    a. At the service prompt, type `fx s` (where *s* is the inactive startup segment), and press **Enter**. A series of Cs appears on your screen.
    b. Click Transfer, and then click Send File. The Send File dialog box appears.



    c. Click the Protocol down arrow and choose Ymodem.
    d. Browse to the location where UAP.DNL is saved. Double-click this file. The file name appears in the Filename field.
    e. Click Send to start the file transfer. A 'P' appears when the transfer is complete.
11. Transfer the data files to the inactive data segment.
    a. At the service prompt, type `fx s` (where *s* is the inactive data segment), and press **Enter**. A series of Cs appears on your screen.
    b. Click Transfer, and then click Send File. The Send File dialog box appears.
    c. Browse to the location where the data files are saved. Double-click any data file. This file name appears in the Filename field.
    d. To transfer all the data files at once, replace the specific file name with an asterisk (*). For example, if the file name is c:\21xxuap\data\applets.dnl, change it to c:\21xxuap\data*.dnl.
    e. Click Send to start the file transfer. A 'P' appears when the transfer is complete.
12. Activate the inactive startup segment by typing `fb s` (where *s* is the inactive startup segment) at the service prompt and pressing **Enter**. A 'P' appears when the operation is complete.

13. Activate the inactive data segment by typing `fb s` (where *s* is the inactive data segment) at the service prompt and pressing **Enter**. A 'P' appears when the operation is complete.
14. Repeat steps 10 through 13 for the second startup file, uapboot.dnl.
15. Type `x` at the service prompt to return to the uap prompt.
16. To reboot the UAP, type `b` and press **Enter**.
17. Reconfigure the UAP for your installation, if necessary, and save the configuration. To activate the configuration, reboot the UAP.

Using a TFTP Transfer

To upgrade the firmware using a TFTP transfer, you must have a TFTP server installed. When you execute the script file, UPGRADE.DNL, that is included with the firmware release, a TFTP transfer copies all the startup and data files to the UAP. For more information, see the release notes that accompany the firmware upgrade.

To upgrade the firmware using a TFTP transfer

1. Start your TFTP server.
2. Establish a Telnet session with the UAP.
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 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 time; 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 computer reaches zero, the upgrade begins. The UAP reboots after the upgrade is complete.

Upgrading Other UAPs

After you have upgraded the root UAP, you can upgrade the other UAPs in your network.

Note: You MUST perform the Upgrade Other UAPs from the root UAP.

To upgrade other UAPs

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Upgrade Other Access Points. The Network Software Upgrade screen appears.

3. Click the check box next to each UAP you want to upgrade to select, or click Select All Access Points to select all of your UAPs.
4. Click the Now down arrow and select a time to start the upgrade. You can choose to start the upgrade immediately or you can delay the start of the upgrade one to twelve hours.
5. Click the From this UAP down arrow and select the source for the upgrade. You can choose to use the version that the root access point is currently running, or you can use a backup copy.
6. Click the Upgrade UAPs down arrow and select the access points that will be rebooted after the upgrade is complete. You can choose to reboot only the upgraded UAPs, or you can choose to upgrade all the UAPs.
7. Click Start Upgrade. The upgrade starts at the time you specified.

Each UAP on a wired LAN requires approximately three minutes to upgrade (slightly longer for wireless UAPs). The browser screen updates every 30 seconds as the upgrade progresses and shows the final status when all upgrades are complete. If you selected Reboot All Access Points, the browser disconnects. Press Refresh on your browser to log in again.

Errors may occur during the upgrade or during the final reboot. If an error occurs, an explanation appears on the browser screen.

If an error occurs during the upgrade, none of the access points reboot. You should

1. recheck the UAPs where the error occurred.
2. press Start Upgrade to attempt the upgrade again.

If the upgrade is successful, the UAPs will reboot according to your Reboot selection.

If an error occurs during reboot, you should

1. wait five minutes for the access points that did not reboot to refresh.
2. refresh your browser screen and check the access points that are not running the new version.
3. Press Start Upgrade to attempt the upgrade again.

If the upgrade is successful, the UAPs will reboot according to your Reboot selection.

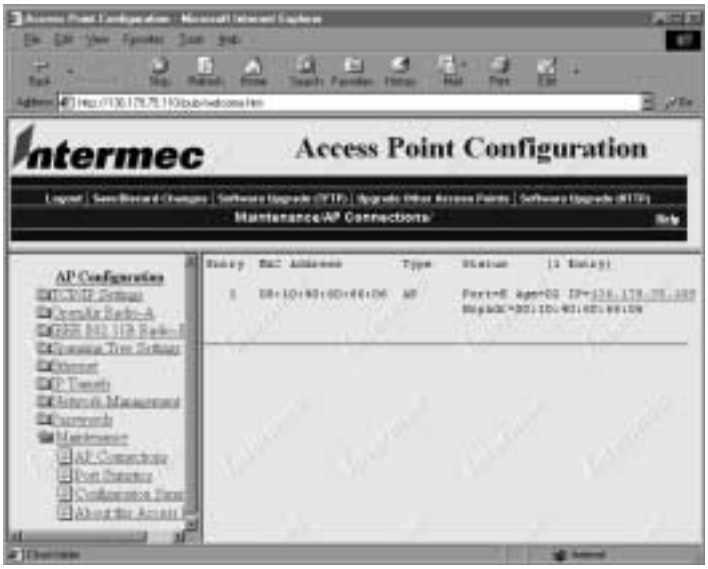
Using Radio MAC Ping

Use Radio MAC Ping to determine the connectivity and signal strength of an 802.11b HR terminal by pinging 802.11b HR terminals that are attached to an access point. Radio MAC Ping runs at the MAC layer, allowing you to ping a device that does not have an IP address.

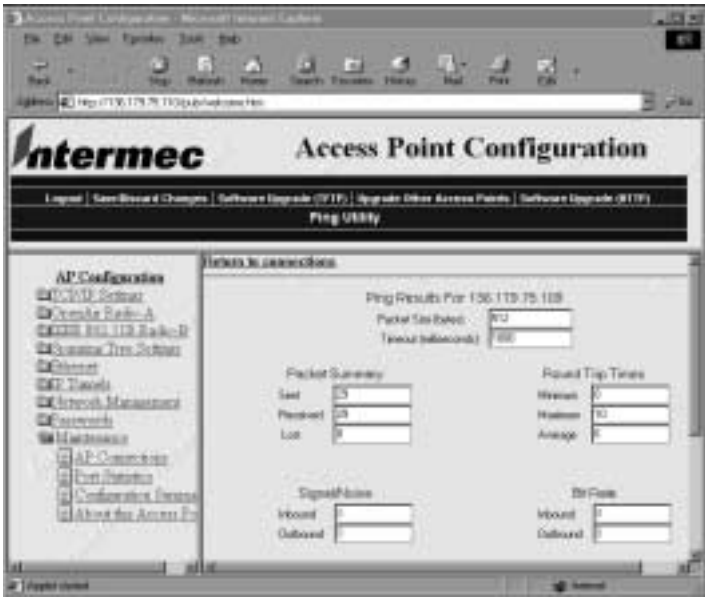
To configure radio MAC ping

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Maintenance. The AP Connections screen appears.

The AP Connections Screen



3. Click the MAC address link in the AP Connections screen. The Ping Utility screen appears showing the results of the ping.



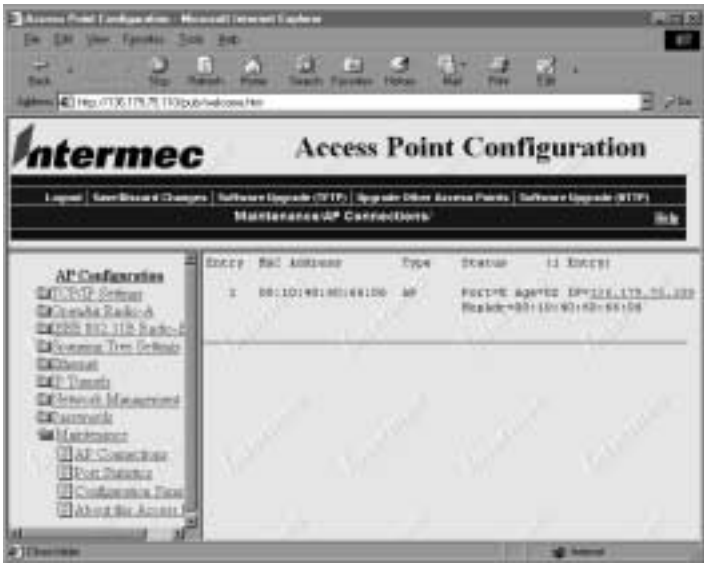
When you are finished viewing the ping results, click Return to connections to return to the AP Connections screen.

Using ICMP Echo

Use ICMP Echo to ping devices using the access point Connections screen. ICMP Echo can be use if the access point has determined the IP address of a client or another access point. If the ARP server is enabled, the access point will determine the IP addresses of the radio clients attached to it and allow you the option of using ICMP Echo on the radio network. The access point always knows the IP address of all access points in the spanning tree.

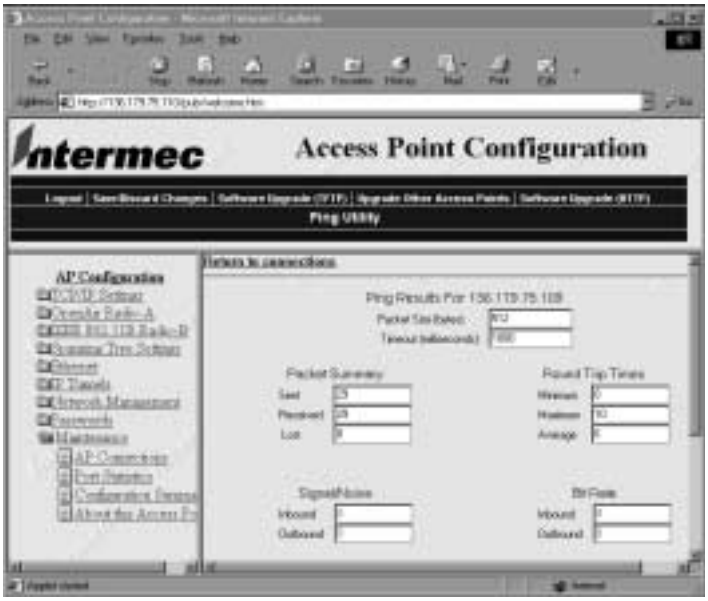
To configure ICMP Echo

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Maintenance. The AP Connections screen appears.



3. Click the IP address link in the AP Connections screen. The Ping Utility screen appears showing the results of the ping.

The Ping Utility Screen



When you are finished viewing the ping results, click Return to connections to return to the AP Connections screen.

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 community table are shown below.

Type of Access	MIB Password
read only	public
read/write	CR52401

Configuring the SNMP Community

Simple Network Management Protocol (SNMP) community strings are passwords used by SNMP. When you use an SNMP client, you must enter the correct community string to gain access to the UAP SNMP interface.

To configure the SNMP community

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.

2. Click Network Management, and then click Community Strings. The Community Strings screen appears.

3. Configure the SNMP community parameters. When you are finished, click Submit Changes to save your changes.

   The following table explains the SNMP community parameters.

Parameter	Description
SNMP Read Community	Allows read-only access. Defaults to public.
SNMP Write Community	Allows read/write access. Defaults to CR52401.
SNMP Secret Community	Allows read/write access to change the community strings. Defaults to Secret.

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 a serial connection, an error message also appears on your terminal or PC. The error messages are described in the following table.

In the 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 radio installed	When this error message appears, additional information also appears on the screen; for example, "Expected 504,000 but found 491 in slot A, nothing in slot B" may appear. The radio may be faulty. Contact your Intermec representative.

Commonly Asked Technical Support Questions

Problem/Question	Possible Solution/Answer
Is the UAP fully booted?	When the UAP is fully booted, the Power LED remains steady green and the Wired LAN LED flashes.
The Power LED is not on.	The UAP may have a hardware problem. 1. Make sure the power cable is firmly plugged into the UAP and the power source. 2. Unplug the UAP, and then plug it back into the power source. Verify that the Power LED remains on. 3. Call Intermec Technical Support.
You 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 your 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.
You cannot ping or Telnet to a new UAP.	You must set an IP address and subnet mask using the serial port before you can remotely connect to the UAP.
You cannot connect to the UAP using a Web browser.	If you access the Internet through a proxy server, be sure you have added the IP address of the UAP to the Exceptions list.

Commonly Asked Technical Support Questions (continued)

Problem/Question	Possible Solution/Answer
The end device cannot connect to the network.	• Choose AP Connections from the Maintenance menu and verify that the MAC address of your end device appears on your PC screen. If it does not appear, your device is not communicating with the UAP. Check your radio configuration settings. • Verify that 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 802.11b HR radios: • Verify that the end device and the UAP have the same frequency and network name. 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 that the end device is configured as a station. If you are using 900 MHz radios: • Verify that the end device and the UAP have the same LAN ID and mode-channel. If you are using S-UHF radios: • Verify that the end device and the UAP have the same frequency.
The end devices are unable to roam between 21XX and 011X devices.	Set the Unicast Flood Mode to Hierarchical. For more information, see "Configuring Global Flooding" on page 3-17.
The 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 switches in your network do not support backward learning, you can create a data link tunnel to force all radio traffic through a fixed point so that roaming is transparent to the bridges or switches. **To create a data link tunnel** 1. Set Ethernet Bridging to Enable on the root UAP 2. Set Ethernet Bridging to Disabled on all UAPs that are separated from the root by a bridge or switch that does not support backward learning. For more information, see Chapter 5, "Configuring Filters and Tunnels."

Commonly Asked Technical Support Questions (continued)

Problem/Question	Possible Solution/Answer
The filters are not filtering properly.	Check all of your filter settings. Conflicts may exist between the various filters.
You need to verify the WEP keys.	You cannot verify the WEP keys. The keys are encrypted after you enter them and are never displayed again. You may need to reconfigure your UAPs and end devices to reset the WEP keys.
You need to confirm which master a WAP is connected to.	To verify that a WAP is communicating with a particular UAP, view the AP Connections screen for the UAP. Click Maintenance, and then click AP Connections.
You cannot establish an IP tunnel to a UAP on a remote subnet.	1. Click TCP/IP Settings and verify that the IP Router (Gateway) address is correct. 2. Click Spanning Tree Settings and verify that the UAPs on both ends of the tunnel have the same LAN ID. 3. Click IP Addresses from the IP Tunnels menu to verify that the IP address of the remote UAP appears in the IP Addresses list.
The throughput seems slow.	• Verify that your antennas are well placed and that they are not blocked by metal or other obstacles. • You may want to add a second UAP and implement roaming if you move the antenna closer to the device and throughput increases. You may be able to set filters to eliminate Ethernet traffic on the wireless side of the network. For more information about filters, see Chapter 5, "Configuring Filters and Tunnels."

Getting Help with Your Installation

The 21XX UAP is designed to be easy to install and configure; however, you may need to call Intermec Technical Support if you have problems. Before calling, 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?

To confirm the firmware version on your UAP

1. Establish a Web browser session if you have not already done so. For more information, see “Establishing a Web Browser Session” on page 2-20.
2. Click Maintenance, and then click About this Access Point. The About this Access Point screen appears.

You should have the information on this screen available when you call Intermec Technical Support.

In the United States, call Intermec Technical Support at 1-800-755-5505. In Canada, call 1-800-668-7043.

7

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 the following five segments in its file system:

- 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 Chapter 6, "Troubleshooting and Maintaining the 21XX 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 the list of available UAP commands. The commands are not case sensitive; you can type the commands using either upper or lower case.

```
UAP Monitor V4.03 July 17,2000
<Press any key within 5 seconds to enter the UAP monitor>
uap>d
------------------------------------------------------------------------
"uap>" commands...
------------------------------------------------------------------------
B       -Reboot                       |              -Device IDs menu
FX s    -Ymodem File Download         | MR           -Display Mfg Record
FD      -File System Directory        | TEST         -Test Menu
FR      -Run Flash Startup File       | SRVC         -Service Menu
        -Manufacturing Menu           | SR z         -Serial Baud Rate
------------------------------------------------------------------------
uap>
```

B

Purpose: Deletes the most recent data record and remains in Accumulate mode. If no data exists, a null string is entered.

Syntax: `B`

FX

Purpose: Performs a Ymodem batch protocol download of a file into the flash segment that is specified by *s*.

Syntax: `FX` *s*

where *s* is segment 1, 2, 3, or 4.

FD

Purpose: Displays the flash file system directory, including information about the boot file.

Syntax: `FD`

FR

Purpose: 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.

Syntax: `FR`

MR

Purpose: Displays the manufacturing record for the UAP. Use the MR command to display the MAC address, configuration string, and serial number for your UAP.

Syntax: `MR`

SR

Purpose: The SR command sets the baud rate of the UAP.

Syntax: `SR` *z*

where *z* is the 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`.

Setting Autobaud Using the SR Command

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 115,200.

To set Autobaud using SR

1. Set the baud rate to 0 using SR.
2. Press Enter twice. 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

Use service mode to perform certain file functions. Because service mode commands can cause undesirable results if not properly executed, you should contact Intermec Technical Support for assistance if you are unsure about the proper procedure to use.

SRVC

Use the SRVC command to enter service mode. In service mode, you can 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.

```
UAP Monitor V4.03 July 17,2000
Press any key within 5 seconds to enter the UAP monitor>
uap>srvc
Enter password : ********
service>d
------------------------------------------------------------------------
"service>" commands...
------------------------------------------------------------------------
FD        - File System Directory | SU b     - Set Upgrade Byte
FDEL f (s)- File Delete           | RU       - Reset Upgrade Bytes
FE <s|all>- Erase Segment(s)      | DU       - Display Upgrade Bytes
FI        - File System Reset     | PN       - Normal power up
FFR f (s) - Run File              | PQ       - Quiet power up
FX s      - Ymodem File Download  | B        - Reboot
FB bs (ds)- Set Boot/Data Segments| X        - Exit
------------------------------------------------------------------------
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

Purpose: Runs a program that is specified by *f*, from a location specified by *s*.

Syntax: FFR *f* (*s*)

where:

f is the program name.

s is the optional segment location of the program.

Example: To run program UAPBOOT.PRG from segment 1, enter:

```
FFR UAPBOOT.PRG 1
```

PN

Purpose: Returns the UAP to normal mode from quiet mode.

Syntax: 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

Purpose: 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.

Syntax: PQ

Using Test Mode Commands

Within the UAP monitor, test mode allows you to perform certain test functions. Because the commands can cause undesirable results if not properly executed, you should contact Intermec Technical Support for assistance if you are unsure about the proper procedure to use.

TEST

Purpose: Allows you to enter test mode where you can perform a variety of test functions.

Syntax: `TEST`

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.

```
UAP Monitor V4.03 July 17, 2000
<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. 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, 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

Purpose: Use the fb command to make an inactive segment the active segment.

Syntax: `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.

Example: To make segment 2 the active boot segment and segment 4 the active data segment, 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
```

After loading software into the UAP a common task is to activate the new software. To activate the new software, enter:

```
Fb ib: id:
```

This command activates the inactive boot and data segments. You do not need to know which of the boot and data segment numbers the flash is loaded into.

fd

Purpose: Use the fd command to display the flash file system directory, which includes information about the boot file.

Syntax: `fd`

Use the fd command to ensure that the correct version of the file is in the active boot segment.

Typing `fd ab:` shows only the files loaded 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

Purpose: Use the fdel command to delete a particular file name from a segment.

Syntax: `fdel filename`

where *filename* is the name of the file to be deleted.

Example: To delete the file UAP.PRG from the inactive boot segment, 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

Purpose: Erases the files in a particular segment. To recover the files after they have been erased, you must reload them from another source.

Syntax: `fe segment`

where *segment* is the name or number of the segment to be erased.

Example: To erase the contents of segment 1, enter:

```
fe 1
```

You can enter `ALL` instead of a segment name or number if you want to erase segments 1 through 4.

Fe ib: erases the contents of the inactive boot segment.

Note: You must execute the fe command before you execute a TFTP transfer.

script

Purpose: Executes a specified file as a list of console commands. You can create a script file to automate a software download.

Syntax: `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” on page 7-18.

Using Sdvars Commands

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

Purpose: Sets the internal variable called serveripaddress to a specified address.

Format: `sdvars set serveripaddress` *`ip address`*

where *ip address* is the address of the server.

Example: To set the IP address of the server to 192.168.49.29, enter:

```
sdvars set serveripaddress 192.168.49.29
```

sdvars set scriptfilename

Purpose: Sets 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.

Syntax: `sdvars set scriptfilename` *`foreign filename`*

where *foreign filename* is a script filename on the TFTP server.

Example: To set the scriptfilename to SCRIPT.DAT, enter:

```
sdvars set scriptfilename script.dat
```

sdvars set starttime

Purpose: Sets 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.

sdvars set starttime (continued)

Syntax: `sdvars set starttime` *`dd:hh:mm:ss`*

where *dd:hh:mm:ss* is how far in the future the download is to begin.

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

Purpose: Sets 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.

Syntax: `sdvars set checkpoint` *`value`*

where *value* is a whole number.

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

Purpose: Sets 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.

Syntax: `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

Purpose: Sets the 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.

Syntax: `sdvars set setactivepointers` *`none/boot/data/both`*

where:

none does not change the active segments. The default is *none.* 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.

Example: To change the inactive boot and data segments to active at the next reboot, enter:

```
sdvars set setactivepointers both
```

sdvars set nextpoweruptime

Purpose: Sets the 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.

Syntax: `sdvars set nextpoweruptime` *`dd:hh:mm:ss`*

where *dd:hh:mm:ss* is how far in the future the reboot is to begin.

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 is successfully completed. If the first attempt fails, the UAP retries after a one-minute delay. With each successive failure, the retry time doubles until it reaches eight minutes. Once this limit is reached, it remains at eight minutes until the command is completed.

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

Purpose: 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.

Syntax: `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 filename 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 filename is optional. If only the segment name is supplied, the filename is set equal to the filename that is embedded in the file header on the server.

tftp get (continued)

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

Purpose: Copies a file from a client to the server or to another UAP.

Syntax: `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.

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
```

tftp put (continued)

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

Purpose: Your UAP can function as a TFTP server. You can use the TFTP server log command to save a history of TFTP client requests.

Syntax: `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

Purpose: 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. Use the TFTP server start command to enable your UAP to act as a server.

Syntax: `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 four concurrent TFTP sessions.

tftp server stop

Purpose: When you are done transferring files, you can stop the UAP from being a TFTP server by using the TFTP server stop command.

Syntax: `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.
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:

#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
```

A

Specifications

This appendix provides 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	-25°C to +70°C (-13°F to +158°F)
Heater Module (optional)	-30°C to +70°C (-22°F to +158°F)
Storage Temperature	-40°C to +70°C (-40°F to +158°F)
Industrial Sealing	IP 54
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 (3.8 in)
Length	355 mm (14.0 in)
Width	236 mm (9.3 in)

Physical Specifications—2101

Operating Temperature	-20°C to +65°C (-4°F to +149°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	526 g (1.16 lb)
Height	38 mm (1.49 in)
Length	250 mm (9.84 in)
Width	159 mm (6.27 in)

Physical Specifications—2102

Operating Temperature	-20°C to +65°C (-4°F to +149°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	232 g (0.51 lb)
Height	9.32 cm (3.67 in)
Length	14.66 cm (5.77 in)
Width	3.53 cm (1.39 in)

Other Specifications

Architecture	Transparent bridge
Ethernet interfaces	10Base2 (thin coaxial BNC)—2100 only 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 interfaces	SNMP, Web browser-based manager, text-based menu system, serial port, Telnet, Ethernet
Software upgrades	Downloadable over the network or serial port
SNMP agent	Version 1 RFC 1213

Radio Specifications—IEEE 802.11b HR

Data rate	11 Mbps (High), 5.5 Mbps (Medium), 2 Mbps (Standard), 1 Mbps (Low) with automatic fallback for increased range
Channels	11 (North America), 13 (Europe), 4 (France), 1 (Japan)
Range (11 Mbps)	160 m (525 ft) open environment 50 m (165 ft) semi-open environment 24 m (80 ft) closed environment
Frequency band	2.4 to 2.5 GHz world-wide
Radio type	Direct sequence, spread spectrum
Radio power output	32 mW (15dBm)

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 (27dBm) 100 mW (20dBm) (Europe)
2101	100 mW (20dBm)
2102	100 mW (20dBm)

Radio Specifications—900 MHz

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	9,000 to 31,500 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—S-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)

Default Settings

The factory default settings for the UAP are listed in this section. You can record the settings for your installation in each table for reference.

TCP/IP Settings 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 (Gateway)	4 nodes, 0 to 255	0.0.0.0	
IP Frame Type	DIX/SNAP	DIX	
Auto ARP Minutes	0 to 120	5	
ARP Server Mode	Disabled, No Flooding, or Normal Flooding	Disabled	
DHCP Mode	Always, Disabled, Enabled (if 0), or DHCP Server	Always Use DHCP	
DHCP Server Name	0 to 31 characters	(blank)	

Spanning Tree Settings Menu Defaults

Parameter Name	Range	Default	Site Setting
AP Name	0 to 16 characters	(UAP serial number)	
LAN ID (Domain)	0 to 254	0	
Root Priority	0 to 7	1	
IAPP Frame Type	DIX/SNAP	DIX	
Ethernet Bridging	Enabled/Disabled	Enabled	
Secondary LAN Bridge Priority	0 to 7	0	

Global Flooding Menu Defaults

Parameter Name	Range	Default	Site Setting
Multicast Flood Mode	Universal, Hierarchical, or Disabled	Disabled	
Multicast Outbound to Terminals	Enabled/Disabled	Enabled	
Multicast Outbound to Secondary LANs	Enabled/Set Locally	Set Locally	
Unicast Flood Mode	Universal, Hierarchical, or Disabled	Disabled	

Global RF Parameters Menu Defaults

Parameter Name	Range	Default	Site Setting
RFC1042/DIX Conversion	Enabled/Disabled	Enabled	
S-UHF Rfp Threshold			
Set Globally	Enabled/Disabled	Disabled	
Value			
S-UHF Frag Size			
Set Globally	Enabled/Disabled	Disabled	
Value			
900 MHz Frag Size			
Set Globally	Enabled/Disabled	Disabled	
Value			
S-UHF/900 MHz Awake Time			
Set Globally	Enabled/Disabled	Disabled	
Value			
RFC1042 Types to Pass Through			
1 through 20			

Ethernet Port Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Hello Period	1, 2, or 3 seconds	2	

Ethernet Filters Menu Defaults

Parameter Name	Range	Default	Site Setting
Address Table		00:00:00:00:00:00	
Frame Type Filters			
Action	Pass/Drop	Pass	
Scope	Unlisted/All	Unlisted	
Predefined Subtype Filters			
Action	Pass/Drop	Pass	
Customizable Subtype Filters			
Action	Pass/Drop	Pass	
SubType	DIX-IP-TCP-Port, DIX-IP-UDP-Port, DIX-IP-Protocol, DIX-IPX-Socket, DIX-EtherType, SNAP-IP-TCP-Port, SNAP -IP-UDP-Port, SNAP -IP-Protocol, SNAP -IPX-Socket, SNAP -EtherType, 802.3-IPX-Socket, 802.2 -IPX-Socket, or 802.2-SAP	DIX-IP-TCP-Port	

Advanced Filters Menu Defaults

Parameter Name	Range	Default	Site Setting
Filter Values			
Value ID		0	
Value		(blank)	
Filter Expressions			
ExprSeq		0	
Offset		0	
Mask		(blank)	
Op	EQ, NE, GT, or LE	EQ	
Value ID		0	
Action	And, Pass, or Drop	And	

IP Tunnels Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Mode	Listen/Originate If Root	Originate If Root	
IGMP	Enabled/Disabled	Disabled	
Hello Period	1, 2, or 3 Seconds	2 Seconds	
IP Addresses	4 nodes, 0 to 255	0.0.0.0	

Tunnel Filters Menu Defaults

Parameter Name	Range	Default	Site Setting
IP Multicast	Pass/Drop	Drop	
Frame Type Filters			
Action	Pass/Drop	Pass	
Scope	Unlisted/All	Unlisted	
Predefined Subtype Filters			
Action	Pass/Drop	Pass	
Customizable Subtype Filters			
Action	Pass/Drop	Pass	
SubType	DIX-IP-TCP-Port, DIX-IP-UDP-Port, DIX-IP-Protocol, DIX-IPX-Socket, DIX-EtherType, SNAP-IP-TCP-Port, SNAP -IP-UDP-Port, SNAP -IP-Protocol, SNAP -IPX-Socket, SNAP -EtherType, 802.3-IPX-Socket, 802.2 -IPX-Socket, or 802.2-SAP	DIX-IP-TCP-Port	
Value		00 00	

Network Management Menu Defaults

Parameter Name	Range	Default	Site Setting
Community Strings			
SNMP Read Community			
SNMP Write Community			
SNMP Secret Community			
IDRS			
IDRS	Enabled/Disabled		
IDRS Server Addr	4 nodes, 0 to 255	0.0.0.0	
IDRS Scope		INTERMEC	

Password Menu Defaults

Parameter Name	Range	Default	Site Setting
User Name		INTERMEC	
Password		INTERMEC	
Read Only Password			
Service Password	Enabled/Disabled	Enabled	
Telnet Access	Enabled/Disabled	Enabled	
Browser Access	Enabled/Disabled	Enabled	
SNMP Access	Enabled/Disabled	Enabled	
RADIUS Client			
Configuration Access	Enabled/Disabled	Disabled	
Server 1			
IP Address	4 nodes, 0 to 255	0.0.0.0	
Secret Key		(blank)	
Server 2			
IP Address	4 nodes, 0 to 255	0.0.0.0	
Secret Key		(blank)	
RADIUS Server			
Server	Enabled/Disabled	Disabled	

IEEE 802.11b HR Radio Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
SSID (Network Name)	0 to 32 characters	INTERMEC	
Frequency	Channel 1 to 14, 2400 to 2500 MHz	Channel 3, 2422 MHz	
Data/Voice Settings	Data Only, Data and Voice, or Voice Only	Data and Voice Traffic	
WEP Encryption	Enabled/Disabled	Disabled	
Wireless Bridging			
Node Type	Station/Master	Station	
Wireless Hops	Enabled/Disabled	Disabled	
Hello Period	1, 2, or 3 Seconds	2 Seconds	
WEP Configuration			
WEP Receive Data	Unencryption Allowed/ Encryption Required	Encryption Required	
WEP Transmit Key		1	
WEP Key 1		(blank)	
WEP Key 2		(blank)	
WEP Key 3		(blank)	
WEP Key 4		(blank)	
Advanced Configuration			
Data Rate	11, 5.5, 2, or 1 MBits	2 MBits (Standard)	
Data Rate Fallback	Enabled/Disabled	Enabled	
Basic Rate	11, 5.5, 2, or 1 MBits	2 MBits (Standard)	
Medium Reservation	Enabled/Disabled	Disabled	
Distance Between APs	Large, Medium, or Small	Large	
Microwave Oven Robustness	Enabled/Disabled	Disabled	
Network Name Security	802.11 compliant/Network Name ‘ANY’ not allowed	802.11 compliant	
DTIM Period		1	

OpenAir Radio Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Security ID	0 to 20 characters	(no password)	
Channel		1	
Subchannel		1	
MAC Configuration	Default, Interference, Throughput, or Manual	Default	
Wireless Bridging			
Node Type	Master/Station	Station	
Wireless Hops	Enabled/Disabled	Disabled	
Hello Period	1, 2, or 3 Seconds	2 Seconds	
Manual MAC Parms			
Hop Period	100, 200, or 400 ms	200 ms	
Beacon Frequency	1 to 7	2	
Deferral Slot	Default, 1, 3, or 7	Default	
Fairness Slot	Default, 1, 3, or 7	Default	
Fragment Size	1 to 1540	310	
Transmit Mode	AUTO, BFSK, or 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 Radio Configuration Menu Defaults

Parameter Name	Range	Default	Site Setting
Port Control	Enabled/Disabled	Enabled	
Hello Period	1, 2, or 3 seconds	1	
File Name	_d.bin	_d.bin	

S-UHF Radio 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, or High	High	

B

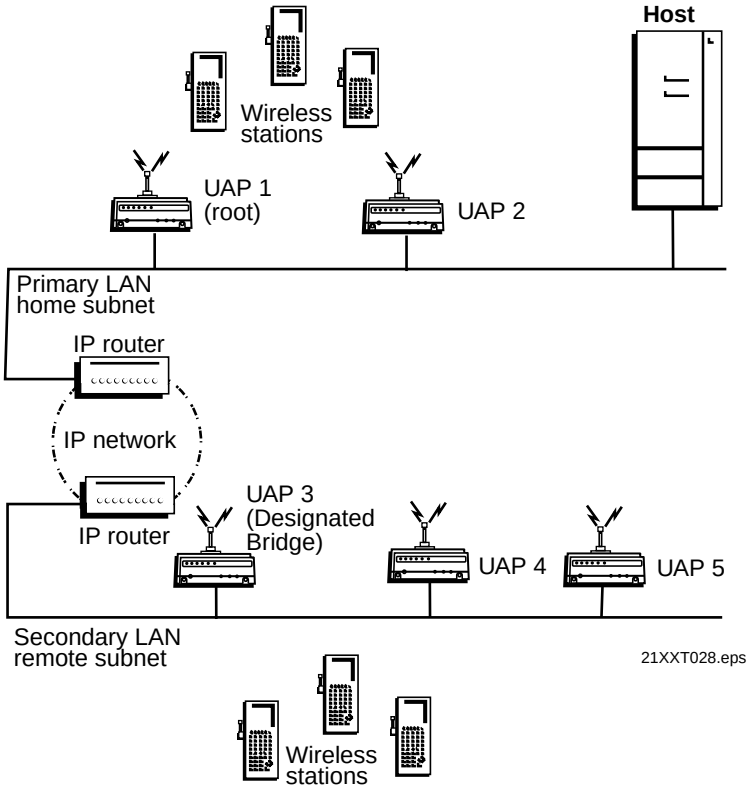
Understanding IP

This appendix provides additional information about IP.

An Overview of 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 Internet Protocol (IP) allows end devices to roam across subnet boundaries.

The IP extension to the open wireless LAN architecture enables a wireless LAN installation to span multiple IP subnets. 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 IP, end devices can roam across IP network subnets without losing network connectivity. 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 IP. 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

To activate IP, configure the root UAP to originate 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 IP port differs from the physical ports within the UAP. The 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.

Operation

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 IP tunnel becomes a branch in the spanning tree. UAPs on remote subnets can be directly connected to an IP tunnel or indirectly connected through another UAP on a remote subnet.

Tunnel Origination

An 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 IP tunnel.
- A wireless link can provide a transparent bridge for both wired and wireless devices on a wireless secondary LAN. An 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 IP tunnels the root can originate is practically unlimited. However, the 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 a network through an IP tunnel if it receives IP hello messages. An IP tunnel is established when a UAP on a remote subnet attaches to the root UAP on its IP port.

Note that a non-root UAP can concurrently receive hello messages on its Ethernet port, its radio port(s), and its logical IP port. However, a UAP uses only one port to attach to the network. UAP port costs are structured so that an Ethernet connection is always selected before an IP or radio connection. An 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 a network. After the root UAP is elected, it transmits hello messages on all enabled ports. The 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 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 in the root UAP, the root sends hello messages to each IP address contained in its IP address list. A UAP on a remote IP subnet can automatically establish an IP tunnel if it receives an IP hello message from the root UAP. A UAP that attaches through an IP tunnel transmits hello messages on the remote subnet so that other UAPs on the remote subnet that do not receive IP hello messages can attach to the network.

If you need to bridge to an 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 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 IP hello messages; a single unicast IP address does not provide redundancy.

Usage Guidelines

This section will help you understand operational requirements for IP.

Addressing for IP Stations

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.

Using With Station Protocols Other than IP

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.) IP does not require changes to default 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 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 IP subnets that contain NNL gateways.

Bridging Restrictions

By default, wireless traffic is not bridged to a remote IP subnet. With bridging disabled, all traffic for end devices is forwarded between access points using data link encapsulation, which means that the MAC source/destination addresses correspond to the access points originating/receiving the traffic for the end devices. By using data link encapsulation, you prevent network monitoring tools and other network components from detecting end device MAC/IP addresses that belong to the remote subnet. In some network installations, detecting these addresses may generate alarms or cause switches to behave erroneously. There is no additional forwarding overhead for disabling bridging in this situation.

Intermec strongly recommends using the default setting when you are using IP to provide mobility of other routable protocols, such as IPX.

If you enable bridging to a remote IP subnet, a UAP terminating the tunnel at the remote subnet will simply bridge traffic for end devices onto the local Ethernet network and UAPs serving the end devices will detect and forward traffic to associated end devices. End device MAC/IP addresses are fully visible on the remote subnet.

Bridging can be enabled on remote IP subnets if IP is used to provide mobility for IP and other non-routable protocols, because IP has built-in safeguards and filters for protecting the operation of IP routers and other network components.

In general, bridging should be enabled if the root of the spanning tree and the Intermec gateway that supports the Intermec NNL devices are on different IP subnets. You may also need to enable bridging if your wireless end devices use terminal emulation running the NNL protocol or if you use wireless end devices that are running both IP and NNL.

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. 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 IP.

Wireless Hop Restriction

To use IP, you must configure UAPs that are on different IP subnets so that they have the same LAN ID. Hello messages contain the IP subnet ID of the UAP that originated the message. The protocol does not allow wireless links to exist between UAPs that do not have matching subnet IDs.

Tunnels Manually Enabled

By default, IP tunnel origination is disabled on the UAP. You must manually enable IP tunnel origination in the root UAP before any IP tunnels can be established.

IP Virtual Subnet

IP provides a virtual subnet for end devices because IP tunnels logically extend the home subnet. The UAP's default bridge priority of zero disables the bridging of wireless traffic to remote IP subnets. The default setting allows terminals that are connected to UAPs on a remote IP subnet to communicate with hosts on the primary LAN or home subnet without bridging wireless traffic to the remote IP subnet. Frames that originate on a remote IP subnet are not forwarded inbound through an IP tunnel.

Configuring the IP Tunnel Port

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

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

To configure the IP port

1. Establish a Web browser session if you have not already done so. For more information, see "Establishing a Web Browser Session" on page 2-20.
2. Click IP Tunnels. The IP Tunnels screen appears.

The IP Tunnels Screen

3. Configure the parameters for the IP port. When you are finished, click Submit Changes to save your changes.

   The following table explains each parameter.

Parameter	Explanation
Port Control	Enables or disables the port.
Mode	Controls whether the UAP listens for the IP tunnel or originates IP tunnel connections with other UAPs. **Listen** Sets the UAP to 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** Sets the UAP so it can originate IP tunnels if it is functioning as the root for the network.
IGMP	Establishes multiple IP tunnels using a single multicast IP address. **Enable** Sets the UAP so the root UAP uses a Class D IP multicast address to send IP hello packets through routers to UAPs on other IP subnets. Enabling IGMP on remote IP subnets causes intermediate IP routers to forward the IP hello packets to those subnets. **Disable** Sets the UAP so the root UAP does not use a Class D IP multicast address to send IP hello packets through routers to UAPs on other IP subnets. For more information, see “Configuring IGMP” on page 5-24.
Hello Period	Controls how frequently the UAP broadcasts hello packets to the tunneled network. Hello packets are used to maintain the spanning tree and serve as beacon messages to synchronize communications with power-managed stations.

Permanent and User-Defined Filters

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 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 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 IP subnets; traffic from a remote IP subnet is never forwarded inbound through an 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
- 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 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 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 IP tunnel.

IP/ARP Subnet Filtering

IP automatically provides subnet filtering for IP end devices. IP and ARP frames are never forwarded inbound through an 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 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.)

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 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 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 IP hello packets. The root UAP learns the unicast IP address of a remote UAP when the UAP attaches to the 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 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 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 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 IP secondary LAN are not forwarded through IP tunnels if the IP address does not belong to the home subnet of the 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. 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 devices that may move between geographically separated locations.

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 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 IP tunnel functions much like a Mobile IP foreign agent.

The following table summarizes the differences between IP and Mobile IP.

Issue	Mobile IP	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 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 network that may include multiple IP subnets.
Roaming support for non-IP protocols	None.	Configurable using 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 network feature. No additional network software is required.

Configuring an 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 IP subnets with the same LAN ID. If 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 IP to configure root candidates to Originate if Root. 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 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 IP tunnel. 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 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 IP hello messages from the root UAP. A UAP will receive 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.

Topologies

The creation of tunnels between the root UAP and remote IP subnets is controlled by three operational parameters:

- The IP address list in the root UAP, configured through the IP port
- Secondary LAN bridge priority settings
- Enabling/disabling IP ports

A tunnel can never be established on a disabled IP port. The discussion below assumes that IP ports are enabled, unless noted otherwise.

The IP address list can contain any combination of IP unicast, IP broadcast, or IP multicast addresses. Only one 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 IP subnet is disabled. In this default case, any UAP on a remote subnet that can receive IP hello messages can establish an IP tunnel; therefore, multiple IP tunnels can exist between the root UAP and a single remote IP subnet.

If IP hello messages are sent to unicast IP addresses, then some UAPs on a remote subnet will likely not receive hello messages; therefore, those UAPs will not be able to establish an IP tunnel. If bridging is disabled on the subnet, wireless traffic is forwarded to and from these UAPs through data link tunnels. A data link tunnel is logically concatenated with an IP tunnel so that wireless traffic can be completely isolated from the remote IP subnet.

If bridging is enabled on an IP remote subnet, a single UAP functions as the designated bridge for the IP secondary LAN. In this case, only the designated bridge can establish an 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 inter-access-point protocol. The UAP IGMP feature is structured so that it is independent of IP; it can be used to facilitate IP multicast for IP or any other application.

IP multicast provides an ideal way to distribute 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 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 IP tunnel.
- IP hello messages are only forwarded to those IP subnets and IP hosts (such as UAPs) that participate in the multicast group. Directed broadcast packets are forwarded to all IP hosts on the target subnet.

C

Using External Antennas

This appendix provides information about positioning external antennas with the UAP. Specific guidelines for antenna separation are provided for those configurations that have multiple antennas.

General Antenna Placement Guidelines

Every wireless network environment presents its own unique obstacles. 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. For information about antenna options, contact your Intermec representative. 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 Antennas for a 2.4 GHz OpenAir WAP

Because the 2.4 GHz OpenAir WAP has two radios, you need to use external antennas and position them at the recommended distances for proper functioning.

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	0.6 meters (2 feet)	(does not apply)	0.6 meters (2 feet)
Angled	1.1 meters (3.5 feet) vertically and 7.3 meters (24 feet) horizontally	0.6 meters (2 feet) vertically and 3 meters (10 feet) horizontally	0.6 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 Antennas for IEEE 802.11b HR Radios

The 802.11b HR radio features antenna diversity, which means that two antennas can be attached to a single radio. The antenna ports on the radio card are marked | and ||. Port | is the send/receive port; port || is the receive only port. (Note that the antenna diversity system uses only one antenna at a time.)

Intermec recommends that you use two antennas for optimal performance of your 802.11b HR radio. If you attach only one antenna to the 802.11b HR radio, you must attach it to Port |. On the 2101 and 2102 UAPs, both antenna ports are visible. On the 2100, use antenna connectors 2 and 4 to attach antennas to the send/receive ports.

Positioning Antennas for Antenna Diversity

If you are using two antennas for one 802.11b HR radio, 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 802.11b HR radio:

- Use external antennas to achieve 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 inches) 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	0.33 m (13 in) or 0.64 m (25 in)
Moderately reflective warehouse environment	0.64 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)

Positioning Antennas for a UAP With Dual Radios

If your UAP has two radios and one of the radios is an 802.11b HR radio, Intermec recommends that you cable the antennas for the 802.11b HR radio at least 3.05 meters (10 feet) from the UAP.

If your UAP has two 802.11b HR radios, you must position the antennas for one radio at least 3.05 meters (10 feet) from the antennas for the other radio. Intermec also recommends that you position the antennas for one radio at least 0.61 meters (2 feet) apart. Note that these recommendations apply to omni antennas; if you are using gain antennas, you should increase the separation between the antennas.

Intermec 2.4 GHz Antennas and Antenna Accessories

The following table identifies many of the Intermec antennas and antenna accessories for the OpenAir and 802.11b HR radios. Contact your Intermec representative for detailed information.

Description	Part Number	Description
2100 antennas	066147	Antenna, 2.4 GHz, Omni
2100 accessories	067265	Adapter cable (to cable)
	067266	Adapter cable (to antenna)
	071179	Cable, 9.1m, 30 ft
	071178	Cable, 3.7m, 12 ft
2101/2102 antennas	069753	Antenna, 2.4 GHz Omni (also 2101 spare)
	069903	Antenna, 2.4 GHz Omni, 802.11b HR (also 2101 spare)
	070140	Antenna, 2.4 GHz, 3dBi Mini Flat (OpenAir)
	070141	Antenna, 2.4 GHz, 3dBi Mini Flat (802.11b HR)
2101/2102 accessories	069886	Adapter cable, OpenAir (to cable)
	069887	Adapter cable, 802.11b HR (to cable)
	070402	Adapter cable, OpenAir (to antenna)
	070403	Adapter cable, 802.11b HR (to antenna)
21XX antennas	067261	Antenna, 2.4 GHz, 3dBi Mini Omni
	067262	Antenna, 2.4 GHz, 5dBi Dual Flat
	063363	Antenna, 2.4 GHz, 5dBi Omni
	063365	Antenna, 2.4 GHz, 15dBi Yagi
	065349	Antenna, 2.4 GHz, 9dBi Omni
	067263	Antenna, 2.4 GHz, 9dBi Flat Panel
	071121	Antenna, diversity
	071122	Antenna, corner

Intermec Antennas and Antenna Accessories Table (continued)

Description	Part Number	Description
21XX accessories	061475	Cable connector, Type N polarized
	063146	Cable connector, Type N
	063198	Splitter, 2.4 GHz only
	063245	Cable, 1.5 m (5 ft)
	063246	Cable, 6.1 m (20 ft)
	064616	Cable, 7.6 m (2.5 ft)
	064432	LMR400 cable, 30.5 m (100 ft)
	589377	LMR400 cable prep tool
	061868	Lightning suppressor and bracket
	586610	Lightning suppressor capsule

G

Glossary

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 a 2.4 GHz 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 a 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 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 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.

IGMP (Internet Group Management Protocol)

IGMP is a protocol that allows the UAP to have more than eight IP tunnels. IGMP allows a UAP to participate in an IP multicast group without any special router configuration.

inbound frames

Frames moving toward the primary LAN.

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, while 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.

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 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 a 2.4 GHz 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 IP subnet
A secondary LAN attached to the network through an 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 network that can originate 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 network through a radio link or an 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 the 2100, 2101, and 2102 access points 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 the IEEE 802.11b HR radio 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

Numbers

A

B

C

D

E

L

M

N

O

P

Q, R

S

T

U

V

W