Intermec

System Manual

MobileLAN™access

Intermec Technologies Corporation
6001 36th Avenue West
Everett, WA 98203
U.S.A.

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.A. and Canada: Contact your local Intermec service supplier.

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

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

The word Intermec, the Intermec logo, INCA (under license), MobileLAN, JANUS, IRL, Trakker Antares, EZBuilder, TE 2000, Data Collection Browser, dcBrowser, Universal Access Point, UAP, Duratherm, EasyCoder, Precision Print, PrintSet, Virtual Wedge, and CrossBar are either trademarks or registered trademarks of Intermec.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young. (eay@cryptsoft.com)

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

There are U.S. and foreign patents pending.

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	11/1998	Added information about the 900 MHz UAP and WAP, and the OpenAir WAP.
003	6/1999	Added information about the IEEE 802.11 Direct Sequence radio and firmware upgrade features.
004	10/1999	Added 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	12/1999	Revised IEEE 802.11 Direct Sequence radio menus and parameters.
006	10/2000	Revised to support software release 1.4. Features include the addition of the IEEE 802.11b radio, WEP 128, IDRS, and the Web User Name parameter.
007	02/2001	Reorganized and revised to support software release 1.50. Features include the ability to use the access point as a DHCP server, improved access control, and internet software download support.
008	03/2002	Reorganized and revised to support software release 1.7x and the new 2106 with the IEEE 802.11a radio. This revision also reflects the name change for this manual from a technical reference manual to the *MobileLAN access 21XX System Manual*.
009	10/2002	Revised to support the new MobileLAN access WA22 and MobileLAN access WA21. This revision also reflects the name change for this manual from the *MobileLAN access 21XX System Manual* to the *MobileLAN access System Manual*.
010	01/2003	Revised to support software release 1.80. Features include an embedded authentication server, MAC address access control list, secure IAPP, secure wireless hops, secure Web browser, and inbound radio filters.

Contents

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.A. 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. Only Intermec service personnel are allowed to access the internal workings of this product. Changing the radio must be done by an Intermec service technician.

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.

Warnings, Cautions, and Notes

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

Warning

A warning alerts you of an operating procedure, practice, condition, or statement that must be strictly observed to avoid death or serious injury to the persons working on the equipment.

Attention Danger: Un avertissement vous avertit d'une procédure de fonctionnement, d'une méthode, d'un état ou d'un rapport qui doit être strictement respecté pour éviter l'occurrence de mort ou de blessures graves aux personnes manupulant l'équipement.

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.

Attention: 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 *MobileLAN access System Manual* provides you with information about the features of the access points, and how to install, configure, and troubleshoot them. You must be familiar with your host PC, your network, your other Intermec equipment, and your data collection network.

You should know how these terms are used in this manual:

Terminology

Term	Description
access point	These terms are used to describe any of the MobileLAN access products, including the WA22, the 2101, the WA21, the 2100, the 2102, and the 2106 unless specifically stated otherwise. When used with a WAP, access point refers to the MobileLAN access product that is connected to the wired network.
WAP	This term refers specifically to a MobileLAN access product that is configured as a wireless access point or repeater.
end device	Any wireless end device configured to transmit data to and receive data from a MobileLAN access product.

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

Format Conventions

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; 5,696,903; 5,740,366; 5,790,536; 5,844,893; 5,862,171; 5,940,771; 5,960,344.

There may be other U.S. and foreign patents pending.

Other Related Manuals

You may need additional information when working with the MobileLAN products. 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

This chapter introduces the MobileLAN™access family of access points, explains their features, and describes how you can use them to expand your data collection network. This chapter covers these topics:

- Overview of the MobileLAN access family
- How the access point fits in your network
- Configuring the access point for the first time

Overview of the MobileLAN access Family

Intermec's MobileLAN™access family of access points delivers reliable and seamless wireless performance to almost any operational environment. They are designed for standards-based connectivity and they support industry standard IEEE 802.11b, WLI Forum OpenAir, and IEEE 802.11a wireless technologies. The 2100 also supports legacy 902 MHz and S-UHF wireless technologies

The 2101, WA22, 2100, WA21, or 2102 with an IEEE 802.11b radio installed is Wi-Fi certified for interoperability with other 802.11b wireless LAN devices.

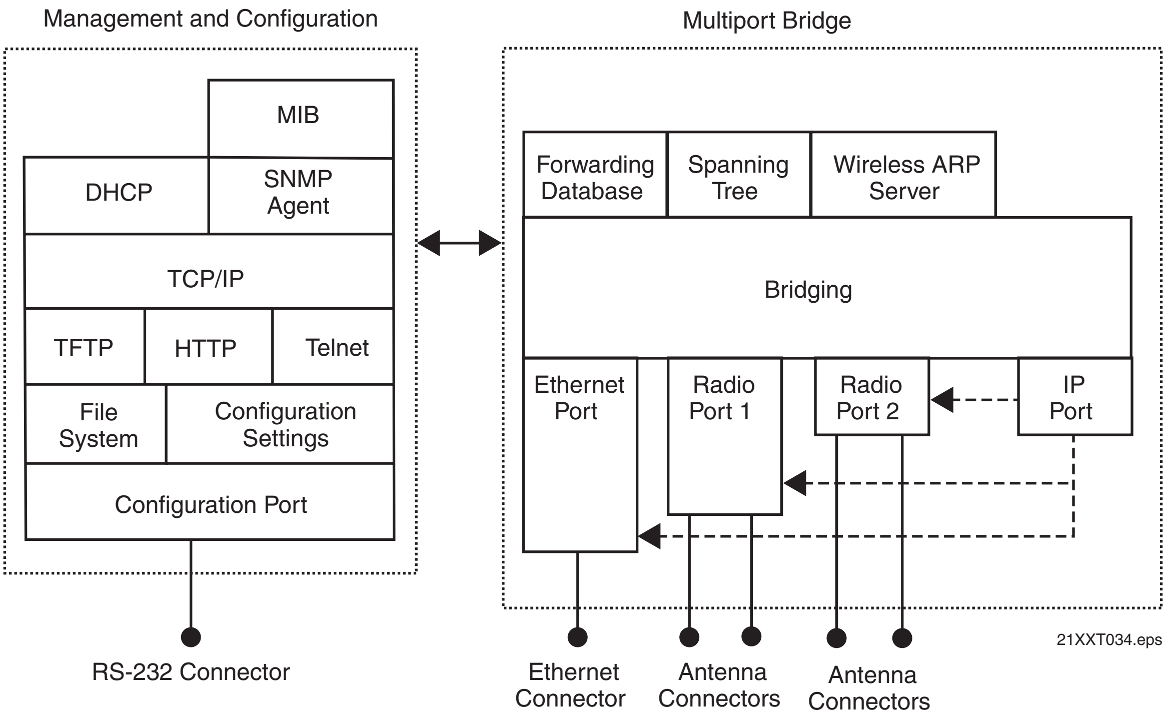
The WA22, WA21, or 2106 with an IEEE 802.11a radio installed is Wi-Fi certified for interoperability with other 802.11a wireless LAN devices.

The MobileLAN access family consists of these access points:

- WA22
- WA21
- 2101
- 2100
- 2102
- 2106

The access point can be configured as an access point or as a point-to-point or point-to-multipoint bridge. Normally, an access point is connected to a wired local area network (LAN) and provides network access for wireless 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. A point-to-multipoint bridge requires two radios and not only connects two wired LANs, but also communicates with wireless end devices.

An access point with two radios can also be configured as a wireless access point (WAP) or repeater. A WAP is not connected to a wired LAN; it receives data from wireless end devices and forwards the data to an access point (that is connected to the wired LAN). A WAP is useful in areas that do not support a wired network connection.



On the left, this illustration shows the ways you can manage and configure the access point, and on the right, it shows the access point's general multiport bridge architecture.

Access points are multiport (Ethernet-to-wireless) bridges, and because wireless end devices operate similarly to other Ethernet devices, all your existing Ethernet applications will work with the wireless network without any special networking software. Any access point, except the root access point, can concurrently receive hello messages on its Ethernet port, its radio port, and its IP tunnel port. However, an access point can use only one port to attach to the network. Port priorities are structured as follows:

1. Ethernet
2. IP tunnel
3. Radio

Unlike the physical Ethernet and radio ports, the IP tunnel port does not have its own output connector. It is a logical port that provides IP encapsulation services for frames that must be routed to reach their destinations. Once frames are encapsulated, they are transmitted or received through the Ethernet or radio port.

Wireless end devices may use power management to maintain battery life. These end devices periodically wake up to receive frames that arrived while their radio was powered down. The access point automatically provides a pending message delivery service that holds frames until the end device is ready to receive them.

Features

The following table summarizes the similarities and differences between the MobileLAN access products.

MobileLAN access Feature Comparison

Feature	WA22	2101	WA21	2100	2102	2106
Access Point	Yes	Yes	Yes	Yes	Yes	Yes
Point-to-Point Bridge (Wireless Bridge)	Yes	Yes	Yes	Yes	Yes	Yes
Wireless Access Point (WAP) or Repeater	Yes	Yes	Yes	Yes	No	No
Secure Wireless Hops	Yes	Yes	Yes	Yes	Yes	Yes
Radios	802.11b, 802.11a	802.11b, OpenAir	802.11b, 802.11a	802.11b, OpenAir, 900 MHz, S-UHF	802.11b, OpenAir	802.11a
Radio Independent™	Yes	Yes	Yes	Yes	Yes	No
Dual Radio Support	Yes	Yes	Yes	Yes	No	No
Wi-Fi Compliant	Yes	Yes	Yes	Yes	Yes	Yes
802.1x	Yes	Yes	Yes	Yes	Yes	Yes
Authenticator	Yes	Yes	Yes	Yes	Yes	Yes
Authentication Server	Yes	Yes (TLS/TTLS – 2101B)	Yes	Yes (TLS/TTLS – 2100D)	No	Yes
Access Control List (ACL)	Yes	Yes (2101B)	Yes	Yes (2100D)	Yes	Yes
Secure Web Browser Interface (HTTPS)	Yes	Yes (2101B)	Yes	Yes (2100D)	No	Yes
10BaseT/100BaseTx	Yes	Yes (2101B)	Yes	Yes (2100D)	10BaseT	Yes
Fiber Optics Option	Yes	Yes	Yes	Yes	No	No
Serial Port	Yes	Yes	Yes	Yes	Yes	No
Data Link Tunneling	Yes	Yes	Yes	Yes	Yes	Yes
IP Tunneling	Yes	Yes	Yes	Yes	Yes	Yes
Antenna Diversity	Yes	Yes	Yes	Yes	Yes	No
Non-incentive Antenna System	Yes	No	Yes	Yes	No	No
NEMA 4/IP 54 Protection	No	No	Yes	Yes	No	No
Power Supply	No	DC	AC	AC	DC	DC
Power Over Ethernet	Yes	Yes with MobileLAN splitter	Yes	Yes, optional	Yes with MobileLAN splitter	Yes with MobileLAN splitter
Heater Option	No	No	Yes	Yes	No	No

Other features of all access points include

- the ability to be managed by MobileLAN manager, a web browser, telnet, and SNMP.
- the ability to be a DHCP server or client and a NAT server.
- the ability to be an ARP server.
- easy software distribution.
- advanced filtering of wired data traffic.
- enhanced power management for wireless end devices.
- fast roaming reliability for wireless end devices.
- load balancing.
- IEEE 802.1x security and dynamically rotating WEP keys for 802.11b or 802.11a networks. The access point can be an authenticator and an authentication server.
- basic WEP 64 or WEP 128 security for 802.11b or 802.11a radios.
- voice over IP optimization (802.11b radio).
- the ability to upgrade over the network or serial port, if the access point has a serial port.

What's New for Software Release 1.80?

Software release 1.80 can be installed on all MobileLAN access products. However, some features are only available on newer access points, which have a faster processor and more flash memory. Newer access points are the WA22, 2101B, WA21, 2100D, and the 2106. To determine the model of your access point, view the AP Connections screen.

New security features include:

- Inbound radio port filters for 802.11b, 802.11a, and OpenAir radios.
- Secure Inter-Access Point protocol (IAPP), which prevents rogue access points from joining the wireless network.
- Secure wireless hops (SWAP).
- Access Control List (ACL) for MAC addresses.
- Ability to configure an ACL and 802.1x security for each radio port.
- Secure web browser interface (HTTPS) – This feature is only available on a WA22, 2101B, WA21, 2100D, or 2106. If you choose not to load your own certificate, a certificate is preloaded.
- Embedded authentication server (EAS) – If you use this feature to authenticate TLS or TTLS devices, it must be running on a WA22, 2101B, WA21, 2100D, or 2106.

- Ability to install certificates if you are using the embedded authentication server feature to authenticate TLS or TTLS devices.

Other new features include:

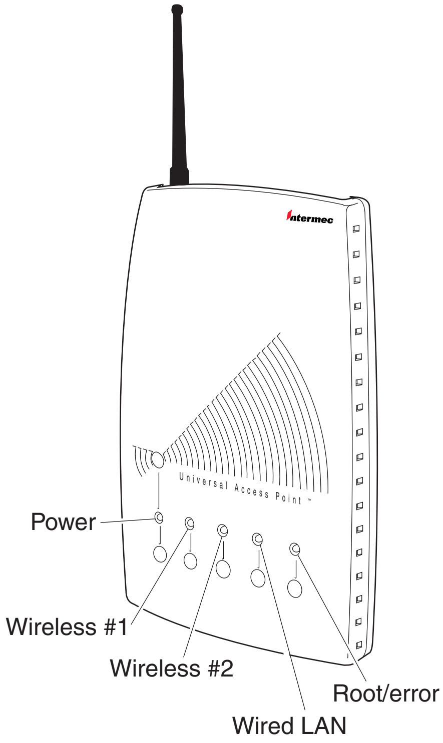
- Wireless hops for 802.11a radio – Currently, this feature works only if an 802.11a radio on the primary LAN is communicating with an 802.11a radio in a designated bridge and the designated bridge only has one 802.11a radio.
- New security traps (that is, access point IP address change, end device starts or ends communicating with the wireless network, unauthorized SNMP management station attempts to access the access point, etc.) sent to a new Security Events log, MobileLAN manager (software release 2.0 or later), or another SNMP management station.
- User interface improvement that includes minor reorganization, use of check boxes, and use of tables.

Understanding the LEDs

The 2102 and 2106 have four LEDs; the 2101 and 2100 have five LEDs. The 2101 and 2100 have a separate LED for each of the radios. To understand the LEDs lighting sequence as the access points boot, see “Understanding the LEDs Lighting Sequence” in Chapter 8. To use the LEDs to help troubleshoot the radios, see “Troubleshooting the Radios” in Chapter 8. To understand the LEDs during normal use, see the next table.

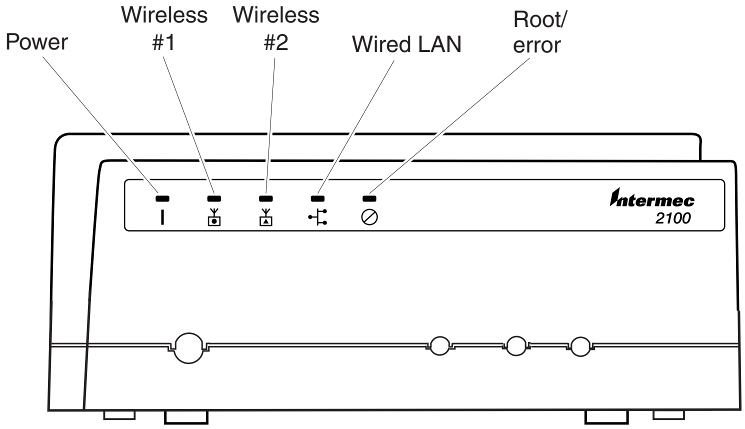
LED Descriptions

Icon	LED	Description
|	Power	Remains on when power is applied.
📡	Wireless #1 or Radio	Flashes when a frame is transmitted or received on the radio port for the radio installed in radio slot 1.
⊶	Wireless #2 (WA22, 2101, WA21, 2100,)	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.



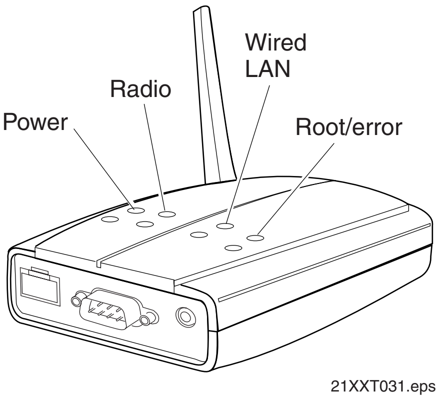
21XXT018.eps

WA22 and 2101 LEDs: *This illustration shows the LEDs that are on the WA22 and the 2101. For help understanding these LEDs, see the LED Descriptions table earlier in this section.*



21XXT003.eps

WA21 and 2100 LEDs: *This illustration shows the LEDs that are on the WA21 and the 2100. For help understanding these LEDs, see the LED Descriptions table earlier in this section.*



2102 and 2106 LEDs: *This illustration shows the LEDs that are on the 2102 and the 2106. For help understanding these LEDs, see the LED Descriptions table earlier in this section.*

Understanding the Ports

The WA22, 2101, 2102, and 2106 ports are located on the bottom of the access point. For more information on connecting the ports, see Chapter 2, "Installing the Access Points."

Port Descriptions

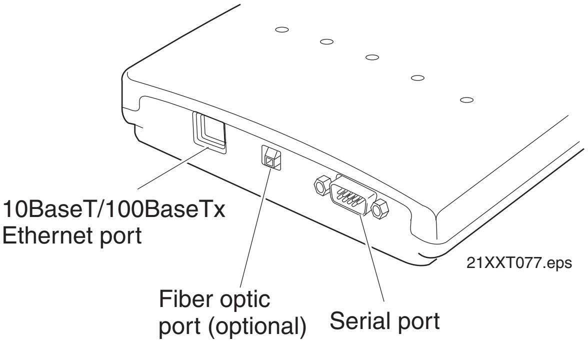
Port	Description
Power (Not WA22, optional WA21)	Used with an appropriate power cable, this port connects the access point to an AC power source.
Serial (Not 2106)	Used with an RS-232 null-modem cable, this port connects the access point to a terminal or PC to perform initial configuration.
10BaseT/100BaseTx (WA22, 2101B, WA21, 2100D, 2106 only)	Used with an appropriate cable, this port connects the access point to your Ethernet network. The access point auto-negotiates with the device it is communicating with so that the data rate is set at the highest rate at which both devices can communicate.
10BaseT (2102 only)	Used with an appropriate cable, this port connects the access point to your Ethernet network.
Fiber optic (WA22, 2101, WA21, 2100 only)	Optional 100BaseFX port. You must use an MT-RJ connector. Used with an appropriate cable, this port connects the access point to your fiber optic network.

To access the ports on the WA21 and the 2100, you must remove the cable access door.

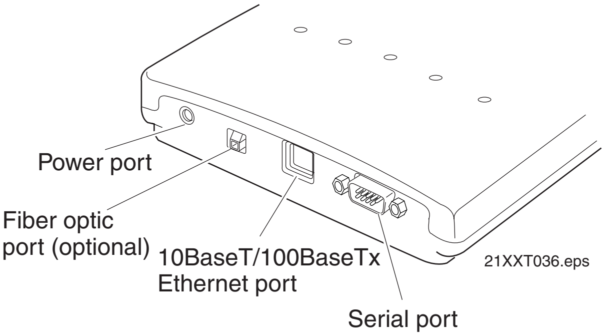
To remove the WA21 or 2100 cable access door

1 Unscrew the two thumbscrews on the cable access door.

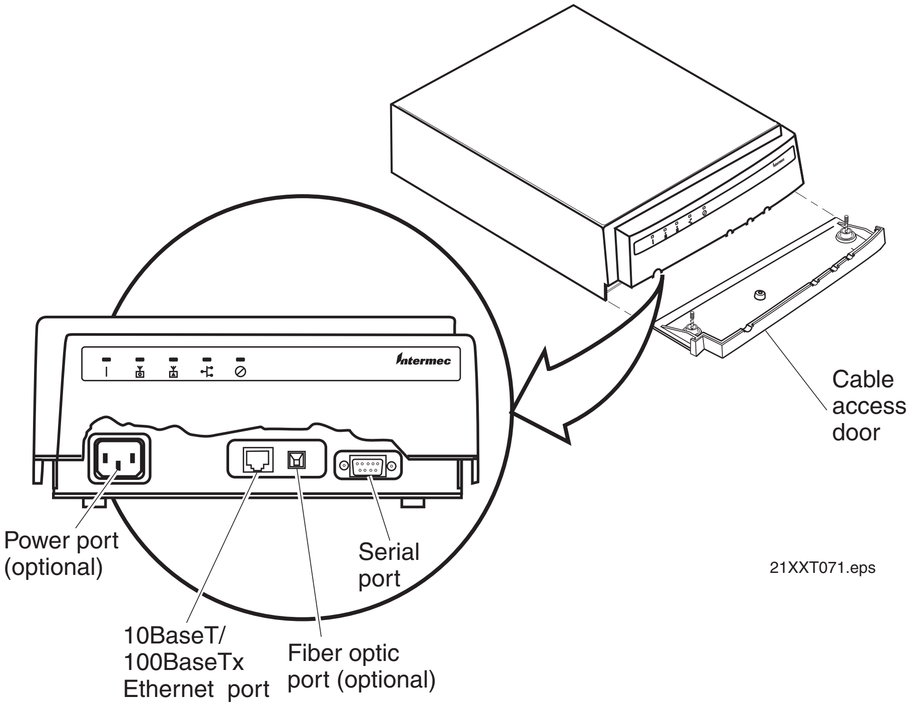
2 Remove the door.



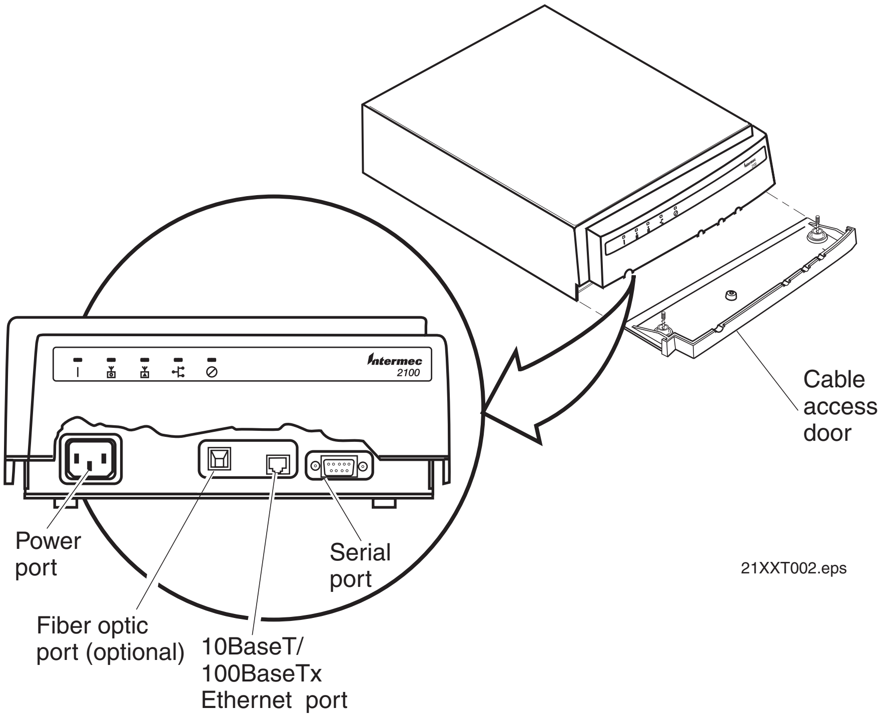
WA22 ports: *This illustration shows the ports that are on the WA22. For help understanding these ports, see the Port Descriptions table earlier in this section.*



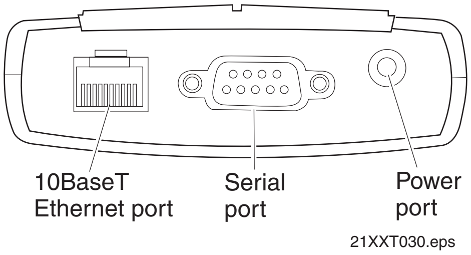
2101 ports: *This illustration shows the ports that are on the 2101. For help understanding these ports, see the Port Descriptions table earlier in this section.*



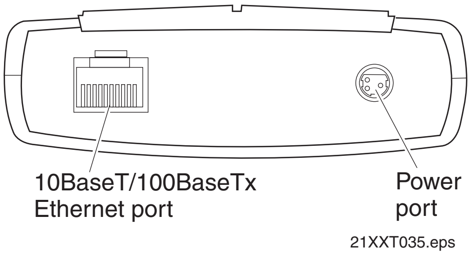
***WA21 ports:** This illustration shows the ports that are on the WA21. For help understanding these ports, see the Port Descriptions table earlier in this section.*



***2100 ports:** This illustration shows the ports that are on the 2100. For help understanding these ports, see the Port Descriptions table earlier in this section.*



***2102 ports:** This illustration shows the ports that are on the 2102. For help understanding these ports, see the Port Descriptions table earlier in this section.*



***2106 ports:** This illustration shows the ports that are on the 2106. For help understanding these ports, see the Port Descriptions table earlier in this section.*

How the Access Point Fits in Your Network

In general, the access point forwards data from wireless end devices to the wired Ethernet network. You can also use the access point as a point-to-point bridge, or if your access point has two radios, you can use it as a point-to-multipoint bridge or a WAP. Use the access point in the following locations and environments.

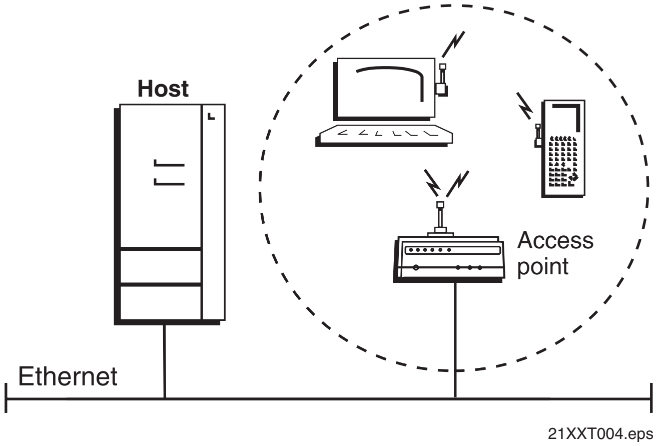
Which Access Point to Use for Your Environment

Access Point	Environment
WA22 and 2101	Use in most indoor environments.
WA21 and 2100	Use in locations where an access point is exposed to extreme environments.
2102 and 2106	Use when you have a simple wireless network, do not need mixed radios, or want a point-to-point bridge to a secondary LAN.

The access point supports a variety of network configurations. These configurations are explained in this section.

Using One Access Point in a Simple Wireless Network

You can use an access point to extend your existing Ethernet network to include wireless end devices. The access point connects directly to your wired network and the end devices a wireless extension of the wired LAN.



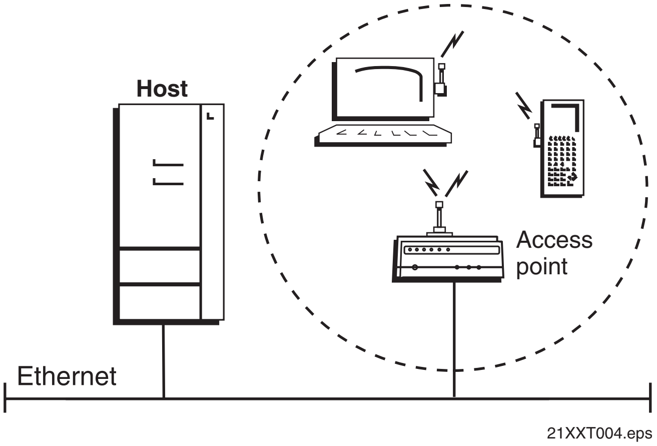
This illustration shows a simple wireless network with one access point and some wireless end devices.

In a simple wireless network, the access point that is connected to the wired network serves as a transparent bridge between the wired network and wireless end devices.

To install a simple wireless network

1. Configure the initial IP address. For help, see “Configuring the Access Point” later in this chapter.
2. Install the access point. For help, see Chapter 2, “Installing the Access Points.”
3. Configure the Ethernet network. For help, see Chapter 3, “Configuring the Ethernet Network.”
4. Configure the radios. For help, see Chapter 4, “Configuring the Radios.”
5. Decide what level of security you want to implement in your network. For help, see Chapter 6, “Configuring Security.”

Example - Configuring an 802.11b Access Point



In this example, there is one 802.11b radio in the access point. Wireless end devices use the access point to communicate with the host and other end devices.

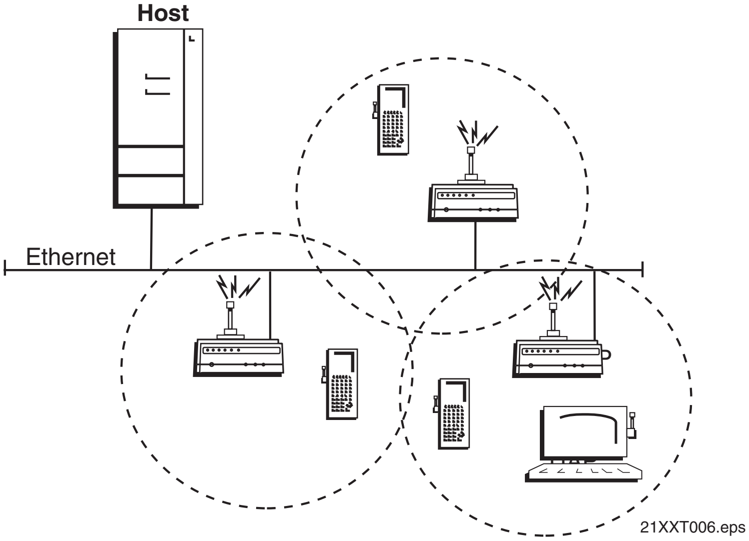
Configuring an 802.11b Access Point Parameters

Screen	Parameter	Access Point
IEEE 802.11b Radio	Node Type	Master
	SSID	Manufacturing
Spanning Tree Settings	Root Priority	5
	Ethernet Bridging Enabled	Checked

Intermec recommends that you always implement some type of security.

Using Multiple Access Points and Roaming Wireless End Devices

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



This illustration shows a wireless network with multiple access points. Wireless end devices can roam between the access points to communicate with the host and other end devices.

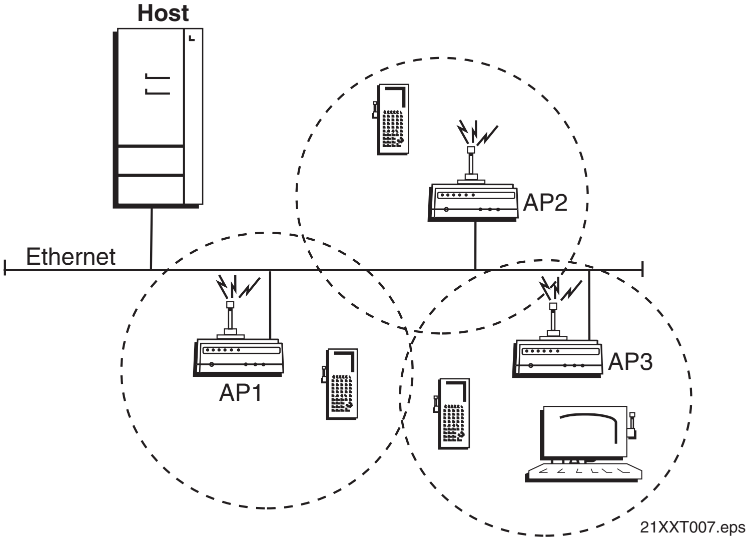
An end device initiates a roam when it attaches to a new access point. The access point sends an attach message to the root access point, which in turn forwards a detach message to the previous access point, allowing each access point to update its forwarding database. Intermediate access points monitor these exchanges and update their forwarding databases.

With the access point's multichannel architecture, you can have more than one access point within the same cell area to increase throughput and provide redundancy. For more information, see "Using Dual Radio Access Points for Redundancy" later in this chapter.

To install multiple access points with roaming end devices

1. Follow the instructions for installing a simple wireless network in the previous section.
2. Configure the LAN ID. For help, see "Configuring the Spanning Tree Parameters" in Chapter 5.
3. Configure one of the access points to be a root access point. For help, see "About the Primary LAN and the Root Access Point" in Chapter 5.
4. If your network has a switch that is not IEEE 802.1d compliant and is located between access points, configure data link tunneling. For help, see "About Data Link Tunneling" in Chapter 5.

Example - Configuring an OpenAir Access Point with Roaming End Devices



In this example, there is one OpenAir radio in each access point. Wireless end devices can roam between the access points to communicate with the host and other end devices.

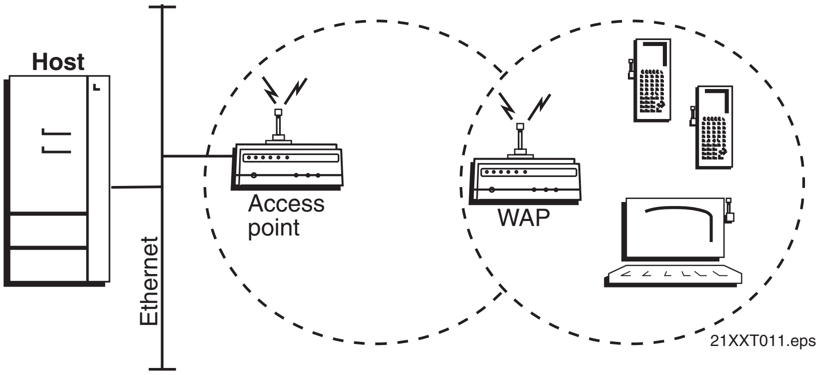
Configuring OpenAir Access Points Parameters

Screen	Parameter	AP1 OpenAir Radio (Root)	AP2 OpenAir Radio	AP3 OpenAir Radio
OpenAir Radio	Node Type	Master	Master	Master
	Security ID	Op3rat!ons	Op3rat!ons	Op3rat!ons
	Channel	1	2	3
	Subchannel	1	1	1
	MAC Configuration	Default	Default	Default
Spanning Tree Settings	LAN ID	0	0	0
	Root Priority	5	4	3
	Ethernet Bridging Enabled	Checked	Checked	Checked

You should configure different channel/subchannel combinations for each access point. The access points communicate with each other through the spanning tree. The wireless end devices are configured as stations with LAN ID set to 0 and Security ID set to Op3rat!ons.

Using an Access Point as a WAP

You can extend the range of your wireless network by configuring a dual radio access point as a wireless access point (WAP). The WAP and the wireless end devices it communicates with comprise a secondary LAN. You can position WAPs in strategic locations so they receive data from end devices, and then forward the data to the wired network. This configuration can be useful when distance or physical layout impedes radio reception and transmission.



This illustration shows a simple wireless network with one access point and one WAP. Wireless end devices use the WAP to forward data to the access point.

WAPs send data from end devices to the access points via wireless hops. Wireless hops are formed when data from end devices move from one access point to another access point through the radio ports. The master radio in the access point transmits hello messages, which allow the WAPs to attach to the spanning tree in the same way as access points.

If you have an 802.11b or an OpenAir network, the WAP must contain two radios. The WAP master radio must match the end devices radios and the WAP station radio must match the master radio in the access point. Currently, 802.11a networks cannot use WAPs to communicate with end devices with 802.11a radios because you cannot configure a WAP with two 802.11a radios with one master and one station radio.

If you have a 902 MHz network, the WAP only needs one 902 MHz radio because this radio can simultaneously be a master and a station. This radio will create wireless hops automatically when it cannot communicate to the wired network.

Note: The 2102 and 2106 cannot be WAPs because they only contain one radio.

Note: S-UHF networks cannot use WAPs because these radios do not support wireless hops.

WAPs must be on the same IP subnet as the access point. Also, data from wireless end devices should not go through more than three wireless hops before it gets to an access point on the primary LAN.

The following procedure explains how to install a simple wireless network with a WAP and no roaming end devices. For help installing a simple wireless network with a WAP and roaming end devices, see the two examples in the next sections.

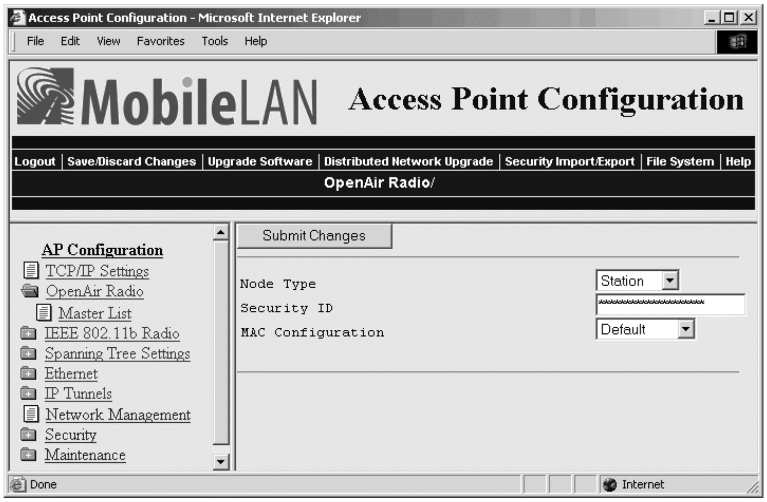
To install a simple wireless network with a WAP and no roaming end devices

1 Follow the instructions for installing a simple wireless network earlier in this chapter.

2 Configure the LAN ID. For help, see “Configuring the Spanning Tree Parameters” in Chapter 5.

3 Configure the station radio in the WAP.

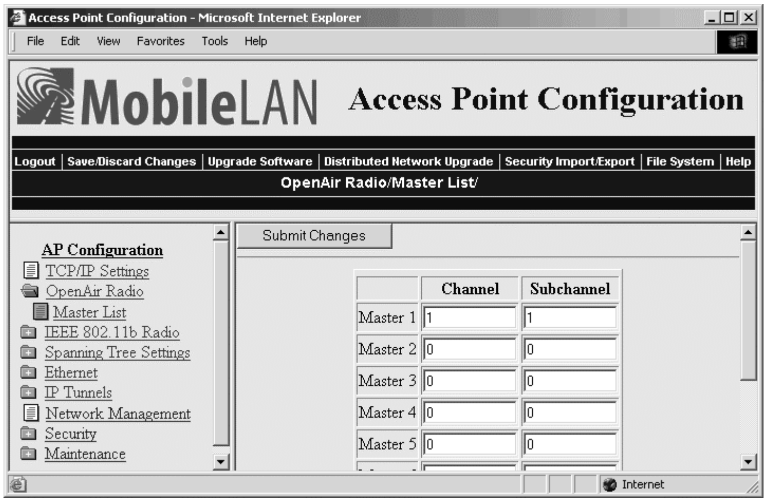
a From the main menu, click the link corresponding to the station radio. The radio screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
OpenAir Radio/
AP Configuration
TCP/IP Settings
OpenAir Radio
Master List
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Done
Internet

Node Type: Station
Security ID: ********************
MAC Configuration: Default

b Click the down arrow on the right side of the Node Type field, choose Station, and click Submit Changes.

c (OpenAir) Click Master List. The Master List screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
OpenAir Radio/Master List/
AP Configuration
TCP/IP Settings
OpenAir Radio
Master List
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	Channel	Subchannel
Master 1	1	1
Master 2	0	0
Master 3	0	0
Master 4	0	0
Master 5	0	0

In the Channel and Subchannel fields, enter the channel and subchannel of all master radios with which this station can communicate.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” later in this chapter.

5 Configure the master radio (in the WAP) to communicate with the end devices. For help, see Chapter 4, “Configuring the Radios.”

6 Configure the master radio in the access point.

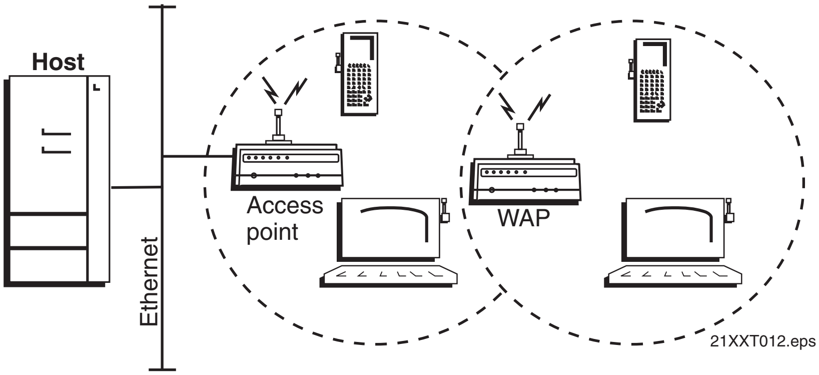
a From the main menu, click the link corresponding to the master radio. The radio screen appears.

b Click the down arrow on the right side of the Node Type field, choose Master, and click Submit Changes.

7 Configure the access point to be a root access point. For help, see “About the Primary LAN and the Root Access Point” in Chapter 5.

8 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” later in this chapter.

Example - Configuring an 802.11b WAP With Roaming End Devices



In this example, there is one 802.11b radio in the access point and there are two 802.11b radios (IEEE 802.11b-1 and IEEE 802.11b-2) in the WAP. Wireless end devices can roam between the WAP and the access point.

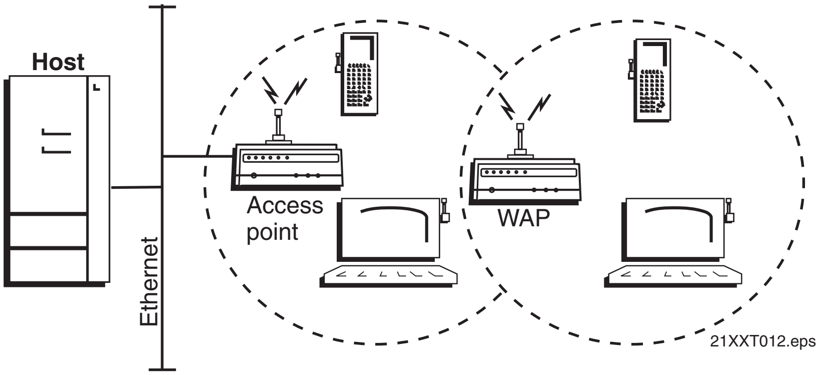
Configuring an 802.11b Access Point and WAP Parameters

Screen	Parameter	Access Point IEEE 802.11b	WAP IEEE 802.11b-1	WAP IEEE 802.11b-2
IEEE 802.11b Radio	Node Type	Master	Master	Station
	SSID	Manufacturing	Manufacturing	Manufacturing
Spanning Tree Settings	LAN ID	0	0	0
	Root Priority	5	0	N/A
	Ethernet Bridging Enabled	Checked	Checked	N/A

You need to configure the wireless end devices to have the same SSID, LAN ID, and frequency as the WAP master radio (IEEE 802.11b-1). You do not need to configure any secondary LAN settings because the WAP is not connected to a secondary LAN.

Intermec recommends that you always implement some type of security.

Example - Configuring an OpenAir WAP With Roaming End Devices



In this example, there are two OpenAir radios in the access point and there are two OpenAir radios in the WAP. To provide better throughput, one master radio in the access point is configured to allow wireless end devices to communicate with it and the other master radio is configured to communicate only with the WAP station radio.

Configuring an OpenAir Access Point and WAP Parameters

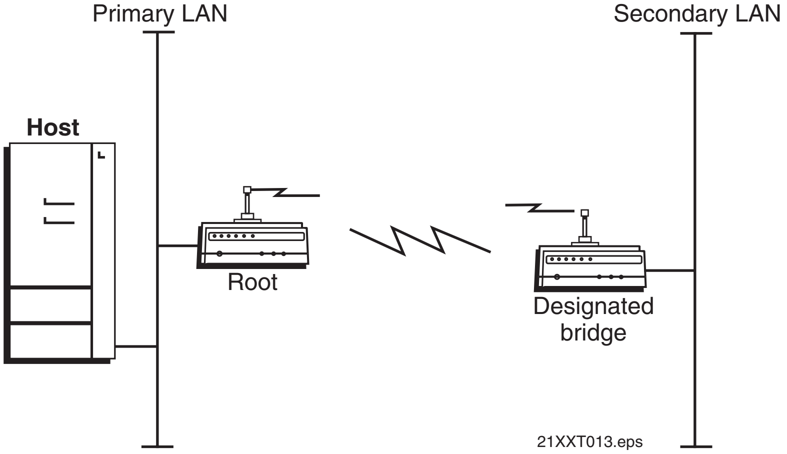
Screen	Parameter	Access Point OpenAir-1	Access Point OpenAir-2	WAP OpenAir-1	WAP OpenAir-2
OpenAir Radio	Node Type	Master	Master	Master	Station
	Security ID	Area2	Area1	Area2	Area1
	Channel	2	1	2	N/A
	Subchannel	1	1	1	N/A
Spanning Tree Settings	LAN ID	0	0	0	0
	Root Priority	5	0	0	0
	Ethernet Bridging Enabled	Checked	Checked	Checked	Checked

You also need to add the channel (1) and the subchannel (1) of the master radio that the WAP station radio is communicating with (Access Point OpenAir-2) to the Master List for the WAP station radio. You do not need to configure any secondary LAN settings because the WAP is not connected to a secondary LAN.

You need to configure the wireless end devices to have the same LAN ID and security ID as the WAP master radio (WAP OpenAir-1).

Using Access Points to Create a Point-to-Point Bridge

You can use access points to create a point-to-point bridge between two wired LANs. That is, you can have one access point wired to a primary LAN in one building and have a second access point wired to a secondary LAN in another building. This configuration lets wired and wireless end devices in both buildings communicate with each other, which can be useful in a campus environment or any other environment where pavement or other objects prevent installation of a wired link.



This illustration shows two simple wireless networks that are connected with access points that are acting as point-to-point bridges. If you have wireless end devices that are communicating with the designated bridge, then the designated bridge needs two radios.

Point-to-point bridges send data from end devices on the secondary LAN to the root access point via wireless hops. Wireless hops are formed when data from end devices move from one access point to another access point through the radio ports. The master radio in the point-to-point bridge on the primary LAN transmits hello messages, which allow the bridge on the secondary LAN to attach to the spanning tree in the same way as access points.

If the access points are simply acting as a point-to-point bridge or if you have a 902 MHz network, each access point only needs one radio. If you have an 802.11b or an OpenAir network and you want the designated bridge to also be able to communicate with wireless end devices (point-to-multipoint), the designated bridge must be a dual radio access point. The designated bridge master radio must match the end device radios and the station radio must match the root master radio. Currently, 802.11a networks cannot have a bridge that also communicate with end devices with 802.11a radios because you cannot configure a bridge with two 802.11a radios with one master and one station radio.

Note: S-UHF networks cannot use point-to-point bridges because these radios do not support wireless hops.

Data from wireless end devices should not go through more than three wireless hops before it gets to an access point on the primary LAN.

You need to set the root priorities and secondary LAN bridge priorities for the bridge on the primary LAN and for the bridge on the secondary LAN:

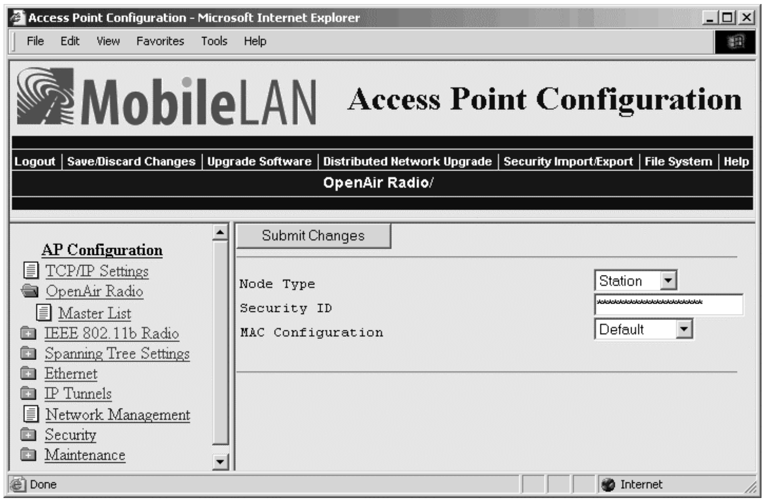
- On the primary LAN bridge, set the root priority to a number that is greater than the root priority of the secondary LAN bridge. The access points will not form a point-to-point bridge if the primary LAN bridge has a lower root priority than the secondary LAN bridge.
- On the secondary LAN bridge, set the secondary LAN bridge priority to a number other than 0.

You may also need to adjust the flooding parameters. Here are some recommendations:

- If there are no end devices on the secondary LAN, the bridge on the secondary LAN can use the default flooding settings.
- If there are end devices on the secondary LAN, the bridge on the secondary LAN should have secondary LAN flooding enabled.
- If there are end devices on the secondary LAN and the end devices communicate with end devices on another secondary LAN, the root access point should have its Multicast Flood Mode parameter set to Universal.

To install a point-to-point or a point-to-multipoint bridge

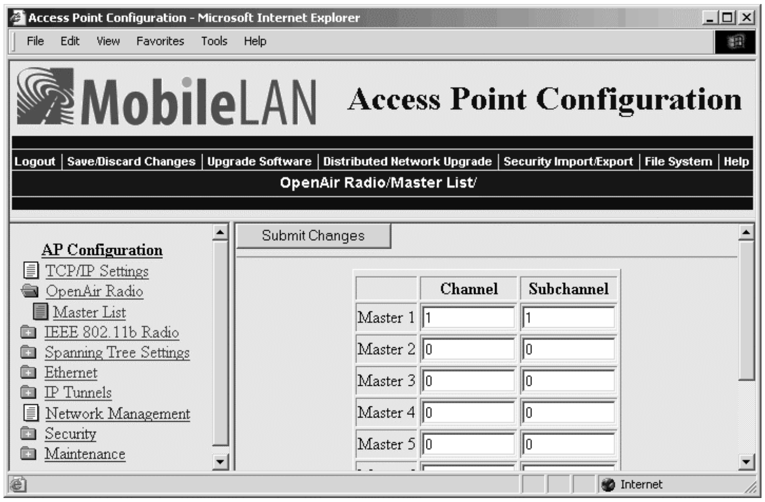
1. Follow the instructions for installing a simple wireless network earlier in this chapter.
2. Configure the LAN ID. For help, see “Configuring the Spanning Tree Parameters” in Chapter 5.
3. Configure the station radio in the point-to-point bridge on the secondary LAN.
   - a From the main menu, click the link corresponding to the station radio. The radio screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
OpenAir Radio/
AP Configuration
TCP/IP Settings
OpenAir Radio
Master List
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Done
Internet

```
Node Type            Station
Security ID          ****************
MAC Configuration    Default
```

b Click the down arrow on the right side of the Node Type field, choose Station, and click Submit Changes to save your changes.

c (OpenAir) Click Master List. The Master List screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
OpenAir Radio/Master List/
AP Configuration
TCP/IP Settings
OpenAir Radio
Master List
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	Channel	Subchannel
Master 1	1	1
Master 2	0	0
Master 3	0	0
Master 4	0	0
Master 5	0	0

In the Channel and Subchannel fields, enter the channel and subchannel of all master radios with which this station can communicate.

4 Configure the spanning tree settings for the point-to-point bridge on the secondary LAN.

a From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.

b In the Root Priority field, enter 0.

c In the Secondary LAN Bridge Priority field, enter a number other than zero.

d Click the down arrow on the right side of the Secondary LAN Flooding field and choose Enabled.

5 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" later in this chapter.

6 Configure the master radio in the point-to-point bridge on the primary LAN.

a From the main menu, click the link corresponding to the master radio. The radio screen appears.

b Click the down arrow on the right side of the Node Type field and choose Master, and then click Submit Changes.

7 Configure the spanning tree settings for the point-to-point bridge on the primary LAN.

a From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.

b In the Root Priority field, enter a number other than 0.

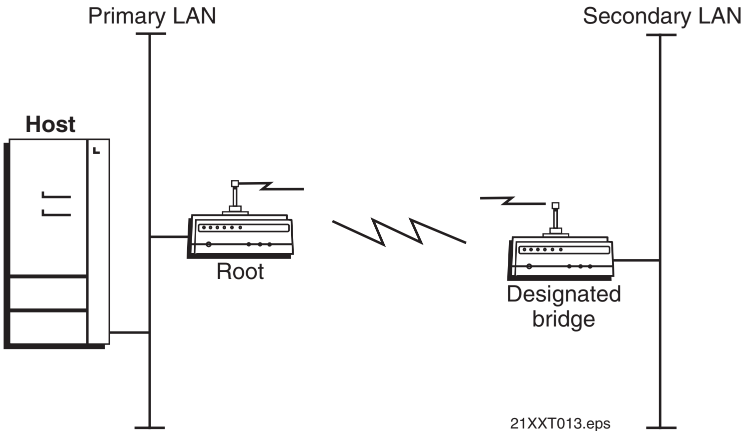
c In the Secondary LAN Bridge Priority field, enter 0.

d Click the down arrow on the right side of the Secondary LAN Flooding field and choose Disabled.

8 If the roaming end devices will be roaming across an IP router, you must configure IP tunnels. For help, see "Configuring IP Tunnels" in Chapter 5.

9 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" later in this chapter.

Example: Configuring an 802.11b Bridge



In this example, each access point only has one 802.11b radio. Since the designated bridge only has a station radio, wireless end devices can only communicate with the root access point. However, wired devices on the secondary LAN can communicate with the primary LAN.

Configuring 802.11b Point-to-Point Bridges Parameters

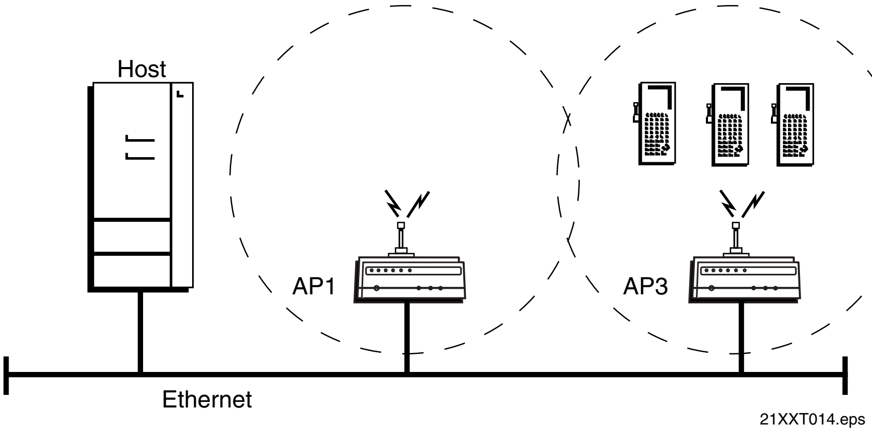
Screen	Parameter	Bridge - Primary LAN (Root)	Bridge – Secondary LAN (Designated Bridge)
IEEE 802.11b Radio	Node Type	Master	Station
	SSID	Manufacturing	Manufacturing
Spanning Tree Settings	LAN ID	0	0
	Root Priority	5	0
	Ethernet Bridging Enabled	Checked	Checked
	Secondary LAN Bridge Priority	0	1
	Secondary LAN Outbound Flooding	Disabled	Enabled

Even though WEP encryption is not required for this configuration, Intermec recommends that you always implement some type of security.

Using Dual Radio Access Points for Redundancy

You can configure WA22s, 2101s, WA21s, and 2100s that have two 802.11b radios or two OpenAir radios to provide redundancy for your network. During normal operations, end devices send frames to the master radio in one of the access points, which bridges the frames to the wired network. If a section of the wired network goes down, the master radio receives the frames, and then the station radio forwards the frames to a master radio in another access point that is within range.

In each access point, you need to configure one radio’s node type as a Master, which communicates with the wireless end devices and configure the other radio’s node type as a Station, which communicates to another access point with a master radio and within range. Currently, 802.11a networks cannot use this feature because you cannot configure the access point with one master and one station radio.



In this example, AP3 is a dual radio access point. It may be located on a loading dock or other remote location. During normal operations, AP3 functions as a normal access point, transmitting frames to and from the host. However, if the Ethernet connection is disrupted, AP3 can function as a WAP and continue operations by transmitting frames to a master radio in AP1. AP3 must be within range of AP1.

To install dual radio access points for redundancy

- Follow the instructions for installing a simple wireless network with a WAP earlier in this chapter.

Configuring the Access Point (Setting the IP Address)

The access point will work out of the box if you are using a DHCP server to assign it an IP address. By default, the access point is configured to be a DHCP client and will respond to offers from any DHCP server. However, if you are not using a DHCP server to assign an IP address, you must assign the access point an initial IP address before you can configure and manage it remotely. To configure the IP address, you can use

- the MobileLAN access Utility. This utility needs to be installed on a PC that is on the same Ethernet segment and subnet as the access point. Or, it can also be installed on a PC that is communicating wirelessly (configured to Intermec's default radio settings) to the access point. For help, see "Using the MobileLAN access Utility" in the next section.
- a communications program (such as HyperTerminal). This program needs to be installed on a PC with an open serial port. You cannot use this method to configure a 2106 since it has no serial port. For help, see "Using a Communications Program" later in this section.

This manual assumes that you are using the MobileLAN access Utility or a communications program for your initial configuration, and then using a web browser interface to perform all other configurations. You can also continue to use a communications program or you can start a telnet session to configure the access point.

Using the MobileLAN access Utility

The MobileLAN access Utility is an easy-to-use Microsoft® Windows™-based utility that lets you

- set the initial IP address for the access point. This utility eliminates the need to serially connect a PC to the access point to configure its IP address.
- restore the access point settings to factory defaults. For help, see the online help and "Restoring the Access Point to the Default Configuration" in Chapter 8.
- recover a failed access point. For help, see the online help and "Recovering a Failed Access Point" in Chapter 8.
- upgrade the access point software. For help, see the online help and "Upgrading the Access Points" in Chapter 8.

After you configure the IP address, you can use a web browser or a telnet session to complete the configuration.

To use the MobileLAN access Utility, you must have the following:

- Windows 95-OSR2/98SE/ME, Windows NT4.0/2000/XP
- Access point software release 1.61 or later

Note: You need to install the MobileLAN access Utility on a PC that is on the same IP subnet as the access point. Or, you need to install it on a PC that is communicating wirelessly (configured to Intermec's default radio settings) to the access point. Before you use the utility, you must have an active radio connection.

To use the MobileLAN access Utility

Caution

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

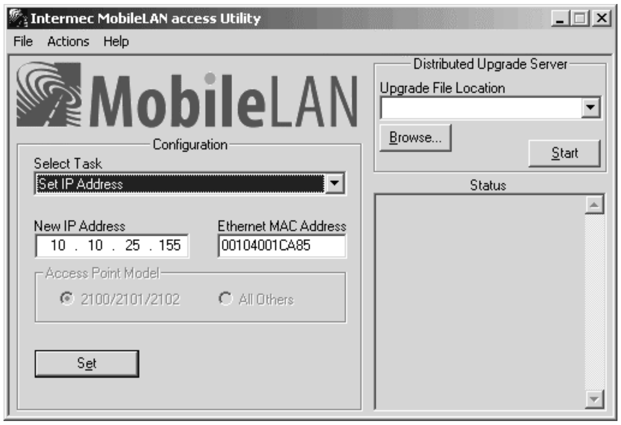
Attention: Vous devez utiliser la source d'alimentation Intermec adéquate avec cet appareil sinon vous risquez d'endommager l'équipement.

1. Insert the MobileLAN access Utility CD into your PC's CD-ROM drive. The CD starts automatically and you will see the CD home page with menu buttons. Click Install Software. If you do not see this home page, from the Start menu, choose Run. In the Open field, type `X:\INDEX.HTM`, where *X* is the CD-ROM drive.

   Or, use a web browser to navigate to www.intermec.com. From the Support menu, click Software Downloads and then MobileLAN to download the MobileLAN access Utility.

2. Follow the instructions that appear on your screen to install the utility.

3 Start the utility. The MobileLAN access Utility main screen appears.



Select Task: Set IP Address

New IP Address: 10 . 10 . 25 . 155

Ethernet MAC Address: 00104001CA85

Access Point Model: ● 2100/2101/2102 ○ All Others

4 Click the down arrow on the right side of the Select Task field and choose Set IP Address.

5 In the New IP Address field, enter the IP address.

6 In the Ethernet MAC Address field, enter the MAC address of the access point. This address is located on the bottom of the access point.

7 Connect the access point to power. The access point has no On/Off switch, so it boots as soon as you apply power.

8 Immediately click Set. The Status box lets you know when the IP address has been set.

9 To continue configuring the access point using a web browser, from the Actions menu choose Configure Access Point, and then enter the new IP address of this access point.

Or, to close the utility, from the File menu choose Exit.

For more help using the utility, from the Help menu choose Contents.

You are now ready to install the access point in your network. See Chapter 2, “Installing the Access Points.”

Using a Communications Program

You can use a communications program (such as HyperTerminal) to set the initial IP address for the access point. After you configure the IP address, you can continue to use the communications program to set other parameters or you can use a web browser or a telnet session to complete the configuration.

To use a communications program, you must have

- a terminal or PC with an open serial port and the communications program.

- an RS-232 null-modem cable. One end of this cable must be a 9-pin socket connector to connect to the serial port on the access point. Intermec offers a 9-socket to 9-socket null-modem cable (P/N 059167).

To use a communications program

Caution

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

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

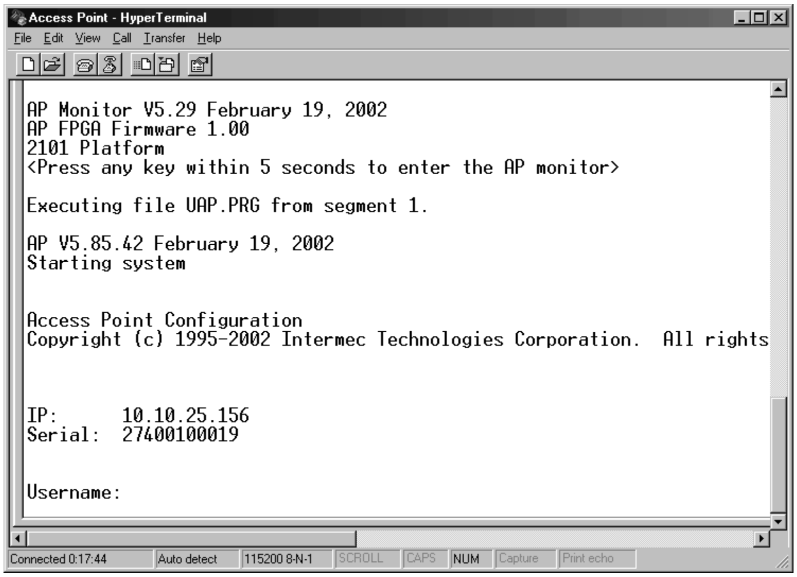
1 Use the RS-232 null-modem cable to connect the serial port on the access point to a serial port on your PC. You may need to remove the serial port plug.

2 Start the communications program and configure the serial port communications parameters on your PC, and then click OK. You should configure the serial port communications parameters to:

Bits per second	9600
Data bits	8
Parity	None
Stop bit	1
Flow control	None

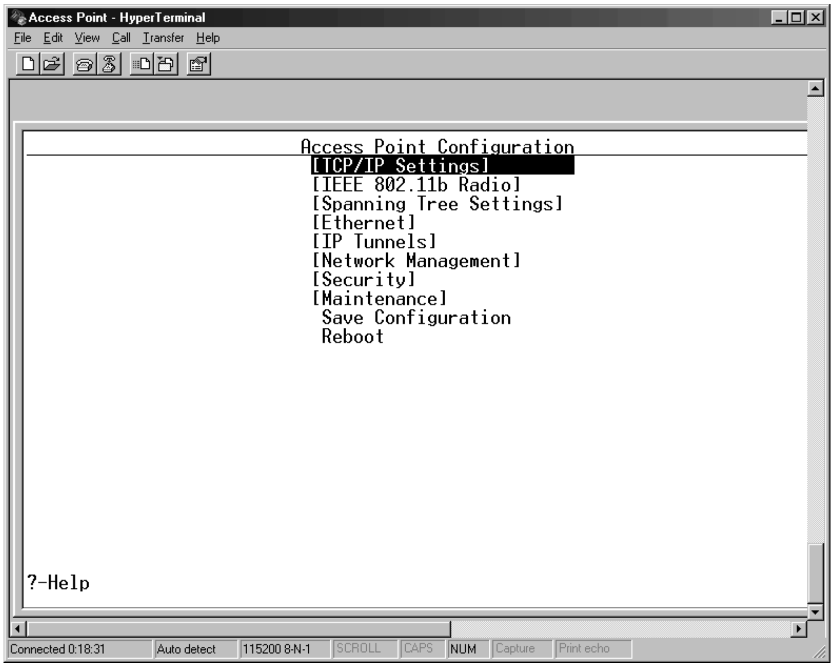
3 Connect the access point to power. The access point has no On/Off switch, so it boots as soon as you apply power.

4 Press Enter when the message “`Starting system`” appears on your PC screen. The Username field appears.



```
AP Monitor V5.29 February 19, 2002
AP FPGA Firmware 1.00
2101 Platform
<Press any key within 5 seconds to enter the AP monitor>

Executing file UAP.PRG from segment 1.

AP V5.85.42 February 19, 2002
Starting system


Access Point Configuration
Copyright (c) 1995-2002 Intermec Technologies Corporation.  All rights



IP:      10.10.25.156
Serial:  27400100019


Username:
```

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



```
                       Access Point Configuration
                        [TCP/IP Settings]
                        [IEEE 802.11b Radio]
                        [Spanning Tree Settings]
                        [Ethernet]
                        [IP Tunnels]
                        [Network Management]
                        [Security]
                        [Maintenance]
                         Save Configuration
                         Reboot

?-Help
```

6 If you are not using a DHCP server, you need to manually assign an IP address. 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) — If the access point will communicate with devices on another subnet, enter the address of the router that will forward frames.

Or, if you are using a DHCP server to automatically assign an IP address to your access point, configure these 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 access point is to access for automatic address assignment. If no server name is specified, the access point responds to offers from any server.

7 Press **Esc** to return to the Access Point Configuration menu.

8 Choose Save Configuration.

You are now ready to install the access point in your network. See Chapter 2, “Installing the Access Points.”

Using a Web Browser Interface

After you have set the initial IP address, you can configure, manage, and troubleshoot the access point from a remote location using a web browser interface. The web browser interface has been tested using Internet Explorer v3.0 and later and Netscape Communicator v4.0 and later. Remotely accessing the access point using other browsers may provide unpredictable results.

Only one session can be active with the access point at a time. If your session terminates abruptly or a new login screen appears, someone else may have accessed the access point. When using the web browser interface, keep the following points in mind:

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

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

To use a web browser interface

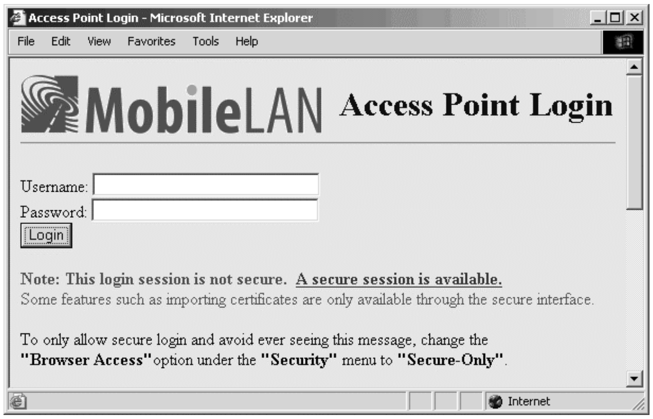
1 Determine the IP address of the access point. If a DHCP server assigned the IP address, you must get the IP address from the DHCP server.

2 Start the web browser application.

3 Access the access point using one of these methods:

- In the Address field (Internet Explorer) or in the Location field (Netscape Communicator), enter the IP address, and press Enter.
- From the File menu, choose Open (Internet Explorer) or choose Open Page (Netscape Communicator). In the field, enter the IP address and press Enter.

The Access Point Login screen appears. If necessary, enter a user name and password. Or, you may want to log in to a secure session.

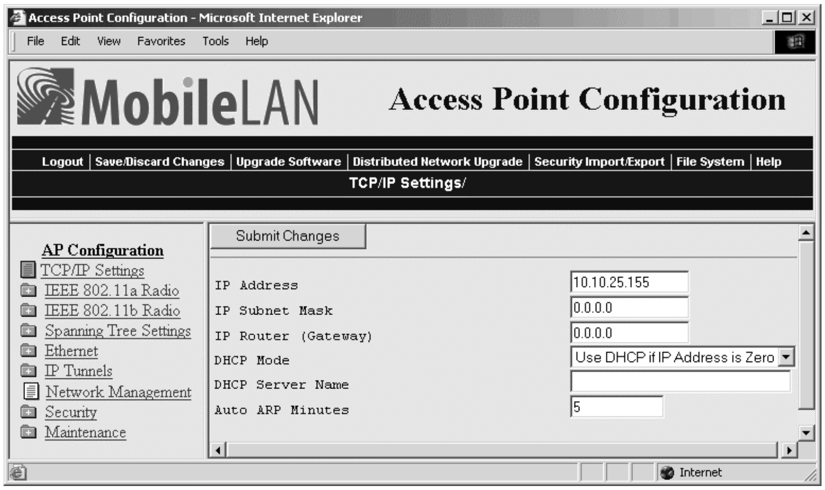

Access Point Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Login
Username:
Password:
Login
Internet

Note: This login session is not secure. A secure session is available.

Some features such as importing certificates are only available through the secure interface.

To only allow secure login and avoid ever seeing this message, change the **"Browser Access"** option under the **"Security"** menu to **"Secure-Only"**.

4 Click Login. The TCP/IP Settings screen appears. You can define a user name and password. For help, see “Setting Up Logins” in Chapter 6.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

TCP/IP Settings/

IP Address	10.10.25.155
IP Subnet Mask	0.0.0.0
IP Router (Gateway)	0.0.0.0
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	
Auto ARP Minutes	5

Your web browser session is established.

Note: Although you can use several different methods to manage the access point remotely, this manual assumes you are using a web browser.

Using a Telnet Session

After you have configured the IP address, you can configure, manage, and troubleshoot the access point from a remote location using a telnet session.

Only one session can be active with the access point at a time. If your session terminates abruptly or a new login screen appears, someone else may have accessed the access point. Also, your session terminates if you do not use it for 15 minutes.

To use a telnet session

1 Determine the IP address of the access point. If a DHCP server assigned the IP address, you must get the IP address from the DHCP server.

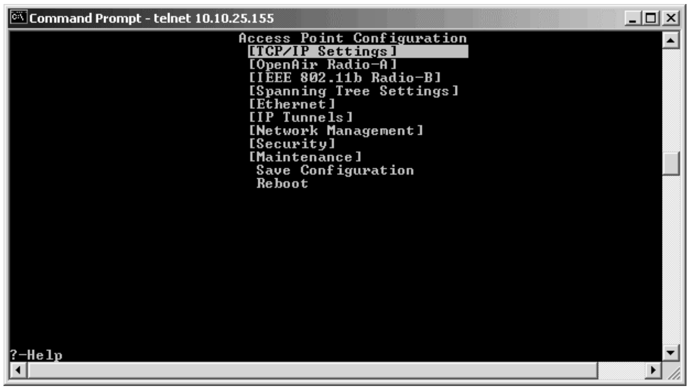
2 From a command prompt, type

```
telnet IPaddress
```

where *IPaddress* is the IP address of the access point.

3 Press Enter.

4 If necessary, enter the user name and press Enter. Then, enter the password and press Enter. The Access Point Configuration menu appears.



```
                             Access Point Configuration
                              [TCP/IP Settings]
                              [OpenAir Radio-A]
                              [IEEE 802.11b Radio-B]
                              [Spanning Tree Settings]
                              [Ethernet]
                              [IP Tunnels]
                              [Network Management]
                              [Security]
                              [Maintenance]
                               Save Configuration
                               Reboot







?-Help
```

Your telnet session is established.

Saving Configuration Changes

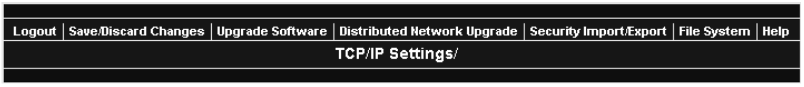
When you are done configuring the access point, you may want to activate your changes immediately or you may want to save the changes now and activate them later. If you choose to activate the changes later, they will become active the next time the access point is booted.

Access Point Configuration Files

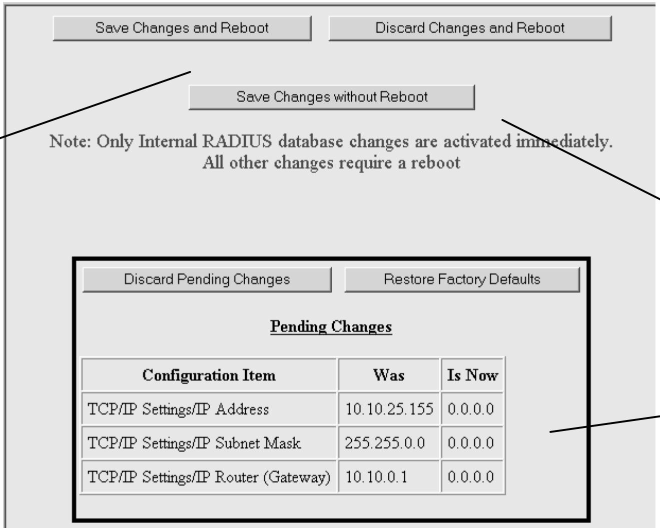
Configuration File	Description
Default	This configuration file is the factory default configuration. For help, see “Restoring the Access Point to the Default Configuration” in Chapter 8.
Current	When you click Submit Changes, the access point updates the current configuration file. The access point does not change the active configuration file. You can see a list of pending changes when you click Save/Discard Changes. Having separate files for the current and active configurations lets you make changes while the access point is running without interrupting communication.
Active	When you click Save/Discard Changes, and then you click Save Changes and Reboot, the access point copies the current configuration file to the active configuration file. The active configuration file is the file that the access point uses.

To save your changes

1 On the menu bar, click Save/Discard Changes.


Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
TCP/IP Settings/

This screen appears.



Note: Only Internal RADIUS database changes are activated immediately.
All other changes require a reboot

Pending Changes

Configuration Item	Was	Is Now
TCP/IP Settings/IP Address	10.10.25.155	0.0.0.0
TCP/IP Settings/IP Subnet Mask	255.255.0.0	0.0.0.0
TCP/IP Settings/IP Router (Gateway)	10.10.0.1	0.0.0.0

Click to use your new configuration now.

Click to use your new configuration the next time you reboot the access point.

Lists configuration changes you have made.

2 Verify that all your configuration changes appear in the Pending Changes box.

3 Click Save Changes and Reboot to reboot the access point and immediately use your new active configuration.

Or, click Save Changes without Reboot. The access point saves the changes to its current configuration and continues to run its active configuration. You will need to reboot the access point when you want the current configuration to become the active configuration.

To discard the changes

- Click Discard Pending Changes.

2 Installing the Access Points

This chapter explains how to install the MobileLAN access products in your data collection network, provides some tips on how to position access points to improve your network performance, and provides some external antenna guidelines. This chapter covers these topics:

- Installation guidelines
- Installing the access points
- Connecting to your fiber optic network
- Connecting power over Ethernet
- External antenna placement guidelines

Installation Guidelines

Intermec recommends that you have Intermec or another certified RF specialist conduct a site survey to determine the ideal locations for all your Intermec wireless network components. To conduct a proper site survey, you need to have special equipment and training.

The following general practices should be followed in any installation:

- Locate access points centrally within areas requiring coverage.
- Overlap access point radio coverage areas to avoid coverage holes.
- Position the access point so that 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 (UPS) when AC power is not reliable.

Proper antenna placement can help improve range. For information about antenna options, contact your local Intermec representative. For more guidelines, see “External Antenna Placement Guidelines” later in this chapter.

When determining ideal locations for the access points, be aware that you may see network performance degradation from microwave ovens, cordless telephones, and other access points. For more information, see the next sections.

Note: Microwave ovens, cordless telephones, and other access points do not degrade the network performance of the 802.11a radio or the S-UHF radio.

Microwave Ovens

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

For the 802.11b radio, the access point has a Microwave Oven Robustness parameter that you can enable to minimize potential interference between your microwave oven and your wireless network. For help, see “Configuring 802.11b Radio Advanced Parameters” in Chapter 4.

Cordless Telephones

If you have an 802.11b, OpenAir, or 902 MHz radio in your access point, the radio may experience interference from some cordless telephones. For optimal performance, consider operating cordless telephones out of range of your access points.

Other Access Points

Access points that are configured for the same frequency and that are in the same radio coverage area may interfere with each other and decrease throughput. You can reduce the chance of interference by configuring access points at least 5 channels apart, such as channels 1, 6, and 11.

Installing the WA22

You can place the WA22 horizontally on a desk or counter. The WA22 also ships with a mounting bracket that lets you mount it vertically to a wall. Additional mounting options that you use with the mounting bracket include a cubicle bracket that lets you mount the WA22 on a cubicle wall or in a locking bracket.

- Cubicle bracket kit (P/N 069926)
- Locking bracket kit (P/N 070184)

To order one of these kits, contact your Intermec representative. Intermec also offers a variety of antennas and antenna accessories. For more information, see “Antennas and Antenna Accessories” in Appendix A.

To install the WA22

1 Attach the antenna or antennas. For more information, see “External Antenna Placement Guidelines” later in this chapter.

Note: If the WA22 has an 802.11a full range radio, you must use the antennas that are already attached to the antenna connectors.

2 Mount the WA22. For help see the *MobileLAN access WA22 Quick Start Guide* and the instructions that shipped with the bracket kit.

3 Connect the WA22 to your wired LAN (unless you are using it as a WAP). For help, see “Connecting the WA22 to Your Wired LAN and Power” in the next section.

4 Connect the WA22 to power. For help, see “Connecting the WA22 to Your Wired LAN and Power” in the next section.

When you are done installing the access points, you need to configure them to communicate with your network.

Connecting the WA22 to Your Wired LAN and Power

Unless you are using the WA22 as a WAP, you must connect it to your Ethernet or fiber optic network. To connect the WA22 to your fiber optic network, you must have a WA22 with the fiber optic option. For help, see "Connecting to Your Fiber Optic Network" later in this chapter.

To connect the WA22 to your Ethernet network and to power, you must first connect it to a MobileLAN power bridge or another 802.3af compliant power over Ethernet network. For help, see "Connecting Power Over Ethernet" later in this chapter and the documentation that shipped with your power bridge.

Installing the 2101

You can place the 2101 horizontally on a desk or counter. The 2101 also ships with a mounting bracket that lets you mount it vertically to a wall.

Additional mounting options include a desk bracket that lets you mount the 2101 upright on a desk or counter, a cubicle bracket that lets you mount the 2101 on a cubicle wall, and a locking bracket. These optional mounting brackets and accessories are available:

- Desk bracket kit (P/N 069657)
- Cubicle bracket kit (P/N 069926)
- Locking bracket kit (P/N 070184)
- Dual antenna bracket kit (P/N 069888)
- Power supply holder kit (P/N 069893)

To order one of these kits, contact your Intermec representative. To mount the 2101, follow the instructions in the kit. Intermec offers a variety of antennas and antenna accessories. For more information, see "Antennas and Antenna Accessories" in Appendix A.

To install the 2101

1 Attach the antenna or antennas. If you attach only one antenna to the 802.11b radio, you must attach it to the | (send/receive) port. For more information, see "External Antenna Placement Guidelines" later in this chapter.

Note: If the 2101 has an 802.11a full range radio, you must use the antennas that are already attached to the antenna connectors.

2 Mount the 2101. For help see the *MobileLAN access 2101 Quick Start Guide* and the instructions that shipped with the bracket kit.

3 Connect the 2101 to your wired LAN (unless you are using it as a WAP). For help, see “Connecting the 2101 to Your Wired LAN” in the next section.

4 Connect the 2101 to power. For help, see “Connecting the 2101 to Power” later in this chapter.

When you are done installing the access points, you need to configure them to communicate with your network.

Connecting the 2101 to Your Wired LAN

Unless you are using the 2101 as a WAP, you must connect it to your Ethernet or fiber optic network. To connect the 2101 to your fiber optic network, you must have a 2101 with the fiber optic option. For help, see “Connecting to Your Fiber Optic Network” later in this chapter.

To connect the 2101 to your Ethernet network

- Attach one end of the Ethernet cable to the 10BaseT/100BaseTx port on the 2101, and attach the other end to your Ethernet network or a MobileLAN splitter (if you are using the power over Ethernet option).

Connecting the 2101 to Power

You use a power supply and power cord to connect the 2101 directly to an AC power outlet.

If you are using the power over Ethernet option, you must have the MobileLAN power splitter and the MobileLAN power bridge or another 802.3af compliant power over Ethernet network. For help, see “Connecting Power Over Ethernet” later in this chapter and the documentation that shipped with your splitter and power bridge.

To connect the 2101 to power

Caution

You must use the appropriate Intermec power supply with this device or equipment damage may occur.

Attention: Vous devez utiliser la source d’alimentation Intermec adéquate avec cet appareil sinon vous risquez endommager l’équipement.

1 Plug one end of the power supply into the power port on the 2101.

2 Plug one end of the power cord into the power supply and the other end into an AC power outlet.

The access point boots as soon as you apply power.

Installing the WA21

You can place the WA21 horizontally or vertically on a desk or counter. If you want to mount the WA21 to a wall or beam using an Intermec mounting bracket kit, you need one of these mounting kits:

- Mounting bracket kit (P/N 068918)
- Rotating mounting bracket kit (P/N 068751)

To order one of these kits, contact your Intermec representative.

To maintain the IP 54 environmental rating, you must mount the WA21 in either the horizontal or vertical position. If you order the WA21 with the heater option, you must use one of the mounting bracket kits to mount the WA21 with the LEDs facing down.

A variety of external antenna options are available for the WA21. Contact your Intermec representative for information about the various antenna options, including higher gain and directional antennas. For more information about antennas and antenna accessories, see “Antennas and Antenna Accessories” in Appendix A.

To install the WA21

1 Attach the antenna or antennas. For more information, see “External Antenna Placement Guidelines” later in this chapter.

Note: If the WA21 has an 802.11a full range radio, you must use the antennas that are already attached to the antenna connectors.

2 Mount the WA21. For help see the *MobileLAN access WA21 Quick Start Guide* and the instructions that shipped with the bracket kit.

3 Connect the WA21 to your wired LAN (unless you are using it as a WAP). For help, see “Connecting the WA21 to Your Wired LAN” in the next section.

4 Connect the WA21 to power. For help, see “Connecting the WA21 to Power” later in this chapter.

When you are done installing the access points, you need to configure them to communicate with your network.

Connecting the WA21 to Your Wired LAN

Unless you are using the WA21 as a WAP, you need to connect it to your Ethernet or fiber optic network. To connect the WA21 to your fiber optic network, you must have a WA21 with the fiber optic option. For help, see "Connecting to Your Fiber Optic Network" later in this chapter.

To connect the WA21 to the Ethernet network

- Attach one end of the Ethernet cable to the 10BaseT/100BaseTx port on the WA21 and attach the other end to your Ethernet network or a MobileLAN power bridge (if you are using power over Ethernet) or another 802.3af compliant power over Ethernet network.

Connecting the WA21 to Power

If your WA21 has the internal power supply option, you can use a power cord to connect the WA21 directly to an AC power outlet.

If you are using the power over Ethernet option, you must have the MobileLAN power bridge or another 802.3af compliant power over Ethernet network. For help, see "Connecting Power Over Ethernet" later in this chapter and the documentation that came with your power bridge.

To connect the WA21 to power

- Plug one end of the power cord into the power port on the WA21 and plug the other end into an AC power outlet. The access point boots as soon as you apply power.

Installing the 2100

You can place the 2100 horizontally or vertically on a desk or counter. If you want to mount the 2100 to a wall or beam using an Intermec mounting bracket kit, you need one of these mounting kits:

- Mounting bracket kit (P/N 068918)
- Rotating mounting bracket kit (P/N 068751)

To order one of these kits, contact your Intermec representative.

To maintain the IP 54 environmental rating, you must mount the 2100 in either the horizontal or vertical position. If you order the 2100 with the heater option, you must use one of the mounting bracket kits to mount the WA21 with the LEDs facing down.

A variety of external antenna options are available for the 2100. Contact your Intermec representative for information about the various antenna options, including higher gain and directional antennas. For more information about antennas and antenna accessories, see "Antennas and Antenna Accessories" in Appendix A.

To install the 2100

1. Attach the antenna or antennas. For more information, see “External Antenna Placement Guidelines” later in this chapter.

   Note: If the 2100 has an 802.11a full range radio, you must use the antennas that are already attached to the antenna connectors.

2. Mount the 2100. For help see the *MobileLAN access 2100 Quick Start Guide* and the instructions that shipped with the bracket kit.
3. Connect the 2100 to your wired LAN (unless you are using it as a WAP). For help, see “Connecting the 2100 to Your Wired LAN” in the next section.
4. Connect the 2100 to power. For help, see “Connecting the 2100 to Power” later in this chapter.

When you are done installing the access points, you need to configure them to communicate with your network.

Connecting the 2100 to Your Wired LAN

Unless you are using the 2100 as a WAP, you need to connect it to your Ethernet or fiber optic network. To connect the 2100 to your fiber optic network, you must have a 2100 with the fiber optic option. For help, see “Connecting to Your Fiber Optic Network” later in this chapter.

To connect the 2100 to the Ethernet network

- Attach one end of the Ethernet cable to the 10BaseT/100BaseTx port on the 2100 and attach the other end to your Ethernet network or a MobileLAN power bridge (if you are using the power over Ethernet option) or another 802.3af compliant power over Ethernet network.

Connecting the 2100 to Power

You can use a power cord to connect the 2100 directly to an AC power outlet.

If you are using the power over Ethernet option, you must have the MobileLAN power bridge or another 802.3af compliant power over Ethernet network. For help, see “Connecting Power Over Ethernet” later in this chapter and the documentation that shipped with your power bridge.

To connect the 2100 to power

- Plug one end of the power cord into the power port on the 2100 and plug the other end into an AC power outlet. The access point boots as soon as you apply power.

Installing the 2102/2106

You can install the 2102 or the 2106 horizontally on a desk or counter, or you can install it vertically to a wall using the mounting bracket that ships with it. An optional cubicle bracket is also available for mounting the 2102 or the 2106 on a cubicle wall. These optional mounting bracket kits and accessories are available for the 2102 or the 2106:

- Cubicle bracket kit (P/N 070366)
- Power supply holder kit (P/N 069893)

This optional mounting bracket kit is available for the 2102:

- Dual antenna bracket kit (P/N 069888)

Intermec also offers a variety of antennas and antenna accessories, including diversity antennas. For more information, see “Antennas and Antenna Accessories” in Appendix A. Contact your Intermec representative for more information about ordering access point accessories.

To install the 2102 or 2106

1. Mount the 2102 or 2106. For help see the *MobileLAN access 2102 Quick Start Guide* or the *MobileLAN access 2106 Quick Start Guide* and the instructions that shipped with your bracket kit.
2. Position or install the antenna. For help, see “Positioning the Standard Antenna” or “Attaching an External Antenna” in the next sections.
3. Connect the 2102 or 2106 to your wired LAN (unless you are using it as a WAP). For help, see “Connecting the 2102 or 2106 to Your Ethernet Network” later in this chapter.
4. Connect the 2102 or 2106 to power. For help, see “Connecting the 2102 or 2106 to Power” later in this chapter.

When you are done installing the access points, you need to configure them to communicate with your network.

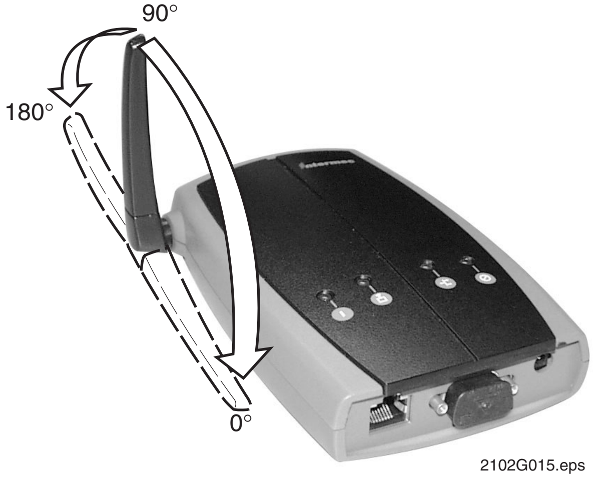
Positioning the Standard Antenna

The 2102 and the 2106 feature a built-in standard antenna that rotates 180° as shown in the next illustration. Use these guidelines when positioning the antenna.

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

- Place the antenna at 0° when storing the 2102 or the 2106.
- Place the antenna at 90° when using the 2102 or the 2106 horizontally; for instance, when the 2102 is positioned on a desk or counter.

- Place the antenna at 180° when using the 2102 or the 2106 vertically; for instance, when it is mounted on a wall or cubicle.



Antenna positions on the 2102 and 2106: *This illustration shows the different ways that you can position the antenna on the 2102 and 2106.*

Attaching an External Antenna (2102)

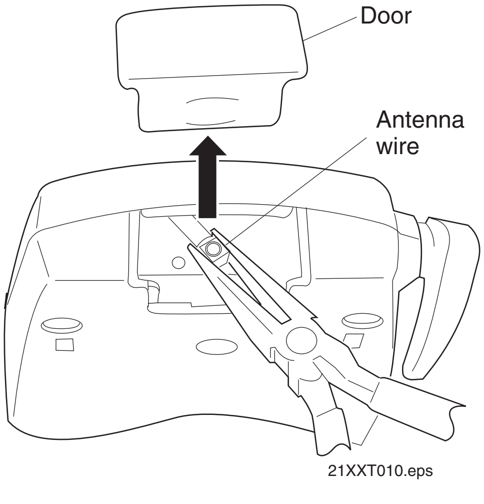
To attach an external antenna to the 2102, you must first disconnect the built-in antenna, and then attach an antenna cable directly to the radio card. You need this tool:

- Needle-nose pliers

To attach an external antenna

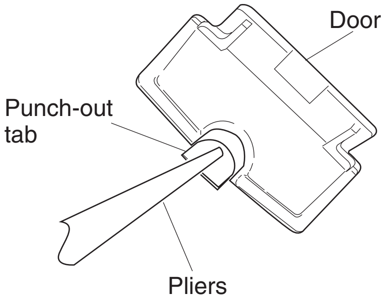
1 Remove the radio card door.

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



3 Tuck the antenna wire inside the 2102 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.

Connecting the 2102 or 2106 to Your Ethernet Network

If you purchased the MobileLAN power splitter and the MobileLAN power bridge so that you can use power over Ethernet, see “Connecting Power Over Ethernet” later in this chapter.

To connect the 2102 or the 2106 to your Ethernet network

- (2102) Attach one end of the 10BaseT cable to the 10BaseT port on the 2102, and attach the other end to your Ethernet network.

  (2106) Attach one end of the Ethernet cable to the 10BaseT/100BaseTx port on the 2106 and attach the other end to your Ethernet network.

Connecting the 2102 or 2106 to Power

You use a power supply and power cord to connect the 2102 or the 2106 directly to an AC power outlet.

If you are using the power over Ethernet option, you must have the MobileLAN power splitter and the MobileLAN power bridge or another 802.3af compliant power over Ethernet network. For help, see “Connecting Power Over Ethernet” later in this chapter and the documentation that shipped with your splitter and power bridge.

Note: The 2102 and 2106 use different power cords.

To connect the 2102 or the 2106 to power

Caution

You must use the appropriate Intermec power supply with this device or equipment damage may occur.

Attention: Vous devez utiliser la source d’alimentation Intermec adéquate avec cet appareil sinon vous risquez endommager l’équipement.

1. Plug one end of the power supply into the power port on the 2102 or the 2106.
2. Plug one end of the power cord into the power supply and plug the other end into an AC power outlet.

The access point boots as soon as you apply power.

Connecting to Your Fiber Optic Network

You can order your WA22, 2101, WA21, or 2100 access points with a fiber optic option. To connect the access point with the fiber optic option to your fiber optic network, you must have a patch cord and an adapter. Patch cords and adapters are available from many different manufacturers. Using adapters and patch cords, you can connect your access point to

- an MT-RJ network.
- a square connector (SC) network.
- a straight tip (ST) network.

For help choosing the proper cord and adapter, contact your local Intermec representative

Note: All cables must be multimode, 62.5/125 µm.

Connecting to an MT-RJ Network

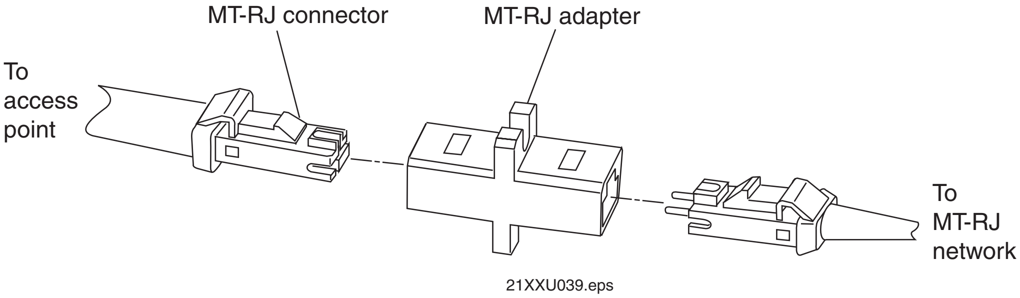
To connect to an MT-RJ network, you need

- a patch cord for connecting the MT-RJ transceiver to the MT-RJ adapter.
- an adapter for connecting an MT-RJ cord to an MT-RJ network.

To connect to an MT-RJ network

1 Remove any cable protectors attached to the patch cord and adapter.

2 Connect the access point to your network.



Connecting to an SC Network

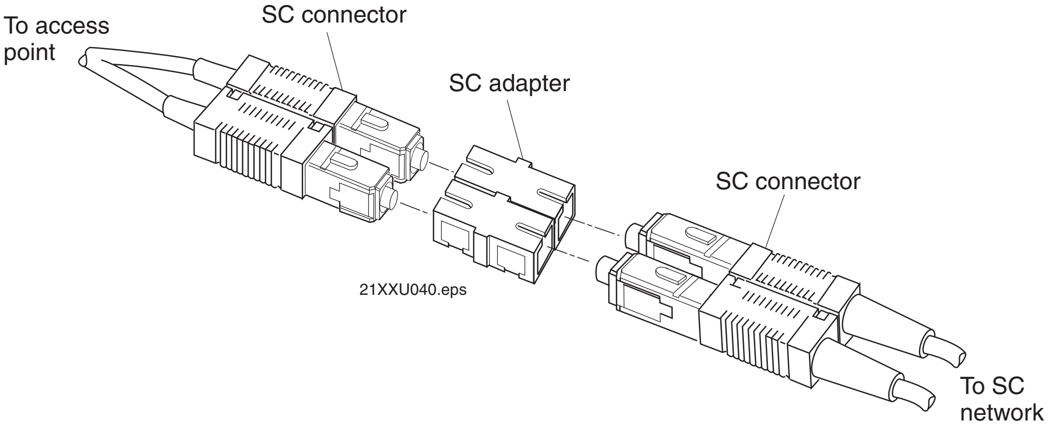
To connect to an SC network, you need

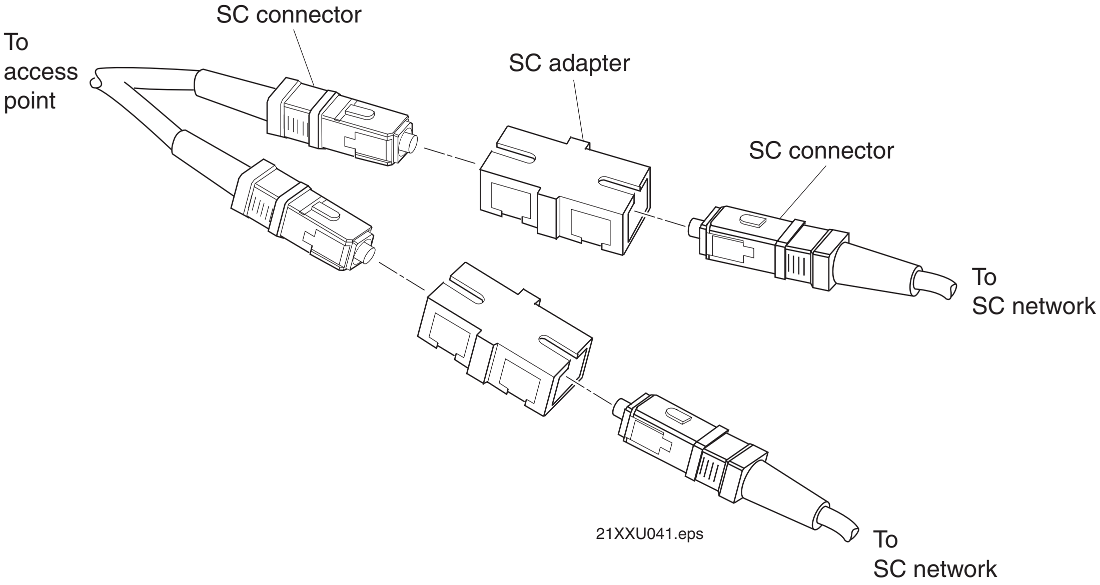
- a patch cord for connecting the MT-RJ transceiver to the SC adapter.
- an adapter for connecting an SC cord to an SC network.

To connect to an SC network

1 Remove any cable protectors attached to the patch cord and adapter.

2 Connect the access point to your network as shown in the next illustrations.





Connecting to an ST Network

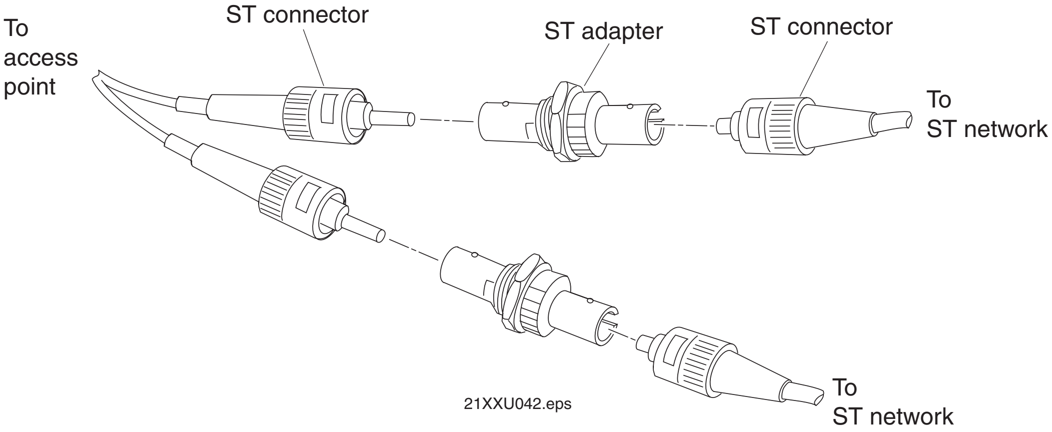
To connect to an ST network, you need

- a patch cord for connecting the MT-RJ transceiver to the ST adapter.
- an adapter for connecting an ST cord to an ST network.

To connect to an ST network

1 Remove any cable protectors attached to the patch cord and adapter.

2 Connect the access point to your network.



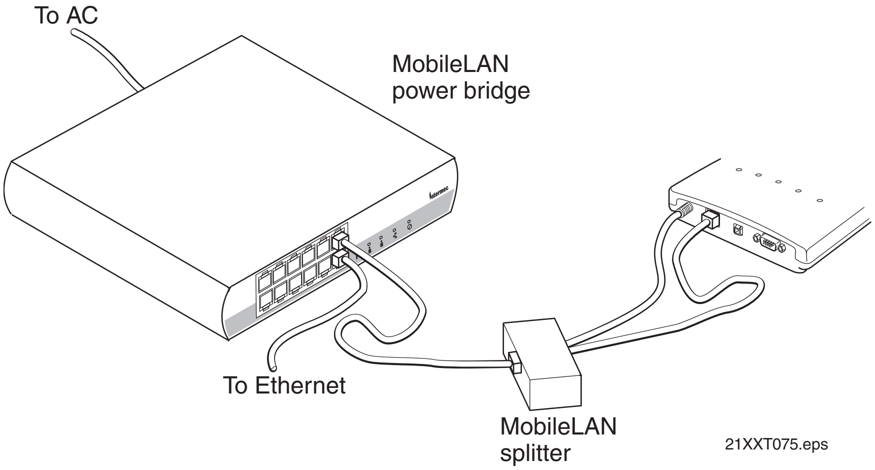
Connecting Power Over Ethernet

The WA22 is powered by power over Ethernet. The WA21 can be powered by AC power or by power over Ethernet or both. The 2100 is normally powered by AC power, but you can order power over Ethernet as an option. You can power the 2101, 2102, or 2106 using power over Ethernet if you connect them to a MobileLAN splitter. For all access points, you need a MobileLAN power bridge.

You order the splitter and the power bridges as accessories.

- (2101, 2102) MobileLAN power splitter, 5 VDC (P/N 071581)
- (2106) MobileLAN power splitter, 3.3 VDC (P/N 072158)
- MobileLAN power bridge (1-port, P/N 071620)
- MobileLAN power bridge (6-port, P/N 071578)
- MobileLAN power bridge (12-port, P/N 071579)

You connect the splitter to the power bridge using a typical Ethernet cable (CAT5). In this cable, four twisted pair lines are used for data and four are unused. Using the data lines, data simply passes through the splitter. Using the unused lines, the splitter receives power from the power bridge, which it converts to the input voltage required by the access point (5 VDC or 3.3 VDC). An LED on the splitter lights when power is being supplied to the access point.



Connecting 2101 using power over Ethernet: *This illustration shows how you connect the 2101 to the MobileLAN splitter and the MobileLAN power bridge so that you can run power over Ethernet.*

To connect power over Ethernet

1. Install the power bridges. For help, see the documentation that shipped with the power bridge.
2. (2101, 2102, 2106) Connect the splitter to the Ethernet port and to the power port of the access point.
3. (2101, 2102, 2106) Use an Ethernet cable to connect the splitter to the power bridge.

   (WA22, WA21, 2100) Use an Ethernet cable to connect the power bridge to the Ethernet port of the access point.

External Antenna Placement Guidelines

Antennas and their placement play a vital role when installing a wireless network. Every wireless network environment presents its own unique obstacles. Therefore, the exact range that you will achieve with each access point 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, 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 m (1,000 ft) of range if positioned outdoors within line of sight, with no obstacles between them. However, the same two radios may only achieve up to 152 m (500 ft) 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 m (300 ft).

Using the proper antennas for your environment and placing them in the proper areas can help improve range. For information about antenna options, contact your local 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.

These next sections provide detailed information about antenna placement for those access points that can have more than one antenna.

Positioning Antennas for 802.11b and 802.11a Radios

The 802.11b radios have two ports: one is a transmit/receive port and the other is a receive-only port. The 802.11a radios have two ports; both ports are transmit/receive ports. Intermec recommends that you use two antennas for optimal performance of the 802.11b and 802.11a radios. If you only attach one antenna to the 802.11b radio, you must attach it to the transmit/receive port.

On the WA22 and the WA21, use antenna connectors 1 and 2 or 3 and 4 to attach antennas to the send/receive ports. On the 2100, use antenna connectors 1 and 3 or 2 and 4 to attach antennas to the send/receive ports. On the 2101 and 2102, both antenna ports are visible. The antenna ports are marked | and ||. Port | is the transmit/receive port; port || is the receive-only port.

Note: The antenna diversity system uses only one antenna at a time.

Positioning Antennas for Antenna Diversity

Antenna diversity lets you attach two antennas to one radio to increase the odds of receiving a better signal on either of the antennas. The 802.11b radio and the 802.11a radio feature antenna diversity. If you are using antenna diversity, 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 antenna can hear. Note these important points:

- Use external antennas to achieve the recommended antenna separation for placement of either omni or directional antennas.
- Position omni antennas for the 802.11b or the 802.11a radio at least 0.61 m (2 ft) apart.
- Position directional antennas so they point in the same direction.
- 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.
- Follow the recommended antenna separation precisely when using the closest distances. Movement of as little as 3.05 cm (1.2 in) may strongly affect performance. You should choose the greatest distance possible within the constraints of your environment.

Recommended Antenna Separation for Antenna Diversity

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 Dual Radio Access Points

These recommendations apply to omni antennas; if you are using directional antennas, you should increase the separation between the antennas.

- If your access point has two 802.11b or two 802.11a radios, position the antennas for one radio at least 3.05 m (10 ft) from the antennas for the other radio.
- If your access point has at least one 802.11b or one 802.11a radio (the other radio may be any radio), cable the antennas for the 802.11b or 802.11a radio at least 3.05 m (10 ft) from the access point.
- If your access point has an 802.11b radio and an 802.11a full-range radio, cable the antennas for the 802.11b at least 3.05 m (10 ft) from the access point.
- If your access point an 802.11b radio and an 802.11a mid-range radio, cable the antennas for either the 802.11b radio or the 802.11a radio at least 3.05 m (10 ft) from the access point.

Positioning Antennas for an OpenAir WAP

For OpenAir WAPs, you must 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 two omni antennas, two directional antennas or you can use one omni antenna and one directional antenna. The following table shows the minimum distance that must exist between the two antennas.

Recommended Antenna Separation for an OpenAir WAP

Position	2 Omni Antennas	2 Directional Antennas	1 Omni, 1 Directional Antenna
Horizontal	3dBi omni, 3 m (10 ft) 6dBi omni, 6.1 m (20 ft) 9dBi omni, 12.2 m (40 ft)	3 m (10 ft)	6.1 m (20 ft)
Stacked	0.6 m (2 ft)	(does not apply)	0.6 m (2 ft)
Angled	1.1 m (3.5 ft) vertically and 7.3 m (24 ft) horizontally	0.6 m (2 ft) vertically and 3 m (10 ft) horizontally	0.6 m (2 ft) vertically and 6.1 m (20 ft) horizontally
Mounting	Mount so antennas point down	Mount antennas back-to-back.	If antennas are not stacked, mount the directional antenna pointing away from the omni antenna. If the antennas are stacked, mount the directional antenna above the omni antenna.

Positioning Antennas for S-UHF Radios

You should position the antenna at least 3 m (10 ft) away from the access point to achieve the specified performance.

3 Configuring the Ethernet Network

This chapter explains how to configure the MobileLAN access products so that they communicate with your Ethernet network. This chapter explains:

- Configuring TCP/IP settings
- Configuring other Ethernet or fiber optic settings
- Configuring Ethernet filters

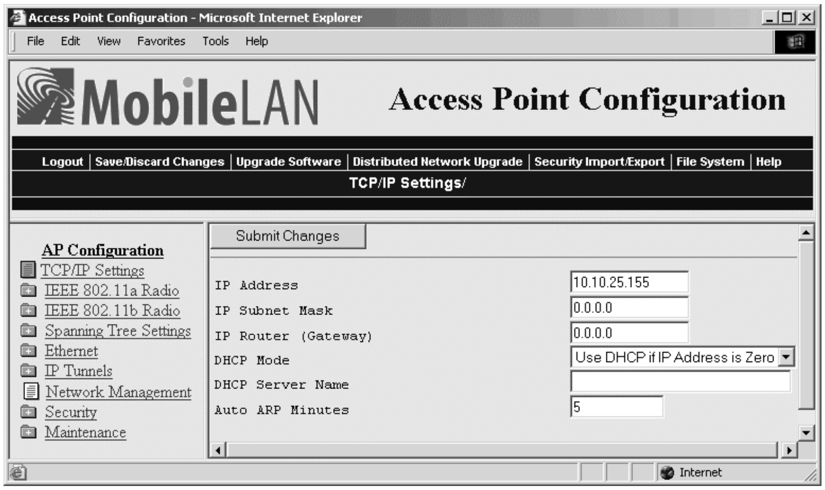
Configuring the TCP/IP Settings

If you are using a DHCP server to automatically assign an IP address to the access point, go to “Configuring the Access Point as a DHCP Client” in the next section. If you are not using a DHCP server, you need to manually assign some TCP/IP parameters.

Note: You should have already configured an IP address for the access point. For help, see “Configuring the Access Point (Setting the IP Address)” in Chapter 1.

To configure the TCP/IP settings

1 From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
TCP/IP Settings/
Submit Changes
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Internet

IP Address	10.10.25.155
IP Subnet Mask	0.0.0.0
IP Router (Gateway)	0.0.0.0
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	
Auto ARP Minutes	5

2 Configure the TCP/IP settings. For help, see the next table.

3 If you want to configure the access point as a DHCP server, see “Configuring the Access Point as a DHCP Server” later in this section.

4 If you want to configure the access point as a NAT server, see “About Network Address Translation (NAT)” later in this section.

5 If you want to configure the access point to send ARP requests, see “Configuring the Access Point to Send ARP Requests” later in this section.

6 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

TCP/IP Settings Descriptions

Parameter	Explanation
IP Address	Enter the IP address of the access point. The IP address has the form *x.x.x.x*, where *x* is a number from 0 to 255.
IP Subnet Mask	Enter the subnet mask that matches the other devices in your network. The subnet mask has the form *x.x.x.x*, where *x* is a number from 0 to 255.
IP Router (Gateway)	Enter the IP address of the router that will forward frames if the access point will communicate with devices on another subnet. The IP address has the form *x.x.x.x*, where *x* is a number from 0 to 255.

Configuring the Access Point as a DHCP Client

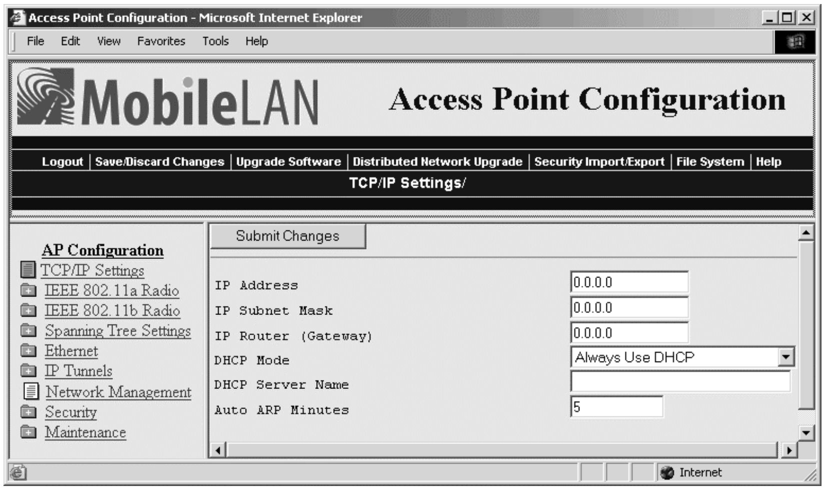
You can use a DHCP server to automatically assign an IP address to your access point; that is, the access point can act as a DHCP client.

Note: You cannot configure the access point as both a DHCP server and a DHCP client.

Note: If you are using the embedded authentication server feature, do not configure the access point as a DHCP client.

To configure the access point as a DHCP client

1 From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
TCP/IP Settings/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

```
IP Address              0.0.0.0
IP Subnet Mask          0.0.0.0
IP Router (Gateway)     0.0.0.0
DHCP Mode               Always Use DHCP
DHCP Server Name
Auto ARP Minutes        5
```

2 Click the down arrow on the right side of the DHCP Mode field and choose either “Always Use DHCP” or “Enabled, if IP Address is Zero.” If you choose “Enabled, if IP Address is Zero,” make sure that the IP Address field is 0.0.0.0.

3 In the DHCP Server Name field, enter the name of the DHCP server that the access point is to access for automatic address assignment. If no server name is specified, the access point responds to offers from any server.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Configuring the Access Point as a DHCP Server

You can configure the access point as a simple DHCP server that provides 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 access points, wireless end devices, wired hosts on the distribution LAN, or wired hosts on secondary LANs.

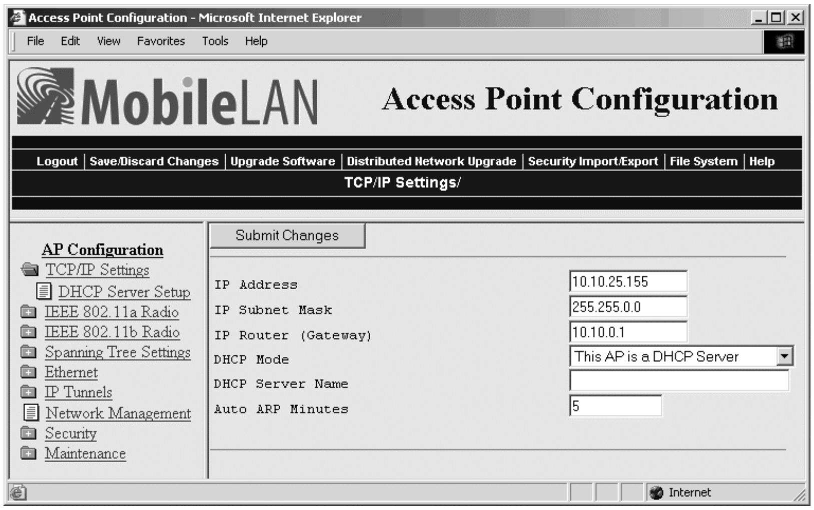
Note: If you configure the access point as a DHCP server, it is not intended to replace a general purpose, configurable DHCP server, and it makes no provisions for synchronizing DHCP policy between itself and other DHCP servers. Customers with complex DHCP policy requirements should use other DHCP server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

Note: You cannot configure the access point as both a DHCP server and a DHCP client.

To avoid a single point of failure, you can configure more than one access point to be a DHCP server; however, the access points do not share DHCP client databases. You should configure each DHCP server with a different address pool from which to allocate client IP addresses.

To configure the access point as a DHCP server

1 From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
TCP/IP Settings/
AP Configuration
TCP/IP Settings
DHCP Server Setup
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

```
IP Address              10.10.25.155
IP Subnet Mask          255.255.0.0
IP Router (Gateway)     10.10.0.1
DHCP Mode               This AP is a DHCP Server
DHCP Server Name
Auto ARP Minutes        5
```

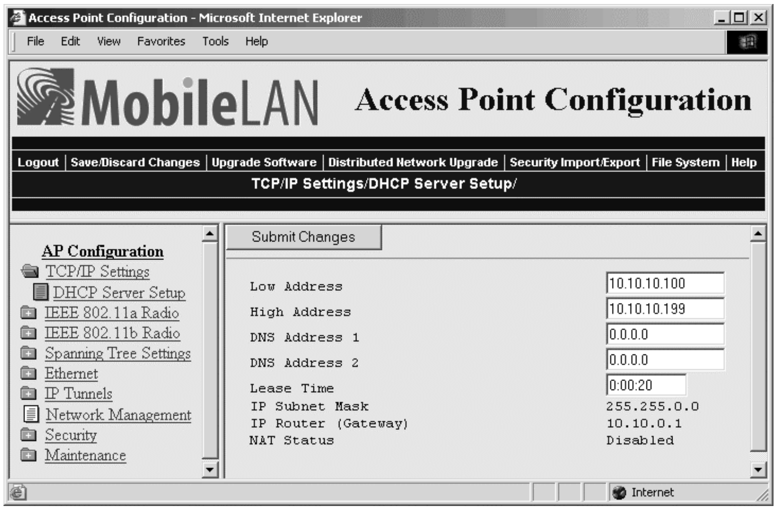
2 Verify that the IP Address field, IP Subnet Mask field, and IP Router field are configured. For help, see “Configuring the TCP/IP Settings” earlier in this chapter.

3 Click the down arrow on the right side of the DHCP Mode field and choose “This AP is a DHCP Server.”

4 In the DHCP Server Name field, enter the name for this access point as a DHCP server.

5 Click Submit Changes to save your changes.

6 Click DHCP Server Setup. The DHCP Server Setup screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
TCP/IP Settings/DHCP Server Setup/
AP Configuration
TCP/IP Settings
DHCP Server Setup
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

```
Low Address             10.10.10.100
High Address            10.10.10.199
DNS Address 1           0.0.0.0
DNS Address 2           0.0.0.0
Lease Time              0:00:20
IP Subnet Mask          255.255.0.0
IP Router (Gateway)     10.10.0.1
NAT Status              Disabled
```

7 Configure the DHCP server. For help, see the next table.

8 Click Submit Changes to save your changes, and then click “here.” To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

DHCP Server Setup Parameter Descriptions

Parameter	Explanation
Low Address	Enter 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 access point, the access point will perform Network Address Translation (NAT) for the clients to which it grants IP addresses.
High Address	Enter 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 access point, the access point will perform Network Address Translation (NAT) for the clients to which it grants IP addresses.
DNS Address 1	Enter 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	Enter 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.
Lease Time	Specifies the duration of the leases that are granted by the DHCP server. Enter the lease time in the format days:hours:minutes. If you set the lease time to 0, infinite leases are granted

Supported DHCP Server Options

When the access point is acting as a DHCP server, it issues IP address leases to configure the IP broadcast address, along with the DNS addresses, IP subnet mask, and IP router. These parameters will contain the same values as those configured for the access point.

Unsupported DHCP Server Options

When the access point is acting as a DHCP server, it 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 frames with a non-zero giaddr (gateway IP address). The DHCP server only responds to requests from its own subnet.

About Network Address Translation (NAT)

NAT allows IP addresses to be used by more than one end device. The access point can act as a NAT server, which instantaneously rewrites IP addresses and port numbers in IP headers so that frames all appear to be coming from (or going to) the single IP address of the access point instead of the actual source or destination.

When an end device uses the access point as an IP router, the access point replaces the IP header, which includes the device MAC address, IP source address, and TCP/UDP port, with its own. You can configure the DHCP server to indicate that the access point is the IP router when the server allocates an IP address. 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 a different subnet from the one the access point is on, the destination MAC address is changed to the IP router that has been configured for the access point. If the destination subnet is the same subnet as the one the access point is on, the access point converts the MAC address to the MAC address that belongs to the destination IP address. This may involve using ARP 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 end device.

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. NAT is enabled if the range of addresses to be given to DHCP clients is not on the same subnet as the access point; thus, you are creating a virtual network and the DHCP server will also perform NAT translation.

When NAT operation is enabled, the access point uses the low address in the range of addresses as its own. The DHCP/NAT clients also use this address as their router IP address. These clients can configure the access point using this internal IP address or the normal external IP address.

To configure the access point as a NAT server

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.
2. Verify that the IP Address field and IP Subnet Mask field are configured. For help, see “Configuring the TCP/IP Settings” earlier in this chapter.
3. Click the down arrow on the right side of the DHCP Mode field and choose “This AP is a DHCP Server.”
4. Click Submit Changes to save your changes.
5. Click DHCP Server Setup and enter a range of IP addresses that are NOT on the same subnet as the access point.
6. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Configuring the Access Point to Send ARP Requests

ARP requests are multicast frames, which means they are sent to all devices on the Ethernet network. You can configure the access point to periodically send an unsolicited ARP request to the IP router so that all routers can update their routing tables. This ARP request lets a network management program learn about the access point on the network by querying routers. The auto ARP period parameter controls the time interval between ARP requests.

If the address of the IP router is 0.0.0.0, then the access point sends an ARP request to its own IP address. Without this option, an access point 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 let the IP address for the access point expire.

To set the auto ARP period

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.
2. In the Auto ARP Minutes field enter a time a period from 1 to 120 minutes. To disable this parameter, set the time period to 0.
3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Configuring Other Ethernet or Fiber Optic Settings

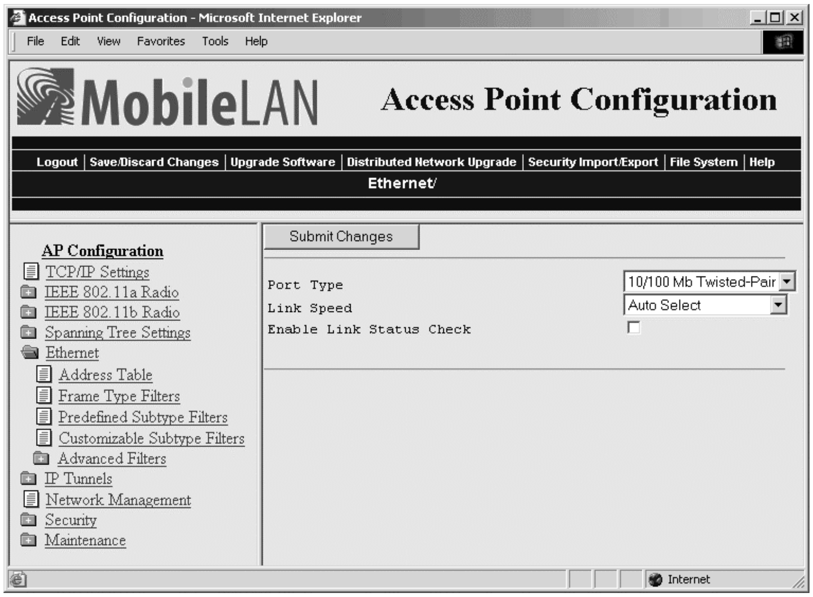
Many of the standard Ethernet or fiber optic settings are configured in the TCP/IP Settings screen. For help, see “Configuring the TCP/IP Settings” earlier in this chapter. In the Ethernet screen, you can

- set the port type. This field specifies the port that the access point uses to communicate with the Ethernet network. If you do not have a fiber optic port, you will not see this field.
- set the link speed. This field specifies the speed and the duplex mode that the access point uses to communicate with the Ethernet network. If you chose the port type to be fiber optic, the link speed is automatically set to 100 Mbps Fiber Optic (full duplex). If you want the access point to auto-negotiate this field, choose Auto Select. Auto Select should work for most networks.

- enable or disable the link status check. Check this check box if you want the access point to periodically check its Ethernet connection. If it loses the connection, this access point can no longer be the root access point and any end devices that are connected to this access point (whether or not it is the root) will roam to a different access point. The access point will attempt to reconnect to the spanning tree through one of its radio ports. Clear this check box if this access point must be the root access point or if it is used as a WAP.

To configure the Ethernet or fiber optic settings

1 From the menu, click Ethernet. The Ethernet screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

Port Type 10/100 Mb Twisted-Pair
Link Speed Auto Select
Enable Link Status Check □

2 In the Port Type field, click the down arrow on the right side of the field. Choose 10/100 Mb Twisted-Pair for Ethernet or 100 Mb Fiber Optic.

3 (10/100 Mb Twisted-Pair only) Click the down arrow on the right side of the Link Speed field and choose the speed and duplex mode you want this port to use to communicate with the Ethernet or fiber optic network.

4 Check or clear the Enable Link Status Check check box.

5 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Configuring the Ethernet Address Table

If you have a secondary LAN, you should configure the Ethernet address table in the designated bridge or WAP on the secondary LAN. This table contains all the MAC addresses on the secondary LAN that are communicating with the primary LAN. You must enter the MAC addresses of all devices on the secondary LAN that do not **always** initiate communication.

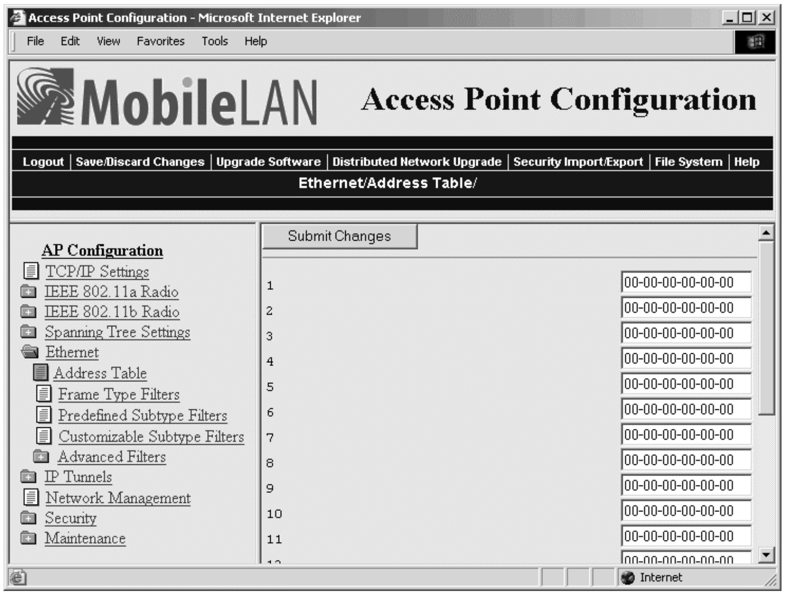
If you choose not to configure this table, the designated bridge or WAP may need to flood frames to the Ethernet and radio ports to learn the path to the MAC address.

These addresses become permanent entries in the forwarding table of the designated bridge or WAP.

To configure the Ethernet address table

1 From the main menu, click Ethernet, and then click Ethernet Filters.

2 Click Address Table. The Address Table screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Address Table/
Submit Changes
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
IP Tunnels
Network Management
Security
Maintenance
Internet

1	00-00-00-00-00-00
2	00-00-00-00-00-00
3	00-00-00-00-00-00
4	00-00-00-00-00-00
5	00-00-00-00-00-00
6	00-00-00-00-00-00
7	00-00-00-00-00-00
8	00-00-00-00-00-00
9	00-00-00-00-00-00
10	00-00-00-00-00-00
11	00-00-00-00-00-00

3 Enter up to 20 MAC addresses. MAC addresses consist of six hex pairs that are separated by spaces, colons, or hyphens.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

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. Setting Ethernet filters prevents the Ethernet port from sending out unnecessary traffic to the wireless network.

Ethernet frame type filter and predefined subtype filter settings override customizable subtype filter settings. However, Intermec recommends that when creating customizable subtype filters, you do not duplicate existing frame type or predefined subtype filters or unexpected results may occur.

For more examples of using Ethernet filters and for help configuring IP filters, see "Configuring IP Tunnel Filters" in Chapter 5.

Using Ethernet Frame Type Filters

You can define filters for common networking protocols such as IP, Novell IPX, and 802.2 LLC. You can also set filters that will 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 not pass the DIX-Other EtherTypes frame parameter, 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, for DIX-IP-TCP ports, you can not pass all frame types. Then, all IP frames with the TCP type will be dropped even if specific TCP parts are set to pass in the subtype menus.

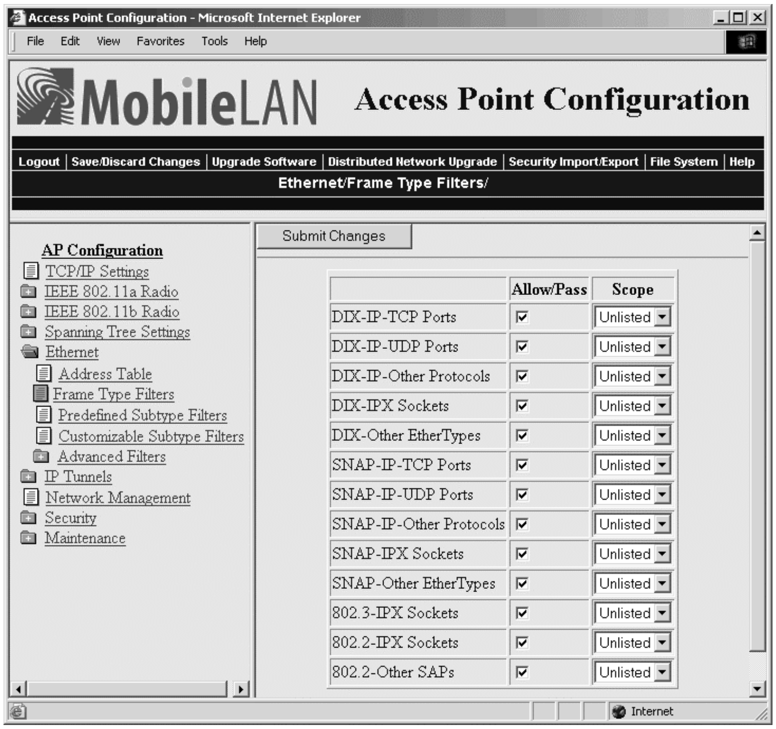
Here is the action and scope you can set for each parameter:

Allow/ Pass Check or clear this check box. Check the check box to pass all frames of that type. Clear the check box to drop all frames of that type.

Scope Set scope to Unlisted or All. If you select All, then all frames of that type are unconditionally passed or dropped, depending on the action you specified. If you select Unlisted, then frames are passed or dropped only if the frame type is not listed in the predefined or customizable tables.

To set frame type filters

1 From the main menu, click Ethernet, and then click Frame Type Filters. The Frame Type Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Frame Type Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	Allow/Pass	Scope
DIX-IP-TCP Ports	☑	Unlisted
DIX-IP-UDP Ports	☑	Unlisted
DIX-IP-Other Protocols	☑	Unlisted
DIX-IPX Sockets	☑	Unlisted
DIX-Other EtherTypes	☑	Unlisted
SNAP-IP-TCP Ports	☑	Unlisted
SNAP-IP-UDP Ports	☑	Unlisted
SNAP-IP-Other Protocols	☑	Unlisted
SNAP-IPX Sockets	☑	Unlisted
SNAP-Other EtherTypes	☑	Unlisted
802.3-IPX Sockets	☑	Unlisted
802.2-IPX Sockets	☑	Unlisted
802.2-Other SAPs	☑	Unlisted

2 For each frame type field, check or clear the check box to configure if the frame types are passed or are dropped. If you check the check box, the frame type is allowed to pass.

For each frame type field, click the down arrow on the right side of the Scope field and set the scope to Unlisted or All.

For help, see the next table.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

4 If you set the Scope field to Unlisted for any of the frame types, you must also configure predefined subtype filters or customizable subtype filters. For help, see “Using Predefined Subtype Filters” or “Customizing Subtype Filters” later in this section.

Frame Type Filter Descriptions

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.

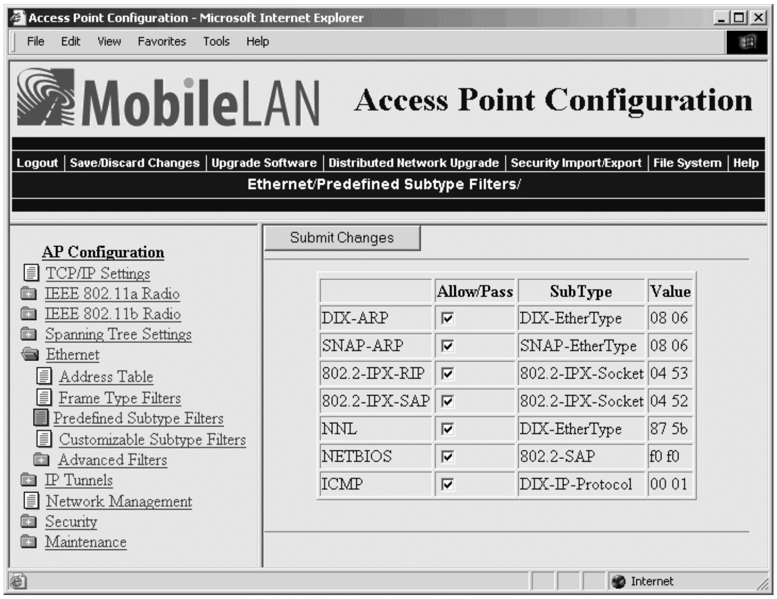
Note: You should not filter HTTP, Telnet, SNMP, and ICMP frames if you are using WAPs because these frame types are used for configuring, troubleshooting, and upgrading WAPs.

Using Predefined Subtype Filters

You can configure the access point to pass or drop certain predefined frame subtypes.

To configure predefined subtype filters

1 From the main menu, click Ethernet, and then click Predefined Subtype Filters. The Predefined Subtype Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Predefined Subtype Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	Allow/Pass	SubType	Value
DIX-ARP	☑	DIX-EtherType	08 06
SNAP-ARP	☑	SNAP-EtherType	08 06
802.2-IPX-RIP	☑	802.2-IPX-Socket	04 53
802.2-IPX-SAP	☑	802.2-IPX-Socket	04 52
NNL	☑	DIX-EtherType	87 5b
NETBIOS	☑	802.2-SAP	f0 f0
ICMP	☑	DIX-IP-Protocol	00 01

2 For each frame subtype field, check or clear the check box to configure if the frame subtypes are passed or are dropped. If you check the check box, the frame subtype is allowed to pass.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" in Chapter 1.

Customizing Subtype Filters

You can configure the access point to pass or drop certain customized frame subtypes. You define the action, subtype, and value parameters.

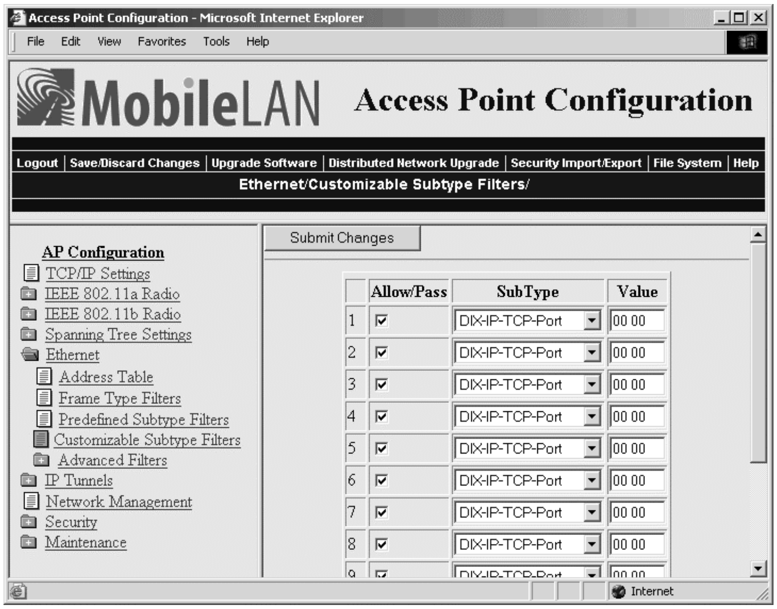
Allow/ Pass Check or clear this check box. Check this check box to pass all frames of the subtype and value. Clear this check box to drop all frames of the subtype and value.

Subtype Selects the frame subtype you wish to configure.

Value The following table describes frame subtypes and their values. The value must be two hex pairs. When a match is found between frame subtype and value, the specified action is taken.

To customize subtype filters

1 From the main menu, click Ethernet, and then click Customizable Subtype Filters. The Customizable Subtype Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Customizable Subtype Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	Allow/Pass	SubType	Value
1	☑	DIX-IP-TCP-Port	00 00
2	☑	DIX-IP-TCP-Port	00 00
3	☑	DIX-IP-TCP-Port	00 00
4	☑	DIX-IP-TCP-Port	00 00
5	☑	DIX-IP-TCP-Port	00 00
6	☑	DIX-IP-TCP-Port	00 00
7	☑	DIX-IP-TCP-Port	00 00
8	☑	DIX-IP-TCP-Port	00 00
9	☑	DIX-IP-TCP-Port	00 00

2 For each subtype field, check or clear the check box to configure if the subtypes are passed or are dropped. If you check the check box, the subtype is allowed to pass.

3 Click the down arrow on the right side of the SubType field and choose the customizable frame subtype. For help, see the next table.

4 Click the down arrow on the right side of the Value field and enter the two hex pairs. For help, see the next table.

5 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

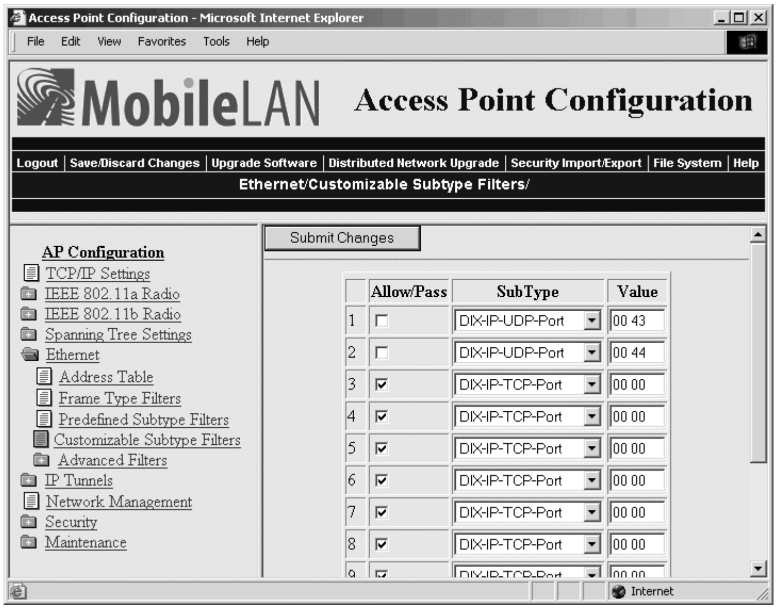
Subtype Filter Descriptions

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.

Example

This example shows you how to use customizable filters to only allow the wireless end devices (DHCP clients) that are communicating with the access point (DHCP server) to receive TCP/IP settings. This example prevents the wireless end devices from receiving TCP/IP settings from another DHCP server on the Ethernet network. It also prevents the access point from providing TCP/IP settings to DHCP clients on the wired network.

For this example, set these customizable subtype filters.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Customizable Subtype Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	Allow/Pass	SubType	Value
1	□	DIX-IP-UDP-Port	00 43
2	□	DIX-IP-UDP-Port	00 44
3	☑	DIX-IP-TCP-Port	00 00
4	☑	DIX-IP-TCP-Port	00 00
5	☑	DIX-IP-TCP-Port	00 00
6	☑	DIX-IP-TCP-Port	00 00
7	☑	DIX-IP-TCP-Port	00 00
8	☑	DIX-IP-TCP-Port	00 00
9	☑	DIX-IP-TCP-Port	00 00

Example – Customizable Subtype Filter

Filter	Parameter	Value	Explanation
1	Allow/Pass Subtype Value	Clear (drop) DIX-IP-UDP-Port 00 43	This filter drops DHCP responses to wireless end devices communicating with this access point.

Filter	Parameter	Value	Explanation
2	Allow/Pass Subtype Value	Clear (drop) DIX-IP-UDP-Port 00 44	This filter drops DHCP requests from DHCP clients on the Ethernet network.

Configuring Advanced Filters

You can configure 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.

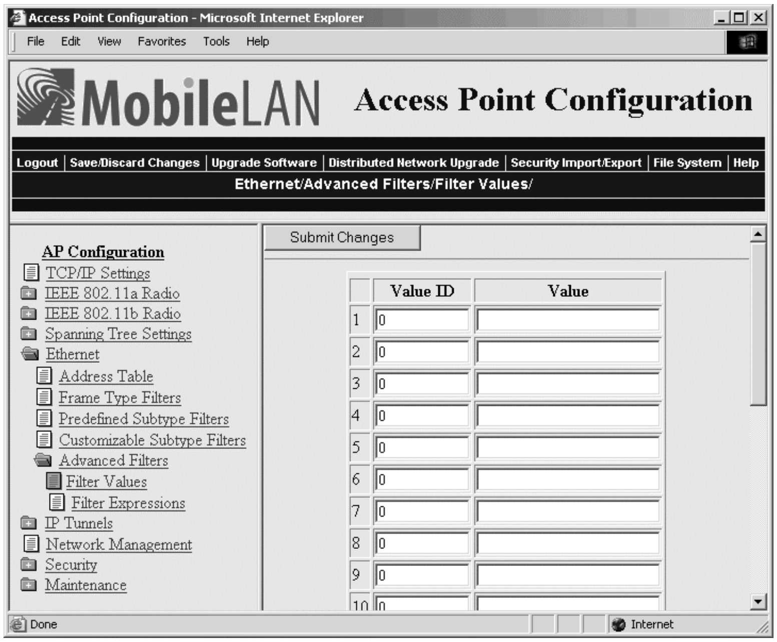
You can use filter values and filter expressions to minimize network traffic over the wireless links; however, Intermec recommends that you use advanced Ethernet filters only if you have an extensive understanding of network frames and their contents. Use other existing filters whenever possible.

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 From the main menu, click Ethernet, and then click Advanced Filters. The Filter Values screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Advanced Filters/Filter Values/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
Filter Values
Filter Expressions
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Done
Internet

	Value ID	Value
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	0	

2 Enter up to 22 value IDs and values.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

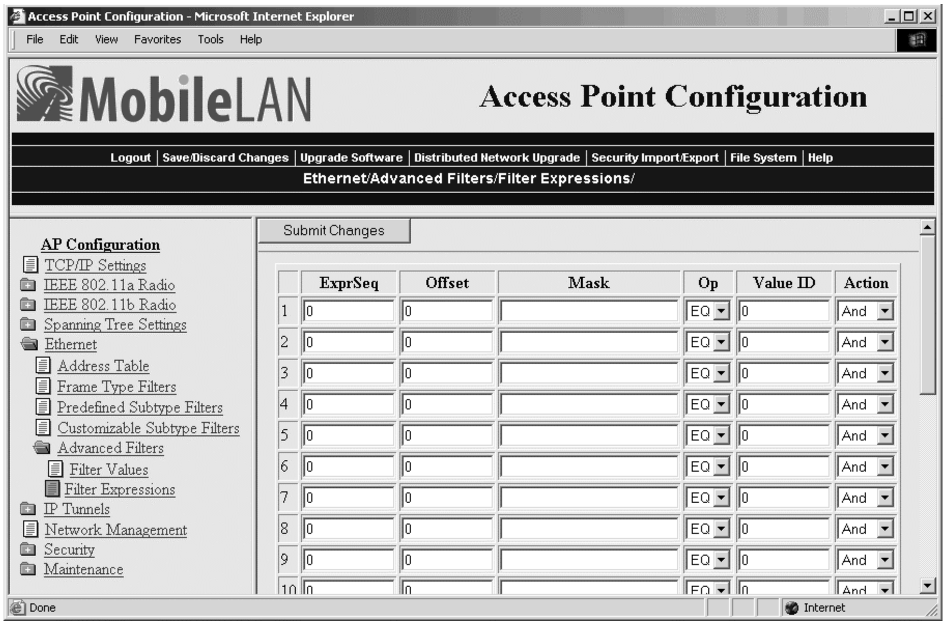
Setting Filter Expressions

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

To set filter expressions

1 From the main menu, click Ethernet, and then click Advanced Filters.

2 Click Filter Expressions. The Filter Expressions screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Advanced Filters/Filter Expressions/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
Filter Values
Filter Expressions
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Done
Internet

	ExprSeq	Offset	Mask	Op	Value ID	Action
1	0	0		EQ	0	And
2	0	0		EQ	0	And
3	0	0		EQ	0	And
4	0	0		EQ	0	And
5	0	0		EQ	0	And
6	0	0		EQ	0	And
7	0	0		EQ	0	And
8	0	0		EQ	0	And
9	0	0		EQ	0	And
10	0	0		EQ	0	And

3 Configure the filter expressions parameters. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Filter Expressions Parameter Descriptions

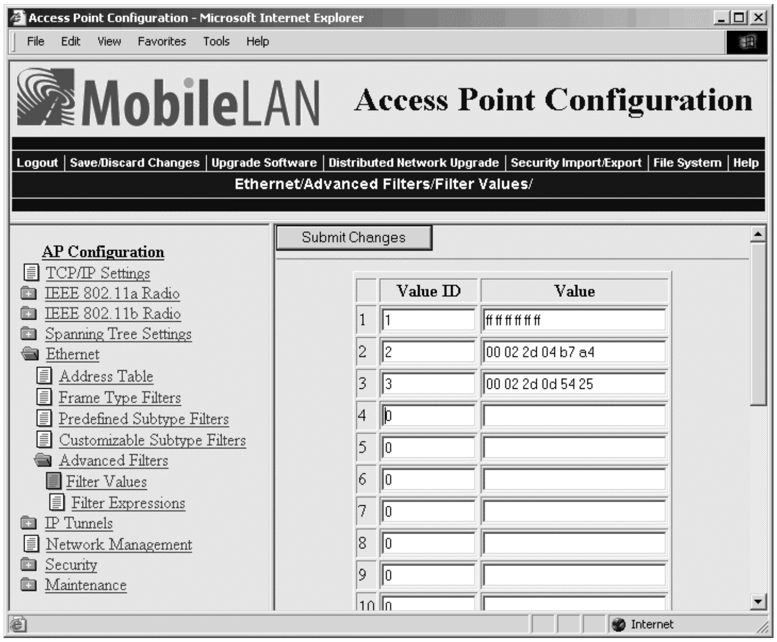
Parameter	Explanation
ExprSeq (Expression Sequence)	Indicates the order in which the filters will be executed. When you change the parameter, the statements are reordered and renumbered so the Expression Sequence order is maintained. The range is from 0 to 255. This parameter works with the Action parameter; for example, if the action is set to And, then the next sequence in another expression is processed.
Offset	Identifies a point inside the frame where testing for the expression is to start. The range is from 0 to 65535.
Mask	Applies a data pattern to the frame. If the data pattern in the mask matches the frame, 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.
Op (Operation)	Performs a logical operation when a data pattern matches a value in the Filter Values menu 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)

Filter Expressions Parameter Descriptions (continued)

Parameter	Explanation
Value ID	Represents a value in the Filter Values menu. The bytes after the frame 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	Sets the action to Pass, Drop, or And. If you set the action to And, the filter expression with the next highest sequence is applied.

Example 1

This example shows you how to use Ethernet filters to filter all traffic that passes through the access point to the wireless network except for traffic for specified MAC addresses. These filters do not prevent wireless traffic from reaching the Ethernet network. For this example, set these filter values.

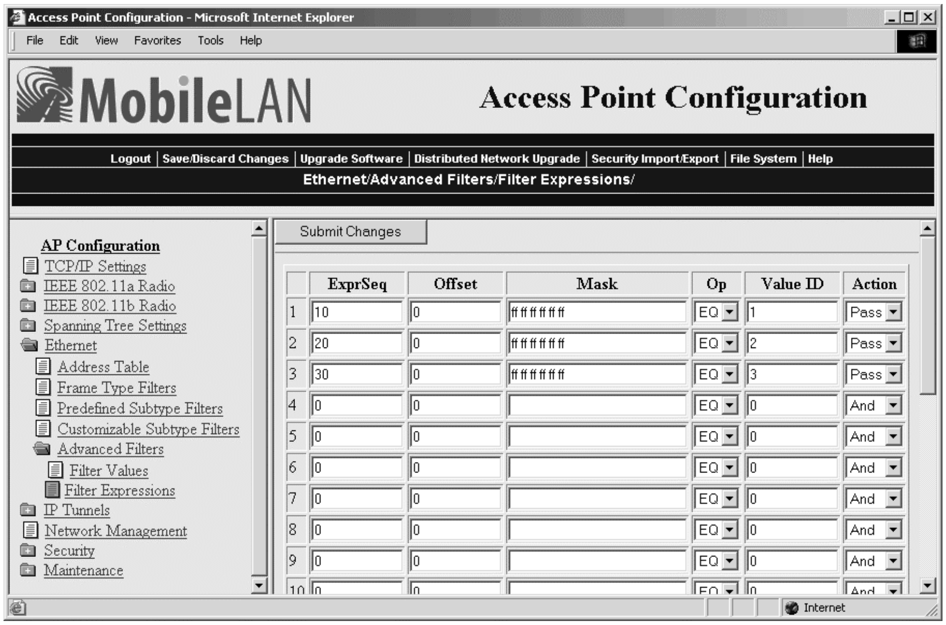

Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Advanced Filters/Filter Values/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
Filter Values
Filter Expressions
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	Value ID	Value
1	1	ff ff ff ff ff ff
2	2	00 02 2d 04 b7 a4
3	3	00 02 2d 0d 54 25
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	0	

Example 1 - Filter Values

Value ID	Value	Description
1	ff ff ff ff ff ff	Allows multicast traffic to enter the wireless network, which is necessary for IP end devices to communicate
2	00 02 2d 04 b7 a4	The MAC address of an end device you want to be able to communicate.
3	00 02 2d 0d 54 25	The MAC address of an end device you want to be able to communicate.

For this example, set these filter expressions.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Advanced Filters/Filter Expressions/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
Filter Values
Filter Expressions
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	ExprSeq	Offset	Mask	Op	Value ID	Action
1	10	0	ff ff ff ff ff ff	EQ	1	Pass
2	20	0	ff ff ff ff ff ff	EQ	2	Pass
3	30	0	ff ff ff ff ff ff	EQ	3	Pass
4	0	0		EQ	0	And
5	0	0		EQ	0	And
6	0	0		EQ	0	And
7	0	0		EQ	0	And
8	0	0		EQ	0	And
9	0	0		EQ	0	And
10	0	0		EQ	0	And

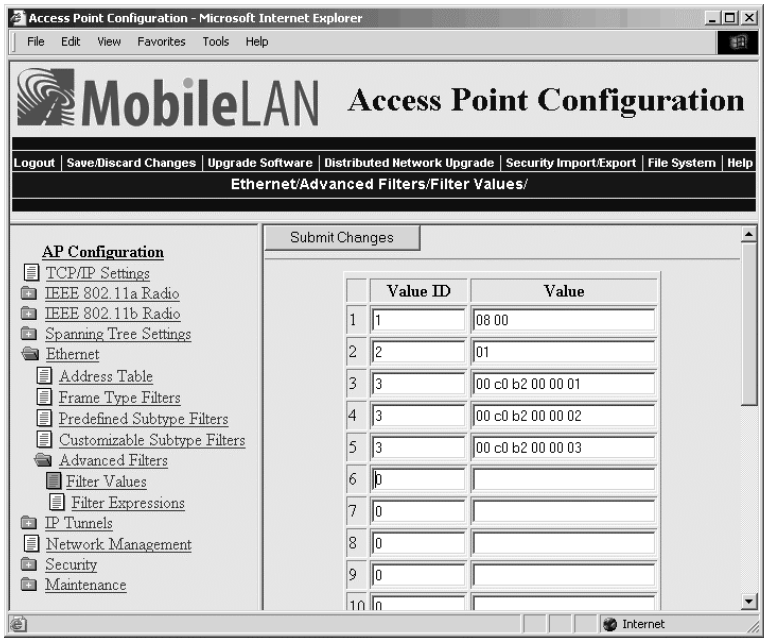
Example 1 –Filter Expressions

Parameter	Value	Explanation
ExprSeq	10	The order that you want the expressions executed. You must have an expression for each Value ID that is listed in the Filter Values menu.
Offset	0	Since the filter is applied to the destination address, which is the first value in the frame, the offset is 0.
Mask	ff ff ff ff ff ff	Compares the entire 6-byte destination address for an exact match.
Op	EQ	Compares the value after the offset and mask are applied to the value of the Value ID from 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.)
Value ID	1	This filter expression applies to value ID 1 from the Filter Values menu.
Action	Pass	If this filter expression is true, continue to the next expression.

You must enter a filter expression for each Value ID in the Filter Values menu. In this example, only the ExprSeq value and the Value ID value change.

Example 2

This example shows how to use Ethernet filters to discard all DIX IP multicast frames except those from selected devices. Three entries have a value ID of 3 to demonstrate how to enter a list. All entries with the same value ID belong to the same list. For this example, set these filter values.



	Value ID	Value
1	1	08 00
2	2	01
3	3	00 c0 b2 00 00 01
4	3	00 c0 b2 00 00 02
5	3	00 c0 b2 00 00 03
6	0	
7	0	
8	0	
9	0	
10	0	

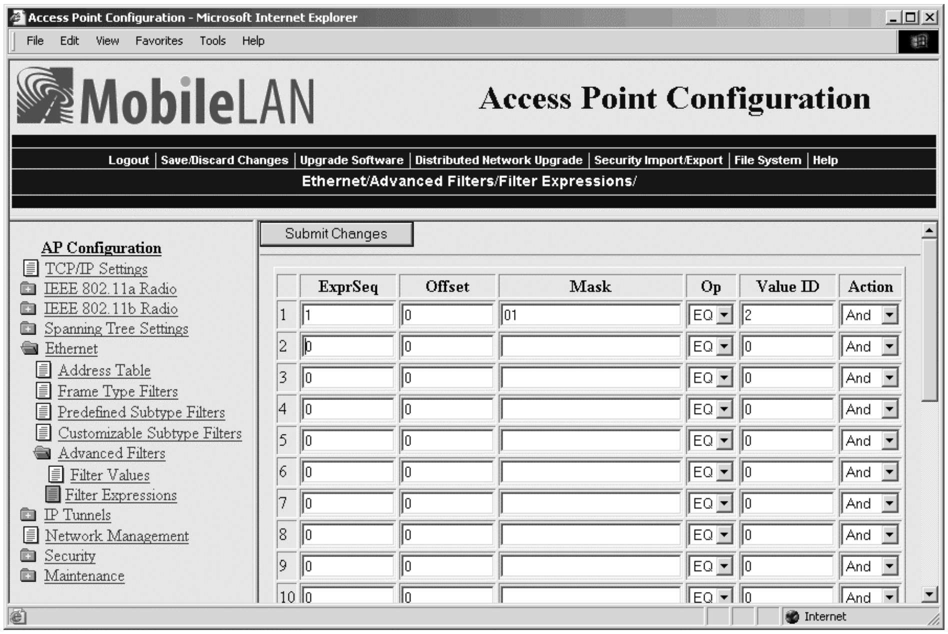
Example 2 - Filter Values

Value ID	Value	Description
1	08 00	Check for a DIX IP frame.
2	01	Check for a multicast frame.
3	00 c0 b2 00 00 01 00 c0 b2 00 00 02 00 c0 b2 00 00 03	Check for these specific MAC device addresses.

You must enter a filter expression for each Value ID in the Filter Values menu. In this example, three expressions 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 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.

Set the first filter expression as shown below.

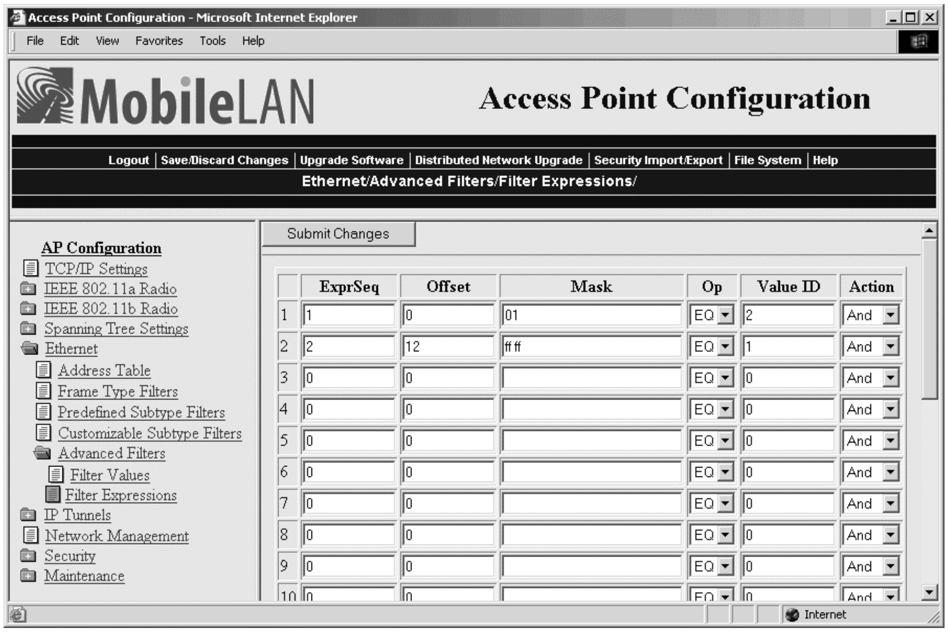

Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Advanced Filters/Filter Expressions/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
Filter Values
Filter Expressions
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	ExprSeq	Offset	Mask	Op	Value ID	Action
1	1	0	01	EQ	2	And
2	0	0		EQ	0	And
3	0	0		EQ	0	And
4	0	0		EQ	0	And
5	0	0		EQ	0	And
6	0	0		EQ	0	And
7	0	0		EQ	0	And
8	0	0		EQ	0	And
9	0	0		EQ	0	And
10	0	0		EQ	0	And

Example 2 – First Filter Expression

Parameter	Value	Explanation
ExprSeq	1	The first expression that is executed. You must have an expression for each Value ID that is listed in the Filter Values menu.
Offset	0	Since the filter is applied to the destination address, which is the first value in the frame, the offset is 0.
Mask	01	Checks only the Ethernet multicast bit.
Op	EQ	Compares the value after the offset and mask are applied to the value of the Value ID from 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.)
Value ID	2	This filter expression applies to value ID 2 from the Filter Values menu.
Action	And	If this filter expression is true, continue to the next expression.

Set the second filter expression as shown below.

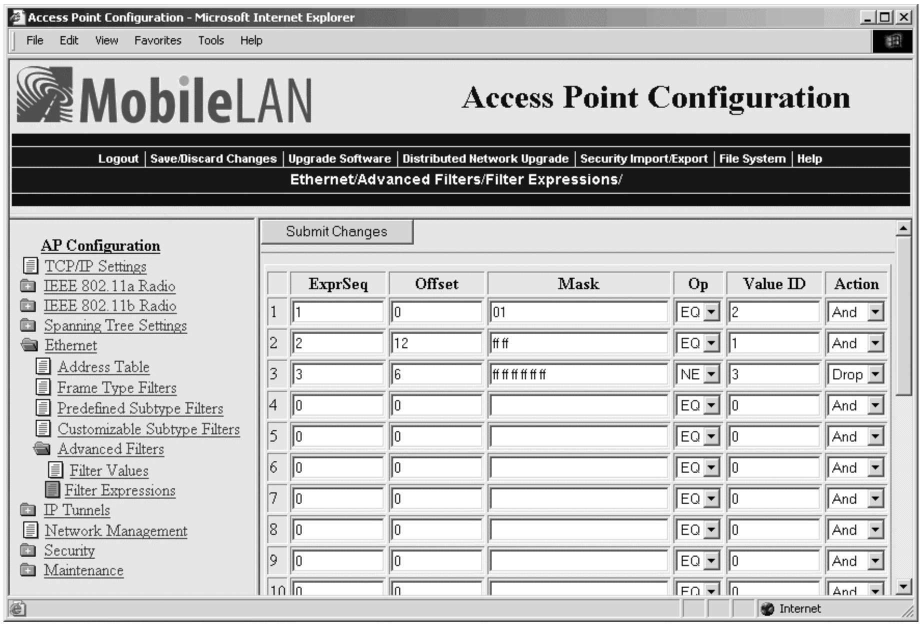

Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Ethernet/Advanced Filters/Filter Expressions/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Address Table
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Advanced Filters
Filter Values
Filter Expressions
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	ExprSeq	Offset	Mask	Op	Value ID	Action
1	1	0	01	EQ	2	And
2	2	12	ff ff	EQ	1	And
3	0	0		EQ	0	And
4	0	0		EQ	0	And
5	0	0		EQ	0	And
6	0	0		EQ	0	And
7	0	0		EQ	0	And
8	0	0		EQ	0	And
9	0	0		EQ	0	And
10	0	0		EQ	0	And

Example 2 – Second Filter Expression

Parameter	Value	Explanation
ExprSeq	2	The second expression that is executed.
Offset	12	Checks for the DIX IP frame type, which starts 12 bytes from the destination address.
Mask	ff ff	Checks the 2-byte DIX IP frame type for an exact match.
Op	EQ	Compares the value after the offset and mask are applied to the value of the Value ID from 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.)
Value ID	1	This filter expression applies to value ID 1 from the Filter Values menu.
Action	And	If this filter expression is true, continue to the next expression.

Set the third filter expression as shown below.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Submit Changes
Internet

Ethernet/Advanced Filters/Filter Expressions/

AP Configuration
- TCP/IP Settings
- IEEE 802.11a Radio
- IEEE 802.11b Radio
- Spanning Tree Settings
- Ethernet
  - Address Table
  - Frame Type Filters
  - Predefined Subtype Filters
  - Customizable Subtype Filters
  - Advanced Filters
    - Filter Values
    - Filter Expressions
- IP Tunnels
- Network Management
- Security
- Maintenance

	ExprSeq	Offset	Mask	Op	Value ID	Action
1	1	0	01	EQ	2	And
2	2	12	ff ff	EQ	1	And
3	3	6	ff ff ff ff ff ff	NE	3	Drop
4	0	0		EQ	0	And
5	0	0		EQ	0	And
6	0	0		EQ	0	And
7	0	0		EQ	0	And
8	0	0		EQ	0	And
9	0	0		EQ	0	And
10	0	0		EQ	0	And

Example 2 – Third Filter Expression

Parameter	Value	Explanation
ExprSeq	3	The third expression that is executed.
Offset	6	Checks the source Ethernet address, which starts 6 bytes from the destination address.
Mask	ff ff ff ff ff ff	Checks the 6-byte source Ethernet address for an exact match.
OP	NE	Compares the value after the offset and mask are applied to the value of the Value ID from the Filter Values menu to see if they are not equal. (Compare the source Ethernet address with the list of MAC addresses from the Filter Values menu.)
Value ID	3	This filter expression applies to value ID 3 from the Filter Values menu.
Action	Drop	If the source Ethernet address does not match any address in the list on the Filter Values menu, then drop the frame.

4 Configuring the Radios

This chapter explains how to configure the radios in the MobileLAN access products so that they communicate with your wireless end devices. This chapter covers these topics:

- Configuring the IEEE 802.11b radio
- Configuring the IEEE 802.11a radio
- Configuring the WLI Forum OpenAir radio
- Configuring the 902 MHz radio
- Configuring the S-UHF radio

About the Radios

MobileLAN access products may contain one or two radios. You can use access points that contain two different types of radios to support two different types of wireless networks, such as legacy networks. You can use access points with two of the same type of radios as WAPs, as point-to-multipoint bridges, to increase throughput in a busy network, or to provide redundancy.

Access Point Radios Supported and Features

Access Point	Radios Supported	Dual Radio Support	Radio Independent
WA22	802.11b, 802.11a	Yes	Yes
2101	802.11b, OpenAir	Yes	Yes
WA21	802.11b, 802.11a	Yes	Yes
2100	802.11b, OpenAir 902 MHz, S-UHF	Yes	Yes
2102	802.11b, OpenAir	No	Yes
2106	802.11a	No	No

The next sections explain how to configure the radios that are in your access point. If the radio is not installed in your access point, then you will not see it listed in the main menu.

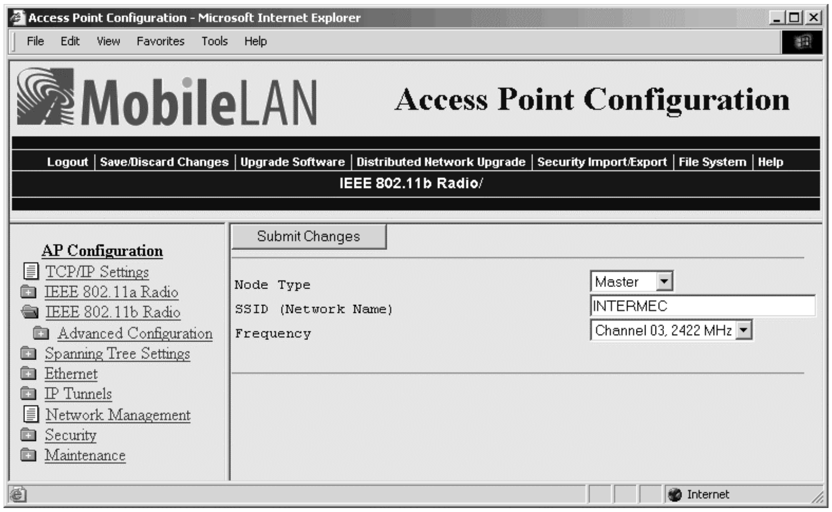
Configuring the IEEE 802.11b Radio

The IEEE 802.11b radio will communicate with other 802.11b radios that have the same

- SSID (Network Name).
- security. For help, see Chapter 6, "Configuring Security."

To configure the 802.11b radio

1 From the main menu, click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IEEE 802.11b Radio/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Advanced Configuration
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

Node Type: Master
SSID (Network Name): INTERMEC
Frequency: Channel 03, 2422 MHz

2 Configure the parameters for the radio. For help, see the next table.

3 Configure the advanced parameters for the radio. For help, see "Configuring 802.11b Radio Advanced Parameters" later in this section.

4 (Master only) Configure inbound filters. For help, see "Configuring 802.11b Radio Inbound Filters" later in this section.

5 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" in Chapter 1.

802.11b Radio Parameter Descriptions

Parameter	Explanation
Node Type	Configure the 802.11b radio as a master or station. You can also disable the radio.
SSID (Network Name)	Enter the network name for this access point. 802.11b radios communicate with other 802.11b radios with the same network name. You need to assign the same network name to the wireless end devices that will connect to the access point. The network name is case sensitive and can be no more than 32 alphanumeric characters.
Frequency (Master radio only)	Choose the frequency within the 2.4 to 2.5 GHz range that this access point uses to transmit and receive frames. The available frequencies are country-dependent and are determined by the radio. See the “Worldwide Frequencies for the 802.11b Radio” table. Configure all access points used in Spain, France, or Japan to a common frequency. For all other countries, configure all access points to a common frequency, or select up to three frequencies that are at least three channels (or 25 MHz) apart. For example, you could select 2412 MHz, 2437 MHz, and 2462 MHz. You may want to use a single frequency to isolate the installation to part of the band; for example, use a single frequency if other wireless networks or microwave ovens are in the area. For optimal performance of master radios in access points that are in range of each other, configure the frequencies to be at least five channels apart. For example, configure the frequency to use channels 1, 6, and 11.

Worldwide Frequencies for the 802.11b Radio

Channel	FCC	ETSI	France	Japan	Israel
1	2412	2412		2412	
2	2417	2417		2417	
3	2422 (default)	2422 (default)		2422 (default)	2422 (default)
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	

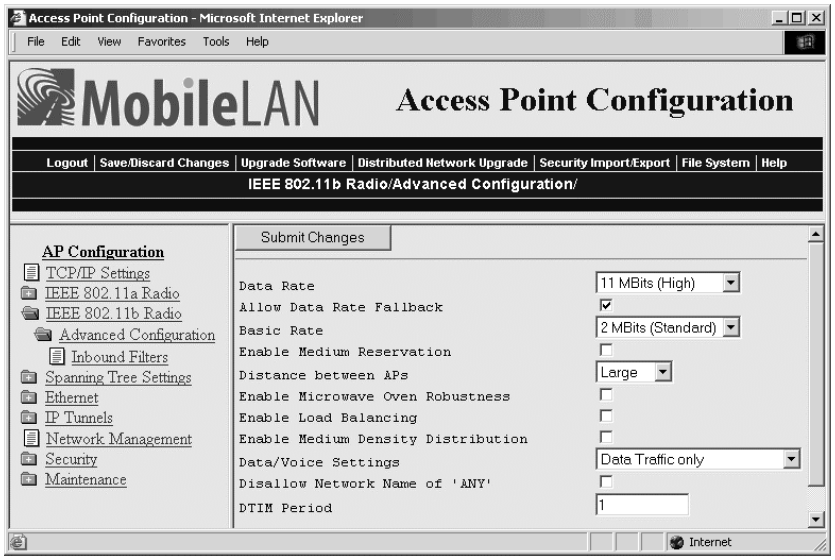
The 802.11b channels that are allowed in a given country may change without notice. Be sure you use only those frequencies that are permissible in the given country. Note the following:

- 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.
- France, Mexico, and Singapore use the same channels.

Configuring 802.11b Radio Advanced Parameters

1 From the main menu, click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears.

2 Click Advanced Configuration. The Advanced Configuration screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IEEE 802.11b Radio/Advanced Configuration/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Advanced Configuration
Inbound Filters
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

Data Rate	11 MBits (High)
Allow Data Rate Fallback	☑
Basic Rate	2 MBits (Standard)
Enable Medium Reservation	□
Distance between APs	Large
Enable Microwave Oven Robustness	□
Enable Load Balancing	□
Enable Medium Density Distribution	□
Data/Voice Settings	Data Traffic only
Disallow Network Name of 'ANY'	□
DTIM Period	1

3 Configure the advanced parameters. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

802.11b Radio Advanced Parameter Descriptions

Parameter	Description
Data Rate	Choose the rate at which the access point transmits data. In general, higher speeds mean shorter range and lower speeds mean longer range. You can set this rate to 11, 5.5, 2, or 1 Mbps.
Allow Data Rate Fallback	Determines if you want the radio to drop to a slower data rate when it has trouble communicating with another radio.
Basic Rate	Choose the rate at which the access point transmits multicast and beacon frames. In general, higher speeds mean shorter range and lower speeds mean longer range. Do not set this rate higher than the maximum rate at which your end devices can receive multicast frames. You can set this rate to 11, 5.5, 2, or 1 Mbps. This parameter should usually be left at the default 2 Mbps.
Enable Medium Reservation	Determines if you want to specify a reservation threshold. Check this check box to set a threshold value. If you clear this check box, you may improve network response time in installations that usually send very small frames or that have no hidden stations.
Reservation Threshold	If you enable medium reservation, you need to set a threshold value, which is the largest data frame that can be transmitted without reserving air time. Air time is normally reserved to help prevent collisions with other transmitters.
Distance Between APs	Controls the roaming sensitivity of your end devices. This setting should match the setting on your end devices. You can use this parameter to virtually reduce the range of your access point. If you choose Small or Medium, you do not reduce the absolute range of your radio, but you modify the collision detection mechanism to allow significant overlap of the wireless cells. Thus, you create a higher performance radio network, but you need more access points to cover an area.
Enable Microwave Oven Robustness	Determines if the access point activates a modified algorithm for automatic rate fallback, which prevents the access point from falling back to 1 Mbps when trying to retransmit radio frames when 2.4 GHz interference is present.
Enable Load Balancing	Determines if end devices can distribute their connections across multiple access points.
Enable Medium Density Distribution	Determines if these access point parameters—Enable Medium Reservation, Distance Between APs, Enable Microwave Oven Robustness—are distributed to end devices that support this feature.

802.11b Radio Advanced Parameter Descriptions (continued)

Parameter	Description
Data/Voice Settings (Master radio only)	Choose the setting that optimizes the wireless network. Set to Data Traffic Only if the access point will transmit only data traffic. Set to SpectraLink Traffic Only if the access point will transmit only voice traffic. MobileLAN™voice 2 telephone frames will be sent with a priority setting. All other multicast/broadcast frames will be dropped. Set to Data and SpectraLink Traffic if the access point will transmit both data and voice traffic. MobileLAN voice 2 telephone frames will be sent in the high priority queue. Frames in the high priority queue are sent ahead of frames in the normal priority queue. No special filtering.
Disallow Network Name of 'ANY' (Master radio only)	Determines if end devices that have their SSID (Network Name) set to ANY or are left blank can associate with this access point. Check this check box to allow these end devices to associate with this access point. This setting is 802.11b compliant, but not very secure. Clear this check box to prevent end devices with an SSID of ANY or are left blank from associating with this access point.
DTIM Period (Master radio only)	Specifies the number of beacon frames to skip before including a DTIM (delivery traffic indication message) in a beacon frame. Setting a higher DTIM period may conserve battery life in an end device, but it may increase response time.

Configuring 802.11b Radio Inbound Filters

When configuring a master radio, you can filter different types of wireless traffic that it may receive. You may want to use this feature by itself or with an access control list (ACL) to help secure your network. If you clear all the check boxes, the radio cannot communicate with any other radios. You check the Allow IAPP check box so the access point can communicate with other access points and participate in the spanning tree.

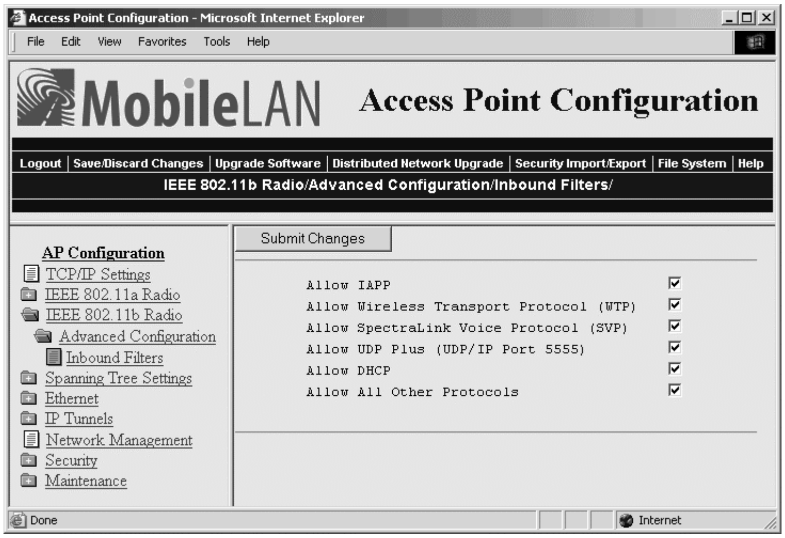
You can use this feature to form a secure wireless hop. Clear all check boxes, except for the Allow IAPP check box. Or, you may want to use this feature in a terminal emulation environment when you know the end devices are sending only UDP Plus or Wireless Transport Protocol (WTP) frames. Check the Allow UDP Plus check box or the Allow Wireless Transport Protocol check box and clear all other check boxes (except the Allow IAPP check box). The access point master radio will only accept the UDP Plus or WTP frames and discard all other frames, which can make a more secure network.

Note: If any of the devices are also DHCP clients, you need to check the Allow DHCP check box.

To configure 802.11b radio inbound filters

1 From the main menu, click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears.

2 Click Advanced Configuration, and then click Inbound Filters. The Inbound Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IEEE 802.11b Radio/Advanced Configuration/Inbound Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Advanced Configuration
Inbound Filters
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Done
Internet

```
Allow IAPP                                   ☑
Allow Wireless Transport Protocol (WTP)      ☑
Allow SpectraLink Voice Protocol (SVP)       ☑
Allow UDP Plus (UDP/IP Port 5555)            ☑
Allow DHCP                                   ☑
Allow All Other Protocols                    ☑
```

3 For each frame type, check or clear each check box. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

802.11b Radio Inbound Filter Descriptions

Parameter	Description
Allow IAPP	Determines if this radio accepts IAPP frames from other access point station radios. The IAPP frames must match Ethernet protocol 875c.
Allow Wireless Transport Protocol (WTP)	Determines if this radio accepts WTP frames from end devices. The WTP frames must match Ethernet protocol 875b.
Allow SpectraLink Voice Protocol (SVP)	Determines if this radio accepts SVP frames from MobileLAN voice wireless telephones. The SVP frames must match IP 119.
Allow UDP Plus (UDP/IP Port 5555)	Determines if this radio accepts UDP Plus frames from end devices. The UDP Plus frames must match the UDP network port 5555 on the DCS 30X or ARP.
Allow DHCP	Determines if this radio accepts DHCP frames. The DHCP frames must match UDP destination port 67 and ARP. Check this check box if the end devices are DHCP clients.
Allow All Other Protocols	Determines if this radio accepts all other protocols that are not filtered by one of the filters in this screen.

Configuring a MobileLAN voice Network

MobileLAN voice wireless telephone systems simplify network infrastructure and network management by combining voice and data traffic over one wireless network, leveraging 802.11b wireless LAN technology. You use your MobileLAN voice telephone to make and receive calls, just like a regular telephone, subject to the restrictions of your PBX.

MobileLAN voice telephones and gateways operate as adjuncts to existing wireless LANs and PBXs. The MobileLAN voice networks use sophisticated digital spread spectrum radio technology and have highest level of integration with enterprise telephone switching and networking systems. This provides the best voice quality possible throughout the coverage area because there are no clicks, no fading, and no dead spots.

If you are using the MobileLAN voice network with your wireless data collection network, you need to configure an 802.11b radio port to accept voice traffic. An 802.11b radio can support both voice and data communications. You still need to define the normal 802.11b parameters, such as SSID (Network Name) and security.

MobileLAN voice Network - Number of Phones Supported

Access Point	Number of 802.11b Radios	Number of Phones Supported (Voice Only)	Number of Phones Supported (Voice and Data)
WA21, WA22, 2101 (any), 2100 (any)	2	7 per radio (both radios set to voice traffic only)	7 (one radio set to voice traffic only, the other radio dedicated to data or data and voice traffic)
WA21, WA22, 2101B, 2100D	1	7	7
2101A, 2100A, 2100B, 2100C	1	7	5
2102	1	7	5

To configure a MobileLAN voice network

1 From the main menu, click IEEE 802.11b Radio. The IEEE 802.11b Radio screen appears.

Note: If your access point contains dual radios, use a different SSID (Network Name) for each radio so you can specify which end devices/telephones attach to which radio. You also must enter the Network Name on each telephone.

2 Click Advanced Configuration. The Advanced Configuration screen appears.

3 Click the down arrow on the right side of the Data/Voice Settings field and choose either Data and SpectraLink Traffic or SpectraLink Traffic only. For help, see “Configuring 802.11b Radio Advanced Parameters” earlier in this chapter.

4 Check the Allow Data Rate Fallback check box.

5 Click the down arrow on the right side of the Basic Rate field.

- If you are using a 2 Mbps MobileLAN voice 2 telephone, set the Basic Rate to 2 Mbps.
- If you are using a 1 Mbps MobileLAN voice 2 telephone, set the Basic Rate to 1 Mbps.

6 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Configuring the IEEE 802.11a Radio

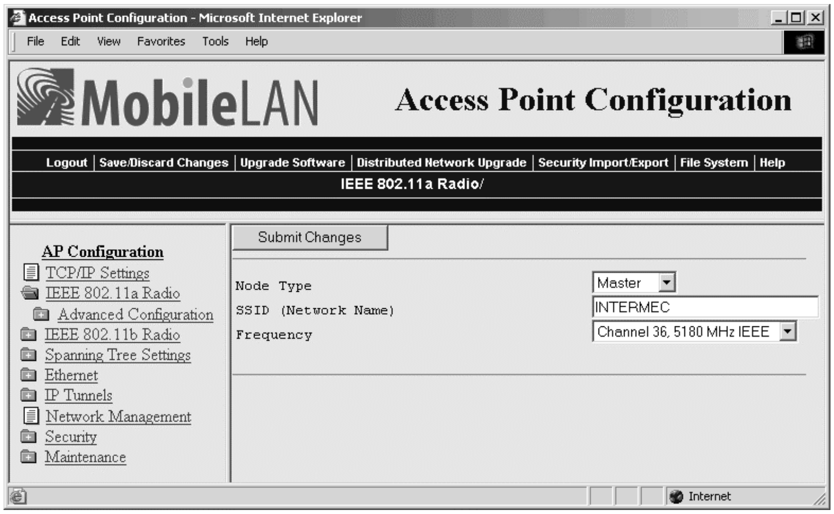
The IEEE 802.11a radio will communicate with other 802.11a radios that have the same

- SSID (Network Name).
- security. For help, see Chapter 6 “Configuring Security.”

The 802.11a radio ships with either the full range (5.15 to 5.35 GHz) option or the mid range (5.25 to 5.35 GHz) option. The full range option can only be used indoors and with the integrated antenna.

To configure the 802.11a radio

1 From the main menu, click IEEE 802.11a Radio. The IEEE 802.11a Radio screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IEEE 802.11a Radio/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
Advanced Configuration
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

Node Type Master

SSID (Network Name) INTERMEC

Frequency Channel 36, 5180 MHz IEEE

2 Configure the parameters for the radio. For help, see the next table.

3 Configure the advanced parameters for the radio. For help, see "Configuring 802.11a Radio Advanced Parameters" later in this section.

4 (Master only) Configure inbound filters. For help, see "Configuring 802.11a Radio Inbound Filters" later in this section.

5 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" in Chapter 1.

802.11a Radio Parameter Descriptions

Parameter	Explanation
Node Type	Configure the 802.11a radio as a master or station. You can also disable the radio.
SSID (Network Name)	Enter the network name for this access point. 802.11a radios communicate with other 802.11a radios with the same network name. You need to assign the same network name to the wireless end devices that will connect to the access point. The network name is case sensitive and can be no more than 32 alphanumeric characters.
Frequency (Master radio only)	Choose the frequency within the 5.15 to 5.35 GHz range that this access point uses to transmit and receive frames. The available frequencies depend on the country and the radio option configured on the access point. See the "Worldwide Frequencies for the 802.11a Radio" table. If the radio is a mid range radio, you can only choose 52, 56, 60, or 64. 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 wireless networks or microwave ovens are in the area.

Worldwide Frequencies for the 802.11a Radio

Channel	FCC	ETSI	France	Japan	Israel
36*	5180 (default)	N/A	N/A	N/A	N/A
40*	5200	N/A	N/A	N/A	N/A
42	5210 Turbo	N/A	N/A	N/A	N/A
44*	5220	N/A	N/A	N/A	N/A
48*	5240	N/A	N/A	N/A	N/A
50	5250 Turbo	N/A	N/A	N/A	N/A
52	5260 (default)	N/A	N/A	N/A	N/A
56	5280	N/A	N/A	N/A	N/A
58	5290 Turbo	N/A	N/A	N/A	N/A
60	5300	N/A	N/A	N/A	N/A
64	5320	N/A	N/A	N/A	N/A

- Channels marked with an asterisk (*) are not available in the mid range radio.
- FCC countries include the United States, Canada, China, Taiwan, India, Thailand, Indonesia, Malaysia, Hong Kong, and most South American countries. The 802.11a 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.

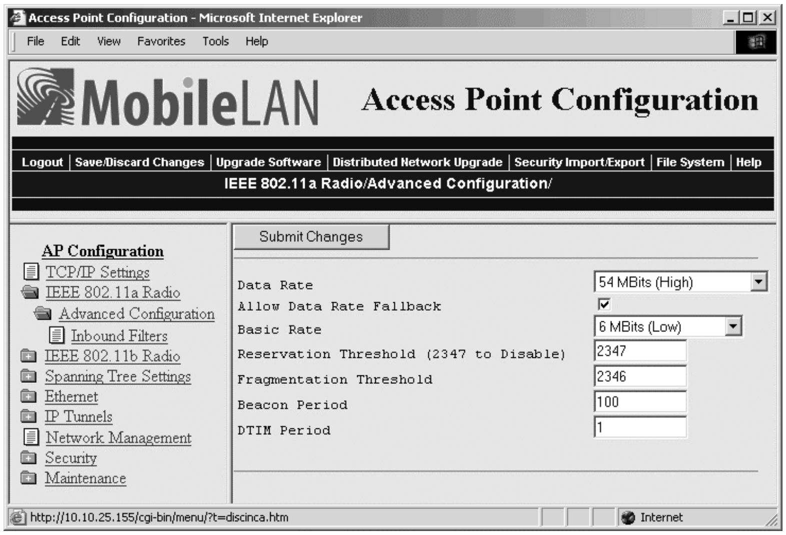
Configuring 802.11a Radio Advanced Parameters

You can configure other advanced parameters for the 802.11a radio, such as Data Rate and Medium Reservation.

To configure other advanced parameters

1 From the main menu, click IEEE 802.11a Radio. The IEEE 802.11a Radio screen appears.

2 Click Advanced Configuration. The Advanced Configuration screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IEEE 802.11a Radio/Advanced Configuration/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
Advanced Configuration
Inbound Filters
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
http://10.10.25.155/cgi-bin/menu/?t=discinca.htm
Internet

Data Rate	54 MBits (High)
Allow Data Rate Fallback	☑
Basic Rate	6 MBits (Low)
Reservation Threshold (2347 to Disable)	2347
Fragmentation Threshold	2346
Beacon Period	100
DTIM Period	1

3 Configure the advanced parameters. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

802.11a Radio Advanced Parameter Descriptions

Parameter	Description
Data Rate	Choose the rate at which the access point transmits data. In general, higher speeds mean shorter range and lower speeds mean longer range. If you choose the Speed Mode to be 802.11 compliant, you can set this rate to 54, 48, 36, 24, 12, or 6 Mbps.
Allow Data Rate Fallback	Determines if you want the radio to drop to a slower data rate when it has trouble communicating with another radio.
Basic Rate	Choose the rate at which the access point transmits multicast and beacon frames. In general, higher speeds mean shorter range and lower speeds mean longer range. Do not set this rate higher than the maximum rate at which your end devices can receive multicast frames. You can set this rate to 24, 12, or 6 Mbps. This parameter should usually be left at the default of 6 Mbps.
Reservation Threshold	You may need to set a threshold value, which is the largest data frame that can be transmitted without reserving air time. Air time is normally reserved to help prevent collisions with other transmitters. If you set this threshold to 2347, this parameter is disabled.
Fragmentation Threshold	Specifies the largest data frame that can be transmitted without fragmentation. On certain radios, the fragmentation does not occur unless the radio detects interference. Larger frame sizes can improve throughput on a reliable connection. Smaller frame sizes can improve throughput on a poor connection.
Beacon Period	Specifies how often the access point sends out a beacon frame. This rate is in TU. A TU is 1024 microseconds, and is often considered to be equivalent to one millisecond.
DTIM Period	Specifies the number of beacon periods to skip before including a DTIM (delivery traffic indication message) in a beacon frame. Setting a higher DTIM period may conserve battery life in an end device, but it may increase response time.

Configuring 802.11a Radio Inbound Filters

When configuring a master radio, you can filter different types of wireless traffic that it may receive. You may want to use this feature by itself or with an access control list (ACL) to help secure your network. If you clear all the check boxes, the radio cannot communicate with any other radios. You check the Allow IAPP check box so the access point can communicate with other access points and participate in the spanning tree.

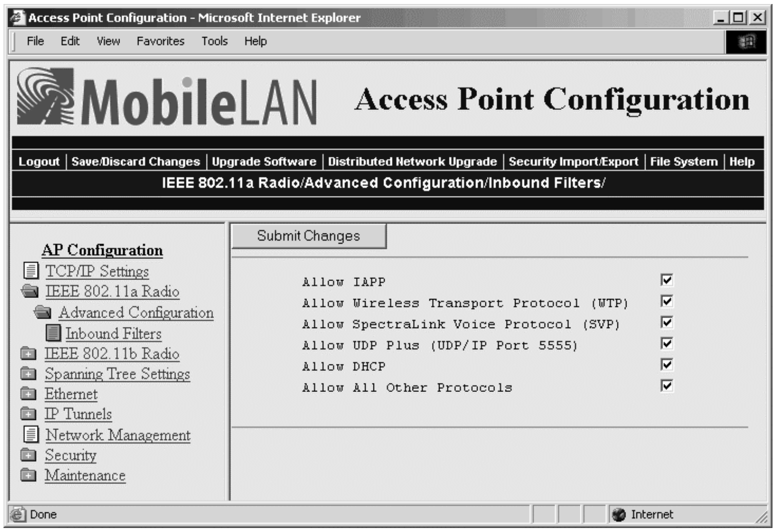
You can use this feature to form a secure wireless hop. Clear all check boxes, except for the Allow IAPP check box. Or, you may want to use this feature in a terminal emulation environment when you know the end devices are sending only UDP Plus or Wireless Transport Protocol (WTP) frames. Check the Allow UDP Plus check box or the Allow Wireless Transport Protocol check box and clear all other check boxes (except the Allow IAPP check box). The access point master radio will only accept the UDP Plus or WTP frames and discard all other frames, which can make a more secure network.

Note: If any of the devices are also DHCP clients, you need to check the Allow DHCP check box.

To configure 802.11a radio inbound filters

1 From the main menu, click IEEE 802.11a Radio. The IEEE 802.11a Radio screen appears.

2 Click Advanced Configuration, and then click Inbound Filters. The Inbound Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IEEE 802.11a Radio/Advanced Configuration/Inbound Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
Advanced Configuration
Inbound Filters
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Done
Internet

```
Allow IAPP                                  ☑
Allow Wireless Transport Protocol (WTP)     ☑
Allow SpectraLink Voice Protocol (SVP)      ☑
Allow UDP Plus (UDP/IP Port 5555)           ☑
Allow DHCP                                  ☑
Allow All Other Protocols                   ☑
```

3 For each frame type, check or clear each check box. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

802.11a Radio Inbound Filter Descriptions

Parameter	Description
Allow IAPP	Determines if this radio accepts IAPP frames from other access point station radios. The IAPP frames must match Ethernet protocol 875c.
Allow Wireless Transport Protocol (WTP)	Determines if this radio accepts WTP frames from end devices. The WTP frames must match Ethernet protocol 875b.
Allow SpectraLink Voice Protocol (SVP)	Determines if this radio accepts SVP frames from MobileLAN voice wireless telephones. The SVP frames must match IP 119.
Allow UDP Plus (UDP/IP Port 5555)	Determines if this radio accepts UDP Plus frames from end devices. The UDP Plus frames must match the UDP network port 5555 on the DCS 30X or ARP.
Allow DHCP	Determines if this radio accepts DHCP frames. The DHCP frames must match UDP destination port 67 and ARP. Check this check box if the end devices are DHCP clients.
Allow All Other Protocols	Determines if this radio accepts all other protocols that are not filtered by one of the filters in this screen.

Configuring the WLI Forum OpenAir Radio

The WLI Forum OpenAir radio will communicate with other OpenAir radios that have the same

- LAN ID (Domain). For help, see “Configuring the Spanning Tree Parameters” in Chapter 5.
- security ID.
- channel.
- subchannel.

You should configure each master radio with a unique channel/subchannel combination. When a station radio locates a master radio that has the same LAN ID and security ID as itself, it autoconfigures its channel and subchannel so it can communicate with the master radio.

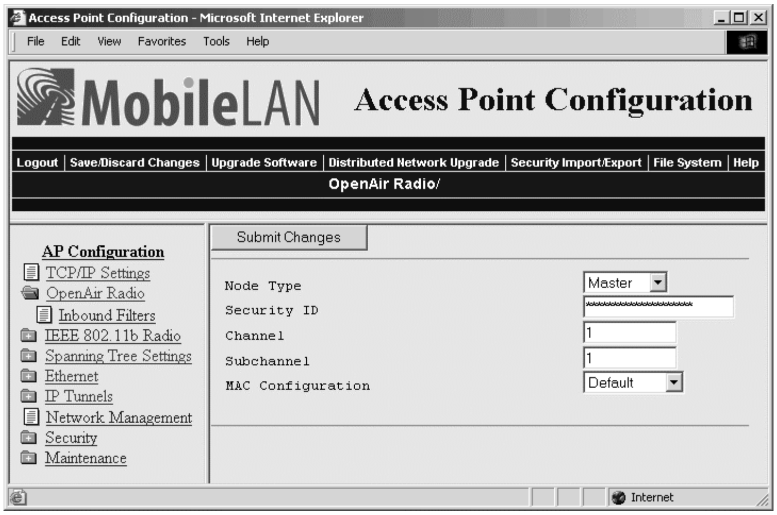
Caution

Intermec recommends that you set the security ID 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.

Attention: Intermec vous recommande de régler l'ID de sécurité 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.

To configure the OpenAir radio

1 From the main menu, click OpenAir Radio. The OpenAir Radio screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
OpenAir Radio/
Submit Changes
AP Configuration
TCP/IP Settings
OpenAir Radio
Inbound Filters
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Internet

Node Type	Master
Security ID	********************
Channel	1
Subchannel	1
MAC Configuration	Default

2 Configure the parameters for the radio. For help, see the next table.

3 (Station only) List the master radios with which this station radio can communicate. For help, see “Configuring the Master List” in the next section.

4 (Master only) Configure inbound filters. For help, see “Configuring OpenAir Radio Inbound Filters” later in this section.

5 (MAC Configuration–Manual only) Configure the manual MAC parameters for the radio. For help, see “Setting Manual MAC Parameters” later in this section.

6 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

OpenAir Radio Parameter Descriptions

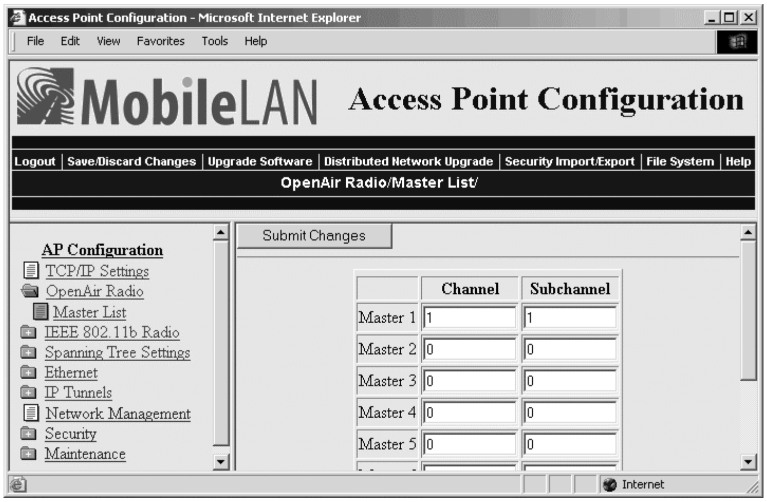
Parameter	Explanation
Node Type	Configure the OpenAir radio as a master or station. You can also disable the radio.
Security ID	Sets a security identification value. All access points and end devices with OpenAir radios must have the same security ID to communicate with each other. Intermec recommends that you set this parameter as it helps prevent unauthorized radios from communicating with the access point. Security ID values can be from 0 to 20 characters. If you have RT1100, RT1700, or RT5900 devices that have OpenAir radios that are communicating with this access point, you must limit the security ID to a maximum of 16 characters.
Channel (Master radio only)	Sets the hopping sequence for the radio. If you have more than one access point in the same coverage area, configure each access point with a unique channel. The Channel value can be any number from 1 to 15.
Subchannel (Master radio only)	Set this parameter if you have more than 16 access points. The subchannel allows access points to share the same channel. If access points have the same channel and different subchannels, they share the same hopping sequence, but behave as if they were on different channels.
MAC Configuration	Adjusting this parameter may enhance the performance of your radio. It changes the settings for the radio protocol in different environments. Intermec recommends that you do not change this parameter from Default unless you are told to do so by Intermec Technical Support. The Interference value may enhance performance in environments with high interference or multipath. The Throughput value may enhance performance of file transfer operations in open or uncongested environments, such as office areas. Manual lets you adjust the MAC parameters individually using the Manual MAC Parms command. To adjust these parameters, see “Setting Manual MAC Parameters” later in this section.

Configuring the Master List

The master list contains the channels and subchannels of all the master radios with which this station radio can communicate.

To configure the master list

1. From the main menu, click OpenAir radio. The OpenAir radio menu appears.
2. Click Master List. The Master List screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
OpenAir Radio/Master List/
AP Configuration
TCP/IP Settings
OpenAir Radio
Master List
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

	Channel	Subchannel
Master 1	1	1
Master 2	0	0
Master 3	0	0
Master 4	0	0
Master 5	0	0

3 For each master radio, enter the channel and subchannel.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Configuring OpenAir Radio Inbound Filters

When configuring a master radio, you can filter different types of wireless traffic that it may receive. You may want to use this feature by itself or with an access control list (ACL) to help secure your network. If you clear all the check boxes, the radio cannot communicate with any other radios. You check the Allow IAPP check box so the access point can communicate with other access points and participate in the spanning tree.

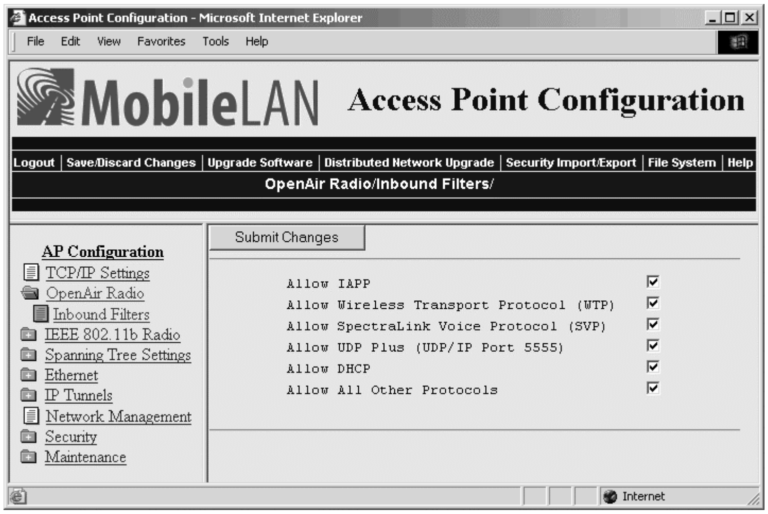
You can use this feature to form a secure wireless hop. Clear all check boxes, except for the Allow IAPP check box. Or, you may want to use this feature in a terminal emulation environment when you know the end devices are sending only UDP Plus or Wireless Transport Protocol (WTP) frames. Check the Allow UDP Plus check box or the Allow Wireless Transport Protocol check box and clear all other check boxes (except the Allow IAPP check box). The access point master radio will only accept the UDP Plus or WTP frames and discard all other frames, which can make a more secure network.

Note: If any of the devices are also DHCP clients, you need to check the Allow DHCP check box.

To configure OpenAir radio inbound filters

1 From the main menu, click OpenAir Radio. The OpenAir Radio screen appears.

2 Click Inbound Filters. The Inbound Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
OpenAir Radio/Inbound Filters/
AP Configuration
TCP/IP Settings
OpenAir Radio
Inbound Filters
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

```
Allow IAPP                                     ☑
Allow Wireless Transport Protocol (WTP)        ☑
Allow SpectraLink Voice Protocol (SVP)         ☑
Allow UDP Plus (UDP/IP Port 5555)              ☑
Allow DHCP                                     ☑
Allow All Other Protocols                      ☑
```

3 For each frame type, check or clear each check box. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

OpenAir Radio Inbound Filter Descriptions

Parameter	Description
Allow IAPP	Determines if this radio accepts IAPP frames from other access point station radios. The IAPP frames must match Ethernet protocol 875c.
Allow Wireless Transport Protocol (WTP)	Determines if this radio accepts WTP frames from end devices. The WTP frames must match Ethernet protocol 875b.
Allow SpectraLink Voice Protocol (SVP)	Determines if this radio accepts SVP frames from MobileLAN voice wireless telephones. The SVP frames must match IP 119.
Allow UDP Plus (UDP/IP Port 5555)	Determines if this radio accepts UDP Plus frames from end devices. The UDP Plus frames must match the UDP network port 5555 on the DCS 30X or ARP.
Allow DHCP	Determines if this radio accepts DHCP frames. The DHCP frames must match UDP destination port 67 and ARP. Check this check box if the end devices are DHCP clients.
Allow All Other Protocols	Determines if this radio accepts all other protocols that are not filtered by one of the filters in this screen.

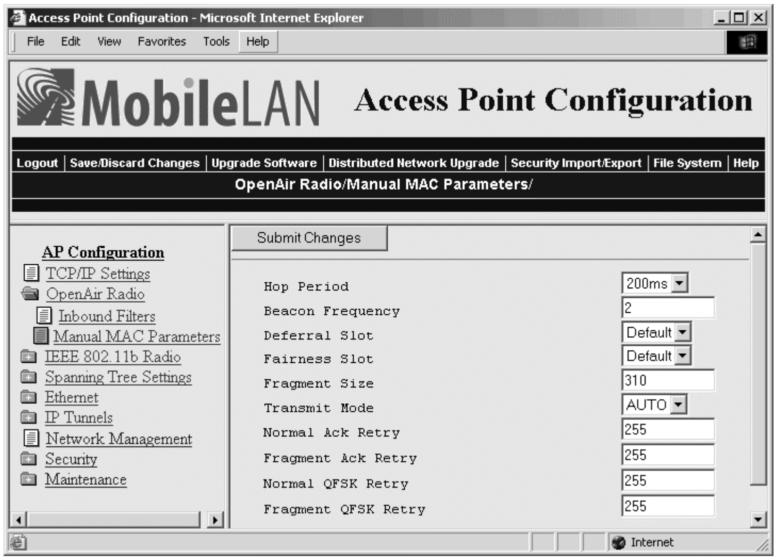
Setting Manual MAC Parameters

Intermec recommends that you do not change the MAC Configuration parameter from Default. Occasionally, you may need to fine-tune your OpenAir radio MAC parameters.

Note: An inefficient MAC Configuration parameter can adversely affect the performance of your wireless network.

To set manual MAC parameters

1 From the main menu, click OpenAir Radio, and then click Manual MAC Parameters. The Manual MAC Parameters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
OpenAir Radio/Manual MAC Parameters/
AP Configuration
TCP/IP Settings
OpenAir Radio
Inbound Filters
Manual MAC Parameters
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

```
Hop Period            200ms
Beacon Frequency      2
Deferral Slot         Default
Fairness Slot         Default
Fragment Size         310
Transmit Mode         AUTO
Normal Ack Retry      255
Fragment Ack Retry    255
Normal QFSK Retry     255
Fragment QFSK Retry   255
```

2 Configure the manual MAC parameters. For help, see the next table.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Manual MAC Parameter Descriptions

Parameter	Explanation
Hop Period (Master radio only)	Specifies how long the master radio stays on a frequency in the hopping sequence before stepping to the next frequency. Longer time periods result in better throughput while shorter time periods result in faster roaming response and immunity from interference. This parameter can be set to 100, 200, or 400 ms.
Beacon Frequency (Master radio only)	Specifies the number of hops between beacons (the access point periodically transmits a beacon to allow end devices to quickly scan each frequency to find a master access point). You can set this parameter to a value from 1 to 7.
Deferral Slot (Master radio only)	Works with the Fairness Slot parameter to determine the average back-off time when the channel is busy. 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. You can set this parameter to 1, 3, 7, or default.
Fairness Slot (Master radio only)	Works with the Deferral Slot parameter to determine the average back-off time when the channel is busy. 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. You can set this parameter to 1, 3, 7, or default.
Fragment Size	Specifies 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 this parameter to a value from 1 to 1540.
Transmit Mode	Modulates the transmit signal and sets the bits per second. AUTO automatically adapts the bit rate to the error conditions. The transmit mode is automatically selected for the best range and throughput. 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.
Normal 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.

Manual MAC Parameter Descriptions (continued)

Parameter	Explanation
Fragment Ack Retry	Controls the number of times a fragmented 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 Fragment Ack Retry count includes the Fragment QFSK Retry count; therefore, Fragment Ack Retry should be greater than Fragment QFSK Retry.
Normal QFSK Retry	When Transmit Mode is set to AUTO, this parameter controls the number of times that an unfragmented QFSK frame is resent unsuccessfully before switching to BFSK. You can set this parameter to a value from 1 to 255.
Fragment QFSK Retry	When Transmit Mode is set to AUTO, this parameter 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.

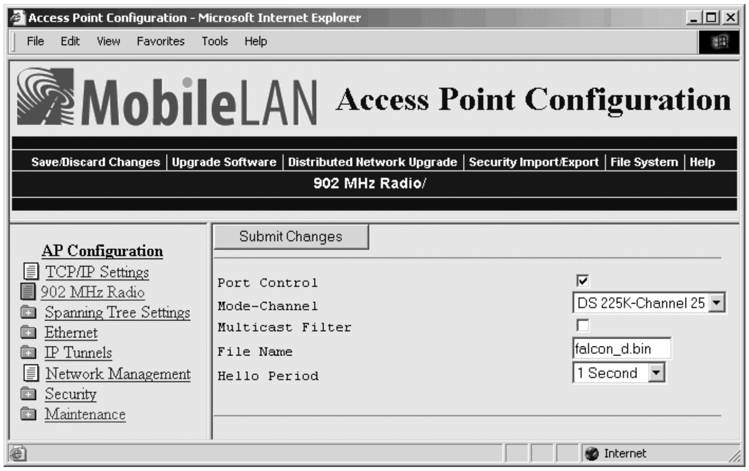
Configuring the 902 MHz Radio (2100 Only)

The 902 MHz radio will communicate with other 902 MHz radios that have the same

- LAN ID. For help, see “Configuring the Spanning Tree Parameters” in Chapter 5.
- Mode-Channel.

To configure the 902 MHz radio

1 From the main menu, click 902 MHz Radio. The 902 MHz Radio screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
902 MHz Radio/
AP Configuration
TCP/IP Settings
902 MHz Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

Port Control ☑
Mode-Channel DS 225K-Channel 25
Multicast Filter □
File Name falcon_d.bin
Hello Period 1 Second

2 Configure the parameters for the radio. For help, see the next table.

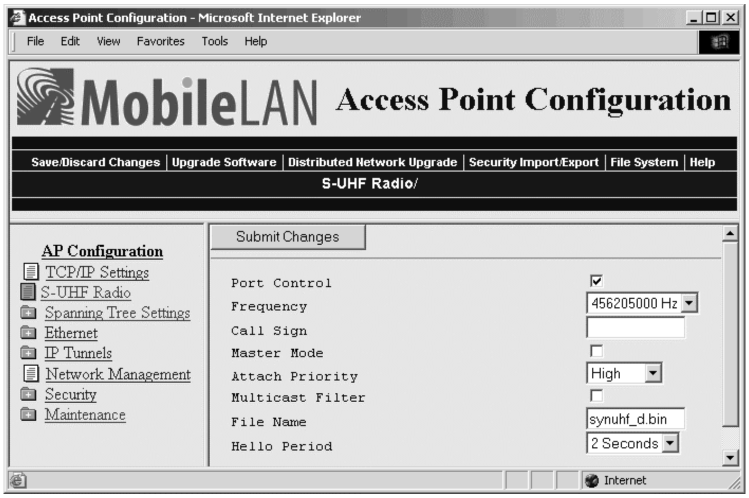
3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

902 MHz Radio Parameter Descriptions

Parameter	Explanation
Port Control	Enable or disable the 902 MHz port.
Mode-Channel	Sets the bit rate option. Generally, the higher the bit rate, the lower the range of the access point. 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 the access point. Mode-Channel options are country-dependent. These combinations are valid in the United States: 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-Channels 10 through 40 use 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.
Multicast Filter	Determines if this radio can receive and send multicast frames.
File Name	Specifies the name of the radio’s driver software. Intermec recommends that you change this name only when directed to do so by Intermec Technical Support.
Hello Period	Controls how frequently the access point broadcasts hello messages on this radio port. Hello messages help maintain the spanning tree and serve as beacon messages to synchronize communications with end devices.

Configuring the S-UHF Radio (2100 Only)

1 From the main menu, click S-UHF radio. The S-UHF Radio screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
S-UHF Radio/
AP Configuration
TCP/IP Settings
S-UHF Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

Port Control ☑
Frequency 456205000 Hz
Call Sign
Master Mode □
Attach Priority High
Multicast Filter □
File Name synuhf_d.bin
Hello Period 2 Seconds

2 Configure the S-UHF radio. For help, see the next table.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

S-UHF Radio Parameter Descriptions

Parameter	Explanation
Port Control	Enable or disable the S-UHF port.
Frequency	Displays the frequencies available on your access point. Some radios have multiple frequencies.
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 access point periodically transmit a call sign. Failure to transmit the call sign is a violation of United States law. The call sign is granted as part of the FCC license process. Insert the call sign from the FCC license certificate in this parameter. The call sign can be from 0 to 12 characters long. Do not set this parameter if you are outside the United States.

S-UHF Radio Parameter Descriptions (continued)

Parameter	Explanation
Master Mode	Determines how channel access is controlled. Check this check box to set the access point 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 access point radio coverage area does not overlap other access points operating in the same area. Clear this check box to cause all radios in the network to cooperate as peers, and access point 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	If Master Mode is disabled, you can set this parameter to determine the likelihood that this access point will obtain media access. Set this parameter when you need a redundant network with some access points serving as standby units. You can set these values: 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. If a higher priority access point fails, end devices fall back to a lower priority access point in the same coverage area.
Multicast Filter	Determines if this radio can receive and send multicast frames. Check this check box if you do not want the radio to receive and send multicast frames.
File Name	Specifies the name of the radio's driver software. Change this name only when directed to do so by Intermec Technical Support.
Hello Period	Controls how frequently the access point broadcasts hello messages on the radio port. Hello messages help maintain the spanning tree and serve as beacon messages to synchronize communications with end devices.

5 Configuring the Spanning Tree

This chapter explains how to configure the MobileLAN access products so that they create a spanning tree topology. This chapter covers these topics:

- About the access point spanning tree
- Configure the spanning tree parameters
- About IP tunnels
- Configuring IP tunnels
- Configuring global parameters

About the Access Point Spanning Tree

MobileLAN access products with the same LAN ID arrange themselves into a self-organized network using a spanning tree topology. The spanning tree provides efficient, loop-free forwarding of frames through the network and allows efficient roaming of wireless end devices. It contains at least a primary LAN and a root access point, but it may also contain secondary LANs, designated bridges, and other access points.

Within the spanning tree, access points use Intermec's IAPP (Inter Access Point Protocol) or secure IAPP to communicate with each other across the Ethernet network, over wireless secondary LANs, and through IP tunnels to remote IP subnets. IAPP also enables fast roaming in an 802.11b or 802.11a network using 802.1x security. Secure IAPP prevents unauthorized MobileLAN access products from joining the spanning tree.

For example, when an end device roams to a new access point, the new access point informs the old access points via the root access point that any traffic for the end device needs to be routed to the new access point. As end devices are added to or removed from the network, access points are automatically updated so they can maintain reliable operation and communication.

About the Primary LAN and the Root Access Point

The primary LAN (also called the root IP subnet) contains the root access point, which initiates the spanning tree. When choosing the primary LAN, ideally you should choose the IP subnet that contains gateways or servers for the wireless end devices. However, these gateways and servers may be on another subnet.

The root coordinates the network and distributes common system parameters to other access points and end devices. The root is elected from a group of access points that are designated as root candidates (access points that are powered on, active, and do not have a root priority of 0). The root should not be an access point that handles a large volume of wireless traffic. The access point with the highest root priority is the root.

The election process also occurs in the event of a root access point failure. Besides the root, you should have two or three access points with a non-zero root priority. If two access points have the same root priority, the access point with the highest Ethernet address becomes the root. You should configure your network with overlapping coverage so that the network can automatically recover from any single point of failure.

After the root access point is elected, it transmits hello messages on all enabled ports. The spanning tree forms as other access points receive hello messages and attach to the network on the optimal path to the root. A non-root access point also transmits hello messages after it is attached to the network. Each hello message contains the LAN ID of the access point that originated the message. IAPP does not allow wireless links to exist between access points that do not have matching LAN IDs.

To configure a root access point

1. On an access point that is installed on the primary LAN, from the main menu click Spanning Tree Settings. The Spanning Tree Settings screen appears.
2. Configure the LAN ID. All access points that want to participate in the spanning tree must have the same LAN ID.
3. Set the Root Priority parameter to be the highest number of all access points on the primary LAN. Verify that the Ethernet Bridging Enabled check box is checked.
4. Verify that the Secondary LAN Bridge Priority is zero and the Secondary LAN Flooding parameter is Disabled.
5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

About Secondary LANs and Designated Bridges

There are two types of secondary LANs: a wireless secondary LAN is connected to the primary LAN wirelessly via a WAP, and a remote IP subnet is connected via an IP tunnel.

Comparison of Wireless Secondary LANS and Remote IP Subnets

Wireless Secondary LANs (WAPs)	Remote IP Subnets (IP tunnels)
Any access point can provide a wireless link to another access point.	Only the root access point can originate an IP tunnel to another access point.
A wireless link provides a transparent bridge for both wired and wireless devices.	An IP tunnel provides a transparent bridge for wireless end devices on a remote IP subnet.

The access point that is responsible for bridging data between a secondary LAN and the primary LAN is called the designated bridge. The designated bridge must be an access point

- on the secondary LAN.
- with the Secondary LAN Bridge Priority value set to a non-zero number.
- with at least one radio set to Station mode or that is the endpoint of an IP tunnel. For more information, see “About IP Tunnels” later in this chapter.

If more than one access point meets these requirements, the access point with the highest secondary LAN bridge priority is the designated bridge. If two access points have the same secondary LAN bridge priority, the access point with the highest Ethernet address becomes the designated bridge. If the designated bridge goes offline, the remaining access points negotiate to determine which access point becomes the new designated bridge.

To configure a designated bridge

1. On an access point that is installed on the secondary LAN and within radio coverage of an access point on the primary LAN, from the main menu click Spanning Tree Settings. The Spanning Tree Settings screen appears.
2. Configure the LAN ID. All access points that want to participate in the spanning tree must have the same LAN ID.
3. Set the Root Priority parameter to zero. All access points on the secondary LAN should have a root priority of zero.
4. Verify that the Ethernet Bridging Enabled check box is checked.
5. Set the Secondary LAN Bridge Priority to be the highest number of all access points on the secondary LAN.
6. Set the Secondary LAN Outbound Flooding parameter to Enabled.
7. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

About Data Link Tunneling

Data link tunneling passes data from wireless end devices communicating with access points on the same subnet to the root access point or designated bridge. Use data link tunneling if you have Ethernet switches that do not support the IEEE 802.1d requirements for backward learning. Some proprietary VLAN switches and ATM LANE bridges do not support this standard.

If the access points are connected to different ports on an Ethernet switch, each time an end device roams to a new access point, it appears on a different port. Thus, frames sent to the end device from the host will be sent to the wrong port. If the switch does not support 802.1d, it may become confused and communications with the end device is disrupted. Data link tunneling makes end device roaming transparent to the switch. All the information appears to originate from only one port on the switch–the port that is connected to the root access point or designated bridge.

You should also use data link tunneling when you are using IP tunnels to provide mobility of other routable protocols, such as IPX. 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.

To enable data link tunneling, disable Ethernet bridging. When an access point receives data from an end device, it encapsulates the data into an OWL data frame. This frame is then forwarded via the Ethernet port to the next access point on the path and so on until the frame reaches the root access point or designated bridge. The root access point or designated bridge unencapsulates the frame and forwards it to the host. When the root access point or designated bridge receives data on the Ethernet network for an end device, it reverses this process.

Unless you need to use data link tunneling, Intermec recommends that you enable Ethernet bridging on all access points. Data link tunneling increases network traffic.

To enable data link tunneling on the primary LAN

1. Make sure that all access points have the same LAN ID.
2. On the root access point, on the Spanning Tree Settings screen verify that the Ethernet Bridging Enabled check box. is checked.
3. On all other access points on the primary LAN, clear the Ethernet Bridging Enabled check box.
4. Make sure that the Root Priority parameter. for all other access points is less than the root access point.

To enable data link tunneling on the secondary LAN

1. Make sure that all access points have the same LAN ID. as the ones on the primary LAN.
2. On the designated bridge, on the Spanning Tree Settings screen verify that the Ethernet Bridging Enabled check box is checked.
3. On all other access points on the secondary LAN, clear the Ethernet Bridging Enabled check box.
4. Make sure that the Secondary LAN Bridge Priority parameter. for all other access points is less than the designated bridge.

If you use data link tunneling on the secondary LAN and end devices have IP addresses on the secondary LAN, network monitoring tools and other network components cannot detect their MAC/IP addresses. For more information, see "About IP Tunnels" later in this chapter.

About Routable and Non-Routable Network Protocols

Hosts that use a routable network protocol such as IP or IPX may be located on any IP subnet; however, triangular routing can be minimized if servers are located on the root IP subnet. (Note that this is also true for standard mobile IP.) You should be able to use default flooding and spanning tree settings if you are using routable protocols, even if hosts are located on remote IP subnets.

Some Intermec wireless end devices use the Intermec NNL protocol, which is a simple Non-routable Network Layer protocol. This NNL protocol 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 hosts. If NNL gateways are located on the root IP subnet, you can use the default flooding and spanning tree settings, and minimize triangular routing. If NNL gateways are located on remote IP subnets, you must enable outbound multicast flooding and secondary bridging.

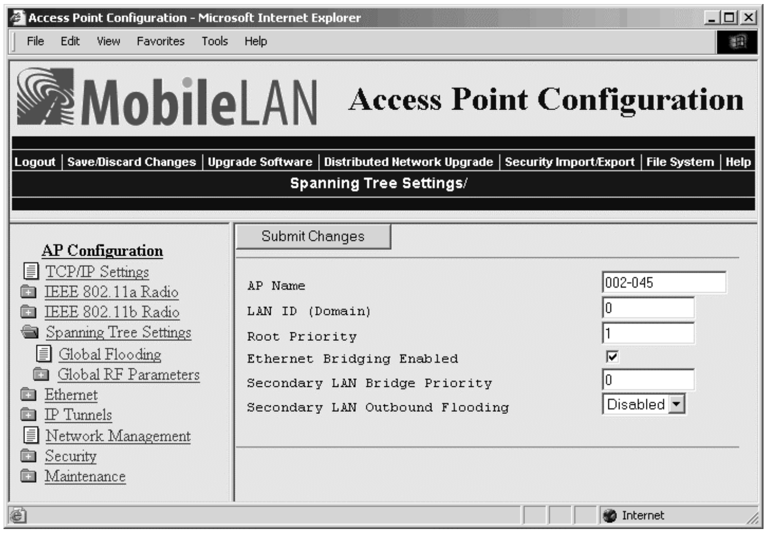
Configuring the Spanning Tree Parameters

When you configure the spanning tree parameters, you identify the access point as part of the spanning tree. That is, you specify if this access point is a root or a backup root or a designated bridge or a backup designated bridge, uses data link tunneling to encapsulate wireless traffic or if wireless traffic gets dumped raw on the Ethernet network.

On the designated bridge, if you enable Ethernet bridging, wireless traffic gets dumped raw on the secondary LAN. If you disable Ethernet bridging or if you set the secondary LAN bridge priority to 0, wireless traffic is encapsulated on the secondary LAN, which eliminates communication from wired devices on the secondary LAN.

To configure the spanning tree parameters

1 From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Spanning Tree Settings/
Submit Changes
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Global Flooding
Global RF Parameters
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Internet

AP Name 002-045

LAN ID (Domain) 0

Root Priority 1

Ethernet Bridging Enabled ☑

Secondary LAN Bridge Priority 0

Secondary LAN Outbound Flooding Disabled

2 Configure the spanning tree parameters. For help, see the next table.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Spanning Tree Parameter Descriptions

Parameter	Explanation
AP Name	Enter a unique name for this access point. The name can be from 1 to 16 characters. The default is the access point serial number. If this access point has an OpenAir master radio, only the first 11 characters are used.
LAN ID (Domain)	Enter the LAN ID. All access points must have the same LAN ID to participate in the same spanning tree. The LAN ID is a number from 0 to 254. If you are using OpenAir radios, all OpenAir devices in a network must have the same LAN ID to be able to communicate. Also, if you assign a LAN ID greater than 15, the access point uses a LAN ID that is the remainder after dividing the LAN ID by 16. For example, if you set the LAN ID to 21 or 37, the access point uses 5.

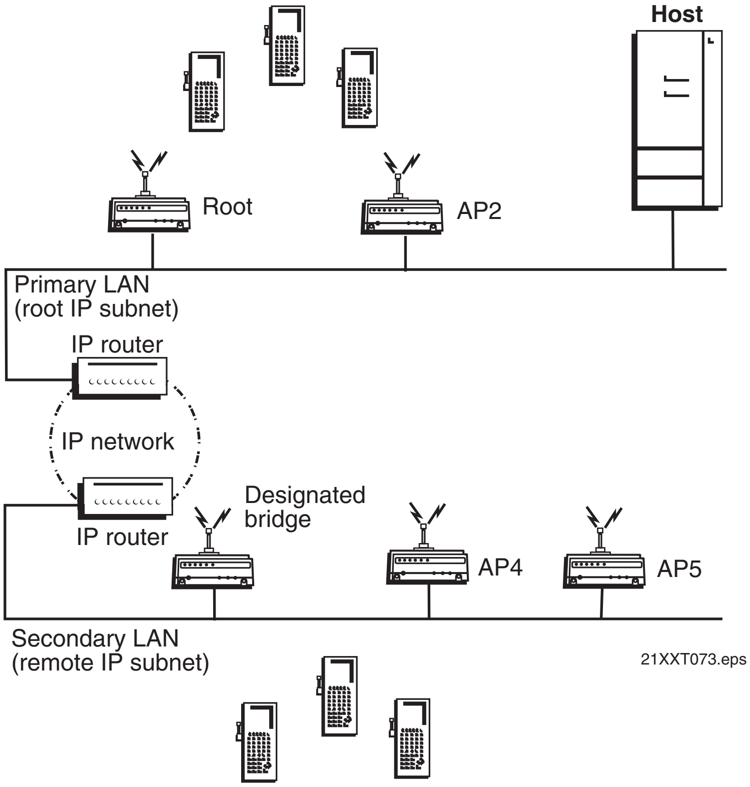
Spanning Tree Parameter Descriptions (continued)

Parameter	Explanation
Root Priority	Determines if this access point is a candidate to become the root of the spanning tree. The access point with the highest root priority becomes the root whenever it is powered on and active. The root priority can be a value from 0 to 7. If you set the root priority to 0, the access point can never become the root access point. For more information, see "About the Primary LAN and the Root Access Point" earlier in this chapter. **Note:** If your network contains 6710 and MobileLAN access products, configure a MobileLAN access product as the root.
Ethernet Bridging Enabled	Determines how frames from end devices are dumped on the Ethernet network and vice versa. Check this check box if you want frames to be forwarded directly to the Ethernet network. Intermec recommends that you enable this parameter on all access points. Enabling this parameter on the root or designated bridge and disabling it on all other access points on the same IP subnet will enable data link tunneling on the IP subnet. For help, see "About Data Link Tunneling" earlier in this chapter.
Secondary LAN Bridge Priority	Determines when this access point can become the designated bridge in a secondary LAN. The access point that meets all the other requirements and has the highest secondary LAN bridge priority becomes the designated bridge. The secondary LAN bridge priority can be a value from 0 to 7. If you set this value to 0, the access point can never become the designated bridge. For more information, see "About Secondary LANs and Designated Bridges" earlier in this section.
Secondary LAN Outbound Flooding (Designated bridge only)	Specifies the types of frames it forwards from the primary LAN to the secondary LAN. Choose Disabled if no flooding occurs unless the root access point (in the Global Flooding screen) enables the Multicast or Unicast Outbound to Secondary LANs parameter. Choose Enabled if multicast and unicast flooding occurs unless the root access point (in the Global Flooding screen) disables multicast or unicast flooding. Choose Multicast if multicast flooding occurs unless the root access point (in the Global Flooding screen) disables multicast flooding. Choose Unicast if unicast flooding occurs unless the root access point (in the Global Flooding screen) disables unicast flooding.

About IP Tunnels

The physical boundary of a network is usually defined by the existence of an IP router. Before IP tunnels technology was developed, wireless end devices could only operate within the limited coverage area of their own network and could not roam across IP subnet boundaries. Using IP tunnel technology, end devices can roam across IP subnet boundaries. IP tunnel technology safely and transparently coexists with routed IP installations while supporting mobility for end devices. IP tunnels do the following:

- Enable access points on different remote IP subnets to belong to the same wireless network.
- Support fast roaming of end devices between access points that are on different IP subnets without losing network connections.
- Support end devices using both IP and other routable or nonroutable protocols.



Only one IP tunnel can exist between the root access point and an access point (usually the designated bridge) on a remote IP subnet. The root access point has a one-to-one relationship with each wireless network. All roaming end devices must have an IP address from the root IP subnet.

IP tunnels use encapsulation to establish a virtual LAN segment through IP routers. The virtual LAN segment includes the root IP subnet and logically extends to include end devices attached to access points on remote IP subnets. IP tunnels are branches in the spanning tree topology.

Any access point on a secondary LAN that can receive IP hello messages can be the endpoint of an IP tunnel. Usually, the access point that is the endpoint of an IP tunnel is also the designated bridge. After an IP tunnel is formed between the root access point and an access point on a remote IP subnet, end devices can roam to the remote IP subnet. End devices must have an IP address from the root IP subnet. However, there are no address restrictions for non-IP end devices. When end devices roam to the remote IP subnet, their data is IP tunneled back to the root IP subnet (where it belongs) and everything works properly.

If you have a DHCP server in your network, it must be on the root IP subnet. All access points on secondary LANs must have permanent IP addresses. On the root access point, you must allow IP multicast frames to pass.

When an access point at the endpoint of the IP tunnel receives data from an end device, it uses a standard IP protocol called Generic Router Encapsulation (GRE) to encapsulate the data into a frame. These encapsulated IP/GRE frames use normal IP routing to pass through IP routers to the root access point. The root access point unencapsulates the frame and forwards it to the host. When the root access point receives data on the Ethernet network for an end device that is communicating on a remote IP subnet, it reverses this process.

IP tunneling also allows non-routable traffic, such as WTP and NNL, to roam across routers. The end devices using these protocols are not IP based, but they work in the same way. Data traffic that is not passed by routers (since they are not IP) will be tunneled from the remote IP subnet to the root subnet. It will be dumped on the Ethernet on the root subnet (where it belongs) and everything works properly.

Creating IP Tunnels

An IP tunnel is established when an access point on a remote IP subnet attaches to the root access point through its IP tunnel port. The number of IP tunnels the root access point can originate is practically unlimited. However, currently the IP address list can only contain eight entries, which effectively limits the number of tunnels that can be created if you want to use unicast and directed broadcast IP addresses.

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.
- One 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.)
- One IP multicast address can be used to create a practically unlimited number of tunnels to remote IP subnets. For help, see “Using One IP Multicast Address for Multiple IP Tunnels” in the next section.

Once you have configured the IP tunnels, the root access point sends IP hello messages to each IP address in its IP address list. An IP tunnel is automatically established when an access point on a remote IP subnet receives this hello message. This access point then transmits IP hello messages on its subnet so that other access points on the same subnet that do not receive hello messages can also attach to the spanning tree.

To create a unicast IP tunnel

1. Make sure that end devices that will roam between the root IP subnet and the remote IP subnet have IP addresses from the root IP subnet and have their default router set the same as the root access point. There are no address restrictions for non-IP end devices.
2. Make sure that the root access point and the access point at the endpoint of the IP tunnel have the same LAN ID.
3. On the root access point, set the Mode parameter to Originate if Root. For help configuring a root access point, see “About the Primary LAN and the Root Access Point” earlier in this chapter.
4. On the access point at the endpoint of the IP tunnel, set the Mode parameter to Listen.
5. On the root access point, click IP Tunnels, and then click IP Addresses. Enter the IP address of the access point at the endpoint of the IP tunnel.
6. On the root access point and the access point at the endpoint of the IP tunnel, click Tunnel Filters, and then click Frame Type Filters. If you have end devices communicating using IP, set these DIX filters to Pass.
    - DIX-IP-TCP Ports
    - DIX-IP-UDP Ports
    - DIX-IP-Other Protocols
    - DIX-IPX Sockets
    - DIX-Other EtherTypes

7 On the root access point and the access point at the endpoint of the IP tunnel, click Tunnel Filters, and then click Predefined Subtype Filters. If you have end devices communicating using IP, set these filters to Pass.

- DIX ARP
- ICMP

8 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" in Chapter 1.

Using One IP Multicast Address for Multiple IP Tunnels

IP tunneling supports IP multicast and Internet Group Management Protocol (IGMP). IP multicast provides an ideal way to distribute IP hello messages. These hello messages are only forwarded to those IP subnets and IP hosts (such as access points) that participate in the multicast group. IP multicast has these advantages:

- You do not have to know the unicast or directed broadcast IP addresses in advance.
- IP multicast provides better built-in redundancy than IP unicast, because any access point can establish an IP tunnel.

IGMP is a standard protocol that lets you originate multiple IP tunnels using one IP multicast address. It allows IP multicast frames to be routed to remote IP subnets that have hosts participating in the multicast group. Note that IGMP is independent of IP; it can be used to facilitate multicast for IP or any other application. IGMP has these advantages:

- Causes IP hello messages to be forwarded only to those subnets that participate in the IP multicast group
- Increases redundancy because multiple access points on a remote subnet can receive IP hello messages

IP routers only forward multicast frames to those subnets that have IP hosts that participate in the respective IP multicast group. An IP host uses IGMP to notify IP routers that it wants to participate in an IP multicast group.

Access points can act as IP hosts and participate in an IP multicast group by enabling IGMP. The Internet Assigned Numbers Authority has allocated 224.0.1.65 for Intermec's Inter Access Point protocol (IAPP). You must enter this address in the IP address list in the root access point. (Note that the address list may contain other IP addresses.) and in the Multicast Address field in the other access points.

If you enable IGMP on the root access point, the root access point uses a Class D IP multicast address to send IP hello messages through IP routers to access points on other subnets. If you enable IGMP on remote IP subnets, intermediate IP routers will forward the IP hello messages to those subnets. Normally, you should enable IGMP and configure the IP multicast address in at least one access point on each remote IP subnet. (Some routers can provide proxy IGMP services for IP hosts.)

To create a multicast IP tunnel

1 Make sure that end devices that will roam between the root IP subnet and the remote IP subnet have IP addresses from the root IP subnet and their default router is set the same as the root access point. There are no address restrictions for non-IP end devices.

2 Make sure that your routers are configured to pass multicast frames.

3 Make sure that the root access point and the access point at the endpoint of the IP tunnel have the same LAN ID.

4 On the root access point, set the Mode parameter to Originate if Root. For help configuring a root access point, see “About the Primary LAN and the Root Access Point” earlier in this chapter.

5 On the access point at the endpoint of the IP tunnel, set the Mode parameter to Listen.

6 On the root access point, click IP Tunnels, and then click IP Addresses. Enter the Intermec multicast address 224.0.1.65.

7 On the access point at the end of the IP tunnel, check the Enable IGMP check box.

8 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

How Frames Are Forwarded Through IP Tunnels

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

Any frame that is sent through an IP tunnel is addressed to the unicast IP address of the access point at the other end of the tunnel. An access point at the remote end of the tunnel learns the unicast IP address of the root access point by listening to IP hello messages. The root access point learns the unicast IP address of a remote access point when the access point attaches to the network.

Outbound Frames

Frames are forwarded outbound (to a secondary LAN) through an IP tunnel if

- an end device is known to be attached to an access point on a remote IP subnet.
- the frame type is configured to pass in the Tunnel Filters screen.

IP and ARP frames are never forwarded outbound through an IP tunnel unless the destination IP address belongs to the root IP subnet. Usually, these frames are destined for wireless end devices that have roamed away from their root IP subnet.

Unicast frames are not flooded. Unicast frames are only forwarded outbound through an IP tunnel if the destination address identifies an end device that has roamed to a remote IP subnet. End devices attach to the root access point, 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 root IP subnet. Usually, ARP requests (which are multicast frames) that originate on the root IP subnet are forwarded outbound to all devices on the network, including through IP tunnels to remote IP subnets. However, if you enable ARP flooding, ARP frames are only sent through the IP tunnel to the destination end device.

MAC frames that are forwarded outbound are encapsulated in the root access point, forwarded through the network, unencapsulated by the access point at the remote end of the IP tunnel, and forwarded to the appropriate access point (if necessary) for delivery to the destination end device.

Inbound Frames

Frames are forwarded inbound (to the primary LAN) through an IP tunnel if

- an end device is known to be attached to an access point on a remote IP subnet.
- the frame type is configured to pass in the Tunnel Filters screen.

IP and ARP frames are only forwarded inbound through the IP tunnel if the source IP address belongs to the root IP subnet. Usually, these frames originate from wireless end devices that have roamed away from their root IP subnet. Frames transmitted by servers or wired devices that are connected to a remote IP subnet are not forwarded inbound through IP tunnels if the IP address does not belong to the root IP subnet.

MAC frames that are forwarded inbound are encapsulated by the access point at the remote end of the IP tunnel, forwarded through the IP tunnel to the root access point, unencapsulated, and placed on the network.

Frame Types That Are Never Forwarded

Certain frame types are never forwarded through IP tunnels. Frame types that are never forwarded include IP frames used for coordinating routers and MAC frames used for coordinating bridges. Other frame types that are never forwarded include:

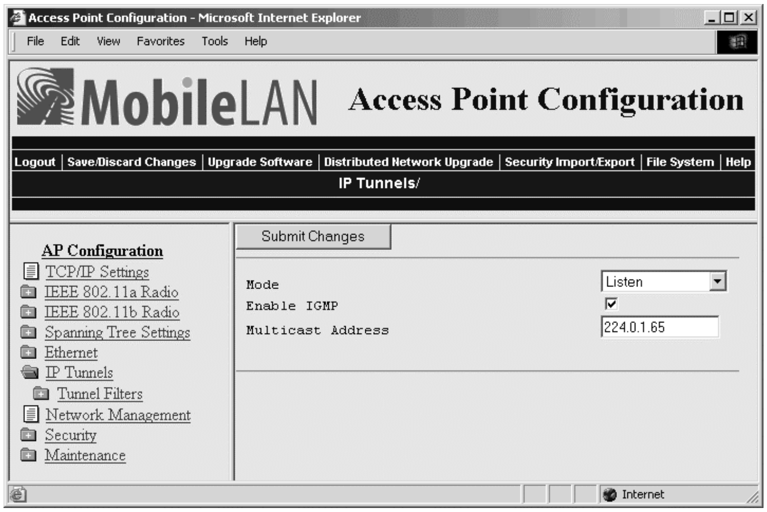
- 802.1d bridge frames
- Proprietary VLAN switch frames
- IP frames with a broadcast or multicast Ethernet address
- IP frames with the following router protocol types and decimal values:
  - DGP (86) (Dissimilar Gateway Protocol)
  - EGP (8) (Exterior Gateway Protocol)
  - IDPR (35) (Inter-Domain Policy 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)

Configuring IP Tunnels

For guidelines, see “About IP Tunnels” earlier in this chapter.

To configure the IP Tunnels screen

1 From the main menu, click IP Tunnels. The IP Tunnels screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IP Tunnels/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Tunnel Filters
Network Management
Security
Maintenance
Submit Changes
Internet

Mode	Listen
Enable IGMP	☑
Multicast Address	224.0.1.65

2 Configure the IP Tunnels parameters. For help, see the next table.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

IP Tunnel Parameter Descriptions

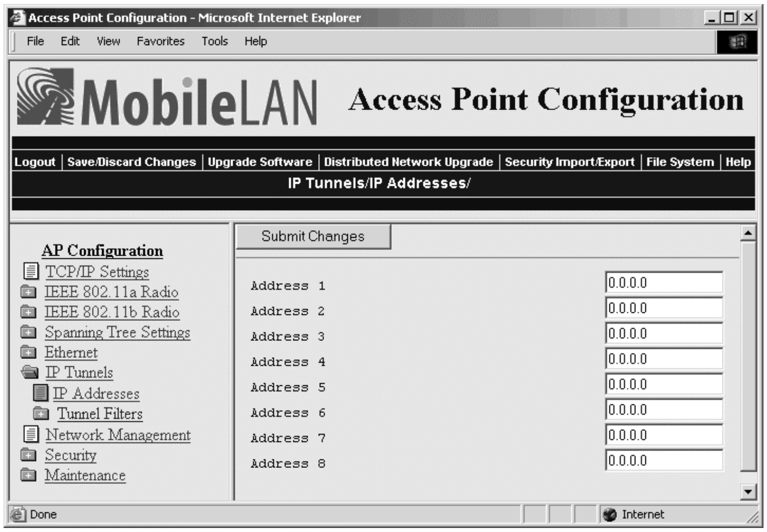
Parameter	Explanation
Mode	Choose Originate if Root to let the root access point and root candidates originate the IP tunnel if they are functioning as the root access point for the network. Choose Listen to configure access points that are designated bridges or designated bridge candidates for their remote IP subnets to serve as the endpoint of an IP tunnel. Choose Disabled to disable the IP tunnel port.
Enable IGMP (Listen only)	Determines if IGMP is enabled or disabled.
Multicast Address (Enable IGMP checked only)	Enter the Class D IP multicast address. You also need to enter this IP address in the root access point’s IP address list. The Internet Assigned Numbers Authority has allocated 224.0.1.65 for Intermec’s inter-access-point protocol (IAPP).

Configuring the IP Address List

On the root access point and root candidates, the IP address list contains the IP addresses of all the access points at the endpoint of the IP tunnels.

To configure the IP address list

1 From the main menu, click IP Tunnels, and then click IP Addresses. The IP Addresses screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IP Tunnels/IP Addresses/
Submit Changes
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
IP Addresses
Tunnel Filters
Network Management
Security
Maintenance
Done
Internet

Address 1	0.0.0.0
Address 2	0.0.0.0
Address 3	0.0.0.0
Address 4	0.0.0.0
Address 5	0.0.0.0
Address 6	0.0.0.0
Address 7	0.0.0.0
Address 8	0.0.0.0

2 If you enabled IGMP, enter the Class D IP multicast address. The default is 224.0.1.65.

3 Enter the IP addresses of all the access points that can be the endpoints of IP tunnels.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Configuring IP Tunnel Filters

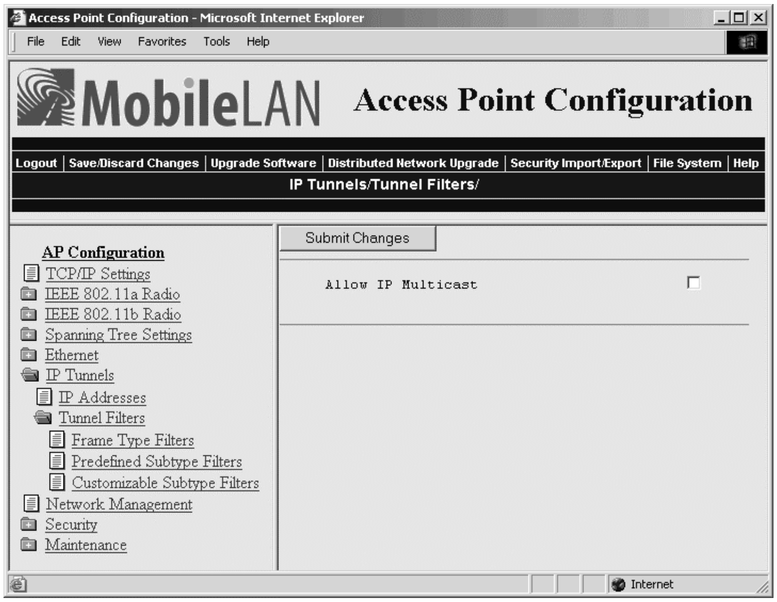
You can set both Ethernet and IP tunnel filters, and you can create protocol filters for predefined protocol types. In addition, you can define arbitrary frame filters based on frame content.

By default, all IP tunnel traffic (except NNL traffic) is dropped. IP tunnel filters are only outbound filters. That is, when you configure IP tunnel filters in the root access point, you are only defining what type of traffic the root will send through the tunnel. The root will receive anything sent to it by the access point at the endpoint of the tunnel. The access point at the endpoint of the tunnel acts the same way. In order for a particular type of traffic to pass, you need to set the same filters to pass in both in the root access point and in the access point at the endpoint of a tunnel.

For help configuring Ethernet filters, see “Configuring Ethernet Filters” in Chapter 3.

To configure IP tunnel filters

1 From the main menu, click IP Tunnels, and then click Tunnel Filters. The Tunnel Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IP Tunnels/Tunnel Filters/
Submit Changes
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
IP Addresses
Tunnel Filters
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Network Management
Security
Maintenance
Internet

Allow IP Multicast □

2 (Originate if Root only) Check or clear the Allow IP Multicast check box. Check this check box if you have a DHCP server issuing TCP/IP information to end devices.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Using IP Tunnel Frame Type Filters

The IP tunnel port automatically provides some filtering for wireless end devices. You can define permanent IP tunnel port filters to prevent unwanted frame forwarding through an IP tunnel. ICMP frames with the following types are always 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

IP and ARP frames are never forwarded inbound through an IP tunnel to the root IP subnet unless the source IP address belongs to the root IP subnet. (Frames are only forwarded inbound if the source IP address in the IP or ARP frame identifies an end device that has roamed away from its root IP subnet.) IP and ARP frames are never forwarded outbound through an IP tunnel by the root access point unless the destination IP address belongs to the root IP subnet. (Frames are only forwarded outbound to end devices that have roamed away from the root IP subnet.) For detailed information about other frame types that are never forwarded, see "Frame Types That Are Never Forwarded" earlier in this chapter.

You can set the default action and scope for general and specific frame types:

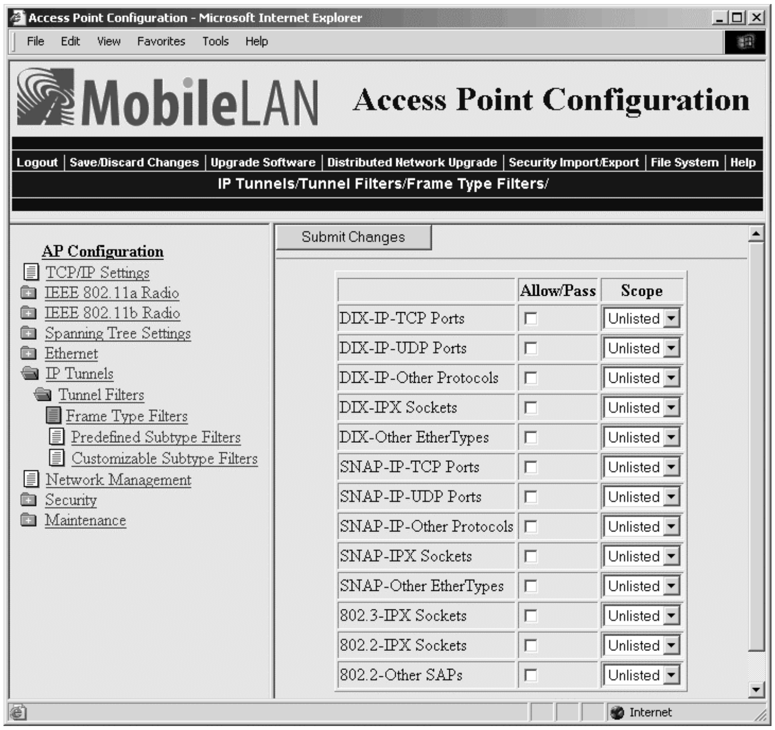
Allow/ Pass Check or clear this check box. Check this check box to pass all frames of the type. Clear this check box to drop all frames of the type.

Scope Set scope to Unlisted or All. If you select All, then all frames of that type are unconditionally passed or dropped, depending on the action you specified. If you select Unlisted, then frames are passed or dropped only if the frame type is not listed in the predefined or customizable tables.

To use IP tunnel frame type filters

1 From the main menu, click IP Tunnels, and then click Tunnel Filters.

2 Click Frame Type Filters. The Frame Type Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IP Tunnels/Tunnel Filters/Frame Type Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Tunnel Filters
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Network Management
Security
Maintenance
Submit Changes
Internet

	Allow/Pass	Scope
DIX-IP-TCP Ports	□	Unlisted
DIX-IP-UDP Ports	□	Unlisted
DIX-IP-Other Protocols	□	Unlisted
DIX-IPX Sockets	□	Unlisted
DIX-Other EtherTypes	□	Unlisted
SNAP-IP-TCP Ports	□	Unlisted
SNAP-IP-UDP Ports	□	Unlisted
SNAP-IP-Other Protocols	□	Unlisted
SNAP-IPX Sockets	□	Unlisted
SNAP-Other EtherTypes	□	Unlisted
802.3-IPX Sockets	□	Unlisted
802.2-IPX Sockets	□	Unlisted
802.2-Other SAPs	□	Unlisted

3 For each frame type field, check or clear the check box to configure if the frame types are passed or are dropped. If you check the check box, the frame type is allowed to pass.

For each frame type field, click the down arrow on the right side of the Scope field and set the scope to Unlisted or All.

For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

5 If you set the Scope field to Unlisted for any of the frame types, you must also configure predefined subtype filters or customizable subtype filters. For help, see “Using Predefined Subtype Filters” or “Customizing Subtype Filters” later in this section.

Frame Type Filter Descriptions

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 should not filter HTTP, Telnet, SNMP, and ICMP frames if you are using IP tunnels, because these filters are used for configuring, troubleshooting, and upgrading access points.

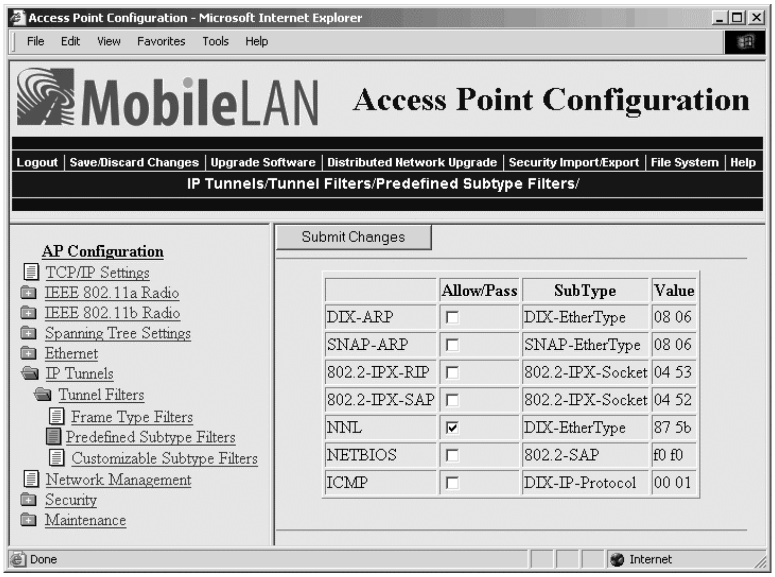
Using Predefined Subtype Filters

You can configure the access point to pass or drop certain predefined frame subtypes.

To configure predefined subtype filters

1 From the main menu, click IP Tunnels, and then click Tunnel Filters.

2 Click Predefined Subtype Filters. The Predefined Subtype Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IP Tunnels/Tunnel Filters/Predefined Subtype Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Tunnel Filters
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Network Management
Security
Maintenance
Submit Changes
Done
Internet

	Allow/Pass	SubType	Value
DIX-ARP	□	DIX-EtherType	08 06
SNAP-ARP	□	SNAP-EtherType	08 06
802.2-IPX-RIP	□	802.2-IPX-Socket	04 53
802.2-IPX-SAP	□	802.2-IPX-Socket	04 52
NNL	☑	DIX-EtherType	87 5b
NETBIOS	□	802.2-SAP	f0 f0
ICMP	□	DIX-IP-Protocol	00 01

3 For each frame subtype field, check or clear the check box to configure if the frame subtypes are passed or are dropped. If you check the check box, the frame subtype is allowed to pass.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Customizing Subtype Filters

You can define output filters that restrict customized frame subtypes 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 port number. By default, the filters drop all protocol types except the NNL DIX Ethernet type (hexadecimal 875B). Filters must be configured in all root candidates and in any access point that can attach to the remote end of an IP tunnel.

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

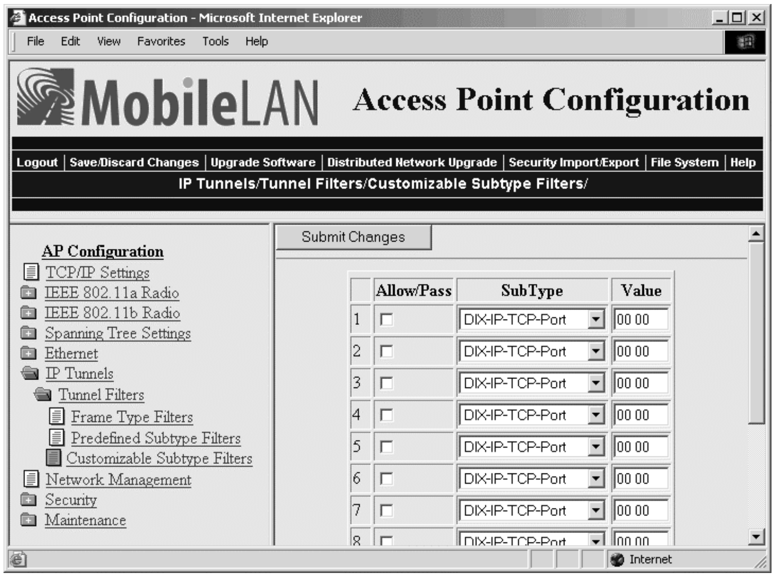
Allow/ Pass Check or clear this check box. Check this check box to pass all frames of the subtype and value. Clear this check box to drop all frames of the subtype and value.

Subtype Selects the frame subtype you wish to configure.

Value The following table describes frame subtypes and their values. The value must be two hex pairs. When a match is found between frame subtype and value, the specified action is taken.

To customize subtype filters

1. From the main menu, click IP Tunnels, and then click Tunnel Filters.
2. Click Customizable Subtype Filters. The Customizable Subtype Filters screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IP Tunnels/Tunnel Filters/Customizable Subtype Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Tunnel Filters
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Network Management
Security
Maintenance
Submit Changes
Internet

	Allow/Pass	SubType	Value
1	□	DIX-IP-TCP-Port	00 00
2	□	DIX-IP-TCP-Port	00 00
3	□	DIX-IP-TCP-Port	00 00
4	□	DIX-IP-TCP-Port	00 00
5	□	DIX-IP-TCP-Port	00 00
6	□	DIX-IP-TCP-Port	00 00
7	□	DIX-IP-TCP-Port	00 00
8	□	DIX-IP-TCP-Port	00 00

3. For each frame subtype field, check or clear the check box to configure if the frame subtypes are passed or are dropped. If you check the check box, the frame subtype is allowed to pass.
4. Click the down arrow on the right side of the SubType field and choose the customizable frame subtype. For help, see the next table.
5. In the Value field enter the two hex pairs. For help, see the next table.
6. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Subtype Filter Descriptions

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.

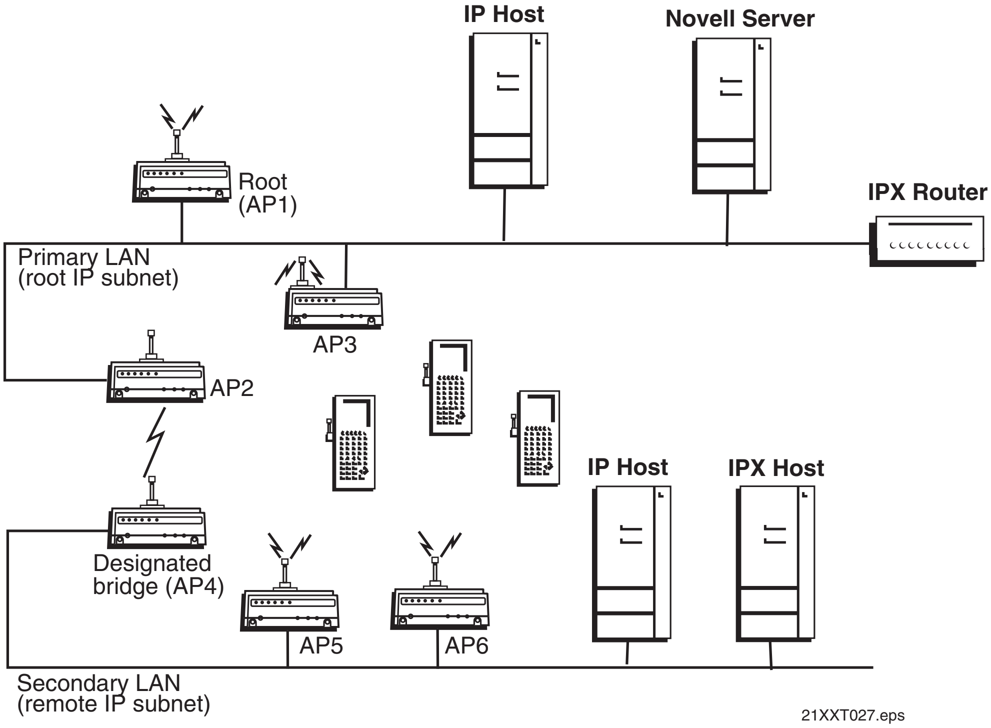
Subtype Filter Descriptions (continued)

Subtype	Value
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.

Filter Examples

These examples illustrate how to set both Ethernet and IP tunnel filters to optimize network performance. The next illustration includes

- wireless end devices using TCP/IP to communicate with other devices.
- a secondary LAN containing IP and IPX hosts, linked by AP2 and AP4.
- an IPX router connecting to another Novell network.
- DIX and 802.3 SNAP frames.

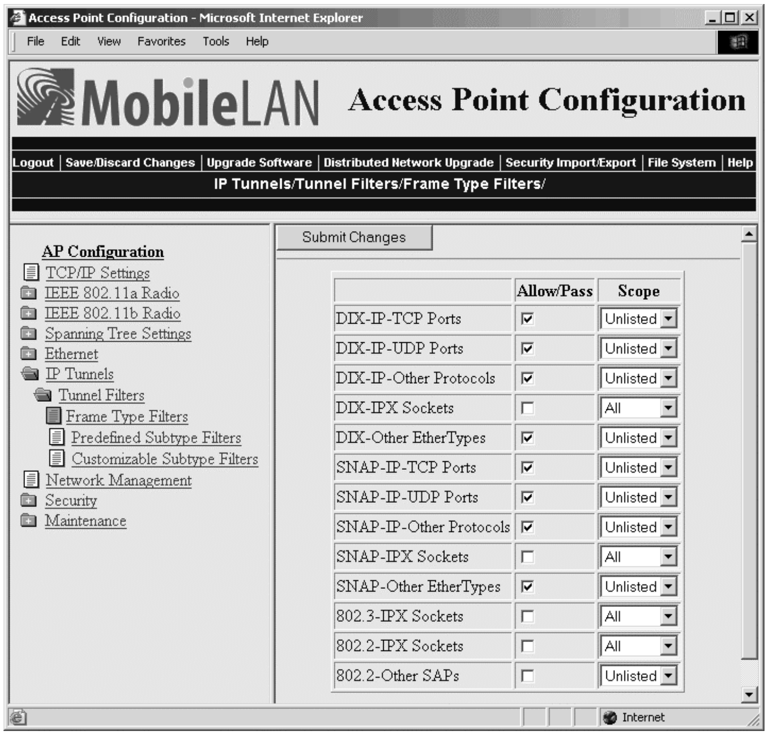


This illustration shows a typical network that will be used in the next examples.

Example 1

The root (AP1), AP3, AP5, and AP6 service only wireless end devices. These access points need to pass IP traffic, but not pass IPX traffic that does not need to be forwarded to the primary or secondary LAN.

For this example, set these options on the Ethernet Frame Type Filters screen. No subtype filters are needed.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IP Tunnels/Tunnel Filters/Frame Type Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Tunnel Filters
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Network Management
Security
Maintenance
Submit Changes
Internet

	Allow/Pass	Scope
DIX-IP-TCP Ports	☑	Unlisted
DIX-IP-UDP Ports	☑	Unlisted
DIX-IP-Other Protocols	☑	Unlisted
DIX-IPX Sockets	□	All
DIX-Other EtherTypes	☑	Unlisted
SNAP-IP-TCP Ports	☑	Unlisted
SNAP-IP-UDP Ports	☑	Unlisted
SNAP-IP-Other Protocols	☑	Unlisted
SNAP-IPX Sockets	□	All
SNAP-Other EtherTypes	☑	Unlisted
802.3-IPX Sockets	□	All
802.2-IPX Sockets	□	All
802.2-Other SAPs	□	Unlisted

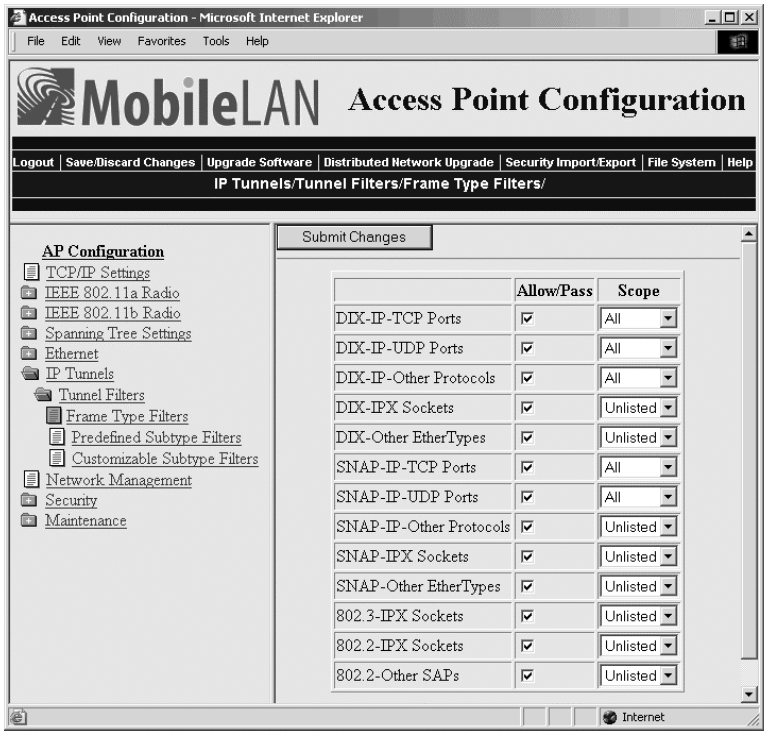
Example 2

AP2 and AP4 (designated bridge) service end devices and the IP host and IPX host on the secondary LAN. Also, these access points 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.

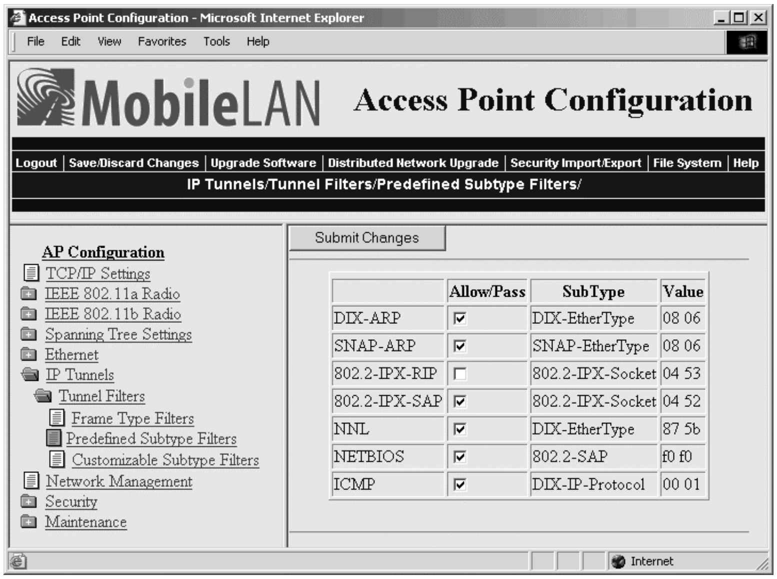
To filter the IPX RIP frames, you need to configure subtype filters. This example sets filters for three different cases: DIX, 802.2, and 802.3 SNAP frames. In many actual networks, only one type of filter is required, because all stations are configured using one of the three options.

For this example, set these options on the Ethernet Frame Type Filters screen.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IP Tunnels/Tunnel Filters/Frame Type Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Tunnel Filters
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Network Management
Security
Maintenance
Submit Changes
Internet

	Allow/Pass	Scope
DIX-IP-TCP Ports	☑	All
DIX-IP-UDP Ports	☑	All
DIX-IP-Other Protocols	☑	All
DIX-IPX Sockets	☑	Unlisted
DIX-Other EtherTypes	☑	Unlisted
SNAP-IP-TCP Ports	☑	All
SNAP-IP-UDP Ports	☑	All
SNAP-IP-Other Protocols	☑	Unlisted
SNAP-IPX Sockets	☑	Unlisted
SNAP-Other EtherTypes	☑	Unlisted
802.3-IPX Sockets	☑	Unlisted
802.2-IPX Sockets	☑	Unlisted
802.2-Other SAPs	☑	Unlisted

In the Predefined Subtype Filters screen, set the 802.2-IPX-RIP field to drop 802.2, DIX, and 802.3 frames.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
IP Tunnels/Tunnel Filters/Predefined Subtype Filters/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Tunnel Filters
Frame Type Filters
Predefined Subtype Filters
Customizable Subtype Filters
Network Management
Security
Maintenance
Submit Changes
Internet

	Allow/Pass	SubType	Value
DIX-ARP	☑	DIX-EtherType	08 06
SNAP-ARP	☑	SNAP-EtherType	08 06
802.2-IPX-RIP	□	802.2-IPX-Socket	04 53
802.2-IPX-SAP	☑	802.2-IPX-Socket	04 52
NNL	☑	DIX-EtherType	87 5b
NETBIOS	☑	802.2-SAP	f0 f0
ICMP	☑	DIX-IP-Protocol	00 01

Example 3

If you have a DHCP server on a Windows NT server and you want to use this DHCP server to assign TCP/IP parameters to end devices on a remote IP subnet, you need to set these filters to allow for the necessary IP tunneling.

1. On the root access point, set these filters:
   - On the Tunnel Filters screen, check the Allow IP Multicast check box.
   - In the IP Tunnel Frame Type Filter table, configure DIX-IP-UDP Ports to pass all frames.
2. On the access point at the endpoint of the IP tunnel, set this filter:
   - In the IP Tunnel Frame Type Filter table, configure DIX-IP-UDP Ports to pass all frames.

Example 4

If you have a Linux or Unix DHCP server and want to use this DHCP server to assign TCP/IP parameters to end devices on a remote subnet, you need to set this filter to allow for the necessary IP tunneling:

- In the IP Tunnel Frame Type Filter table, configure DIX-IP-UDP Port to pass all frames.

Comparing IP Tunnels to Mobile IP

MobileLAN access products support IP tunneling, which allows end devices to roam across different subnets (routers) without having to change IP addresses. IP tunneling supports IETF RFC 1701 using GRE and the same encapsulation technique as mobile IP. IP tunnels technology is designed primarily to operate in local environments, where hand-held or vehicle-mounted devices may move rapidly between access point coverage areas on a subnet (although it is possible to attach a geographically remote subnet through an IP tunnel).

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 wireless end devices that may move between geographically separated locations.

The two technologies are complimentary and may coexist. Both protocols use similar encapsulation to forward frames to or from end devices that have roamed away from a root IP subnet. The root access point functions much like a mobile IP home agent; an access point attached to the remote end of an IP tunnel functions much like a mobile IP foreign agent.

IP Tunnels and Mobile IP Comparison

Issue	IP Tunneling	Mobile IP
Software compatibility	No changes are required to existing IP software stacks in end devices.	Requires a mobile IP client software stack in end devices.
Addressing limitations for IP end devices	Requires that end device IP addresses belong to the root IP subnet.	None.
Security	Guest addresses are not used. Data link security.	Mobile IP authentication is required for “guest” access to foreign subnets.
Roaming detection	Data link indications facilitate fast roaming with no added broadcast traffic.	Foreign agent advertisements.
Roaming restrictions	Currently, roaming is limited to a single network that may include multiple IP subnets.	None.
Roaming support for non-IP protocols	Configurable using IP filters.	None.
Scalability	No practical limitations using IGMP.	Has no inherent limitations.
Special network software	Standard network feature. No additional network software is required.	Requires home and foreign agents located on each network or subnetwork.

Configuring Global Parameters

Global parameters are configured on the root access point and on any other access point that is a root candidate (does not have a root priority of 0). The root access point sends these settings to all other access points in the spanning tree. You should set the same global parameters for the root access point and its backup candidates. Any global parameters you set on the root access point will override those you set in other access points.

Configuring Global Flooding

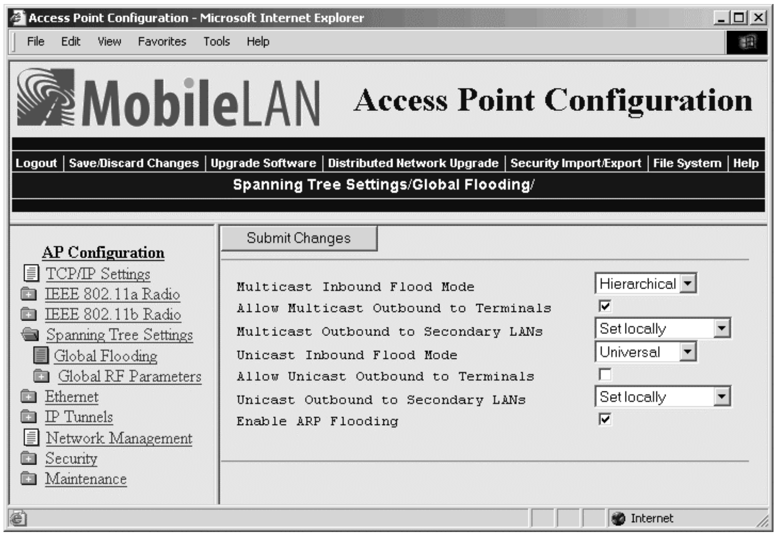
When the destination address is unknown, most bridges flood frames on all ports. Most wireless end devices operate at lower speeds than the Ethernet can support, therefore, indiscriminate flooding from a busy Ethernet network can consume a substantial portion of the available wireless bandwidth and reduce system performance. On the access point, you can set flooding control options for both unicast and multicast frames to free up bandwidth and improve system performance.

Access points try to forward frames to the port with the shortest path to the destination address. When the access point 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.

ARP requests are multicast frames that are periodically sent out to all devices on the Ethernet network. An ARP cache is a table of known MAC addresses and their IP addresses that the access point maintains. When an access point receives an ARP request, it checks its ARP cache to determine if the destination end device’s IP address is known.

To configure global flooding

1. From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.
2. Click Global Flooding. The Global Flooding screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Spanning Tree Settings/Global Flooding/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Global Flooding
Global RF Parameters
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

Multicast Inbound Flood Mode	Hierarchical
Allow Multicast Outbound to Terminals	☑
Multicast Outbound to Secondary LANs	Set locally
Unicast Inbound Flood Mode	Universal
Allow Unicast Outbound to Terminals	☐
Unicast Outbound to Secondary LANs	Set locally
Enable ARP Flooding	☑

3 Configure the Global Flooding parameters. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Global Flooding Parameter Descriptions

Parameter	Explanation
Multicast Inbound Flood Mode	Determines the flooding structure when this access point receives inbound multicast frames on non-root ports with unknown destination addresses. Choose Disabled if you do not want the access point to flood any inbound multicast frames. Choose Universal if the access point forwards the multicast frame to every port. This option uses more bandwidth. Use this option if the root access point is supporting more than one wireless hop to ensure that ARP requests and multicast traffic are distributed. Choose Hierarchical if the access point forwards the multicast frame only to the port to which the root access point is attached.
Allow Multicast Outbound to Terminals (Multicast Flood Mode enabled)	(802.11b, 802.11a, and OpenAir radios only) Determines if outbound multicast frames with unknown destination addresses are flooded toward end devices. Typically, this parameter is checked. However, if your wired devices do not need to initiate communication with wireless end devices, you may want to clear this check box.

Global Flooding Parameter Descriptions (continued)

Parameter	Explanation
Multicast Outbound to Secondary LANs (Multicast Flood Mode enabled)	Specifies if outbound multicast frames with unknown destination addresses are flooded toward secondary LANs. Choose Enabled if the root access point controls flooding for all the designated bridges on secondary LANs. Enabling this parameter makes managing secondary LANs easier because you do not need to set secondary LAN flooding parameters. Choose Set Locally if the designated bridges control flooding on their LANs.
Unicast Inbound Flood Mode	Determines the flooding structure when this access point receives inbound unicast frames on non-root ports with unknown destination addresses. Choose Disabled if you do not want the access point to flood any inbound unicast frames. Choose Universal if the access point forwards the unicast frame to every port. This option uses more bandwidth. Choose Hierarchical if the access point forwards the unicast frame only to the port to which the root access point is attached.
Allow Unicast Outbound to Terminals (Unicast Flood Mode enabled)	(802.11b, 802.11a, and OpenAir radios only) Determines if outbound unicast frames with unknown destination addresses are flooded toward end devices.
Unicast Outbound to Secondary LANs (Unicast Flood Mode enabled)	Specifies if outbound unicast frames with unknown destination addresses are flooded toward secondary LANs. Choose Enabled if the root access point controls flooding for all the designated bridges on secondary LANs. Enabling this parameter makes managing secondary LANs easier because you do not need to set secondary LAN flooding parameters. Choose Set Locally if the designated bridges control flooding on their LANs.
Enable ARP Flooding	Check this check box to enable ARP flooding. When an access point receives an ARP request, it checks its ARP cache to determine if the destination end device's IP address is known. If you enable ARP flooding and • the destination end device is known, the access point translates the ARP request into a unicast frame, which is only forwarded to the destination end device. Therefore, all end devices do not need to wake up to listen to the ARP request, which saves battery life. • the destination end device is not known, the access point forwards the ARP request based on its flooding and filtering settings. If you disable ARP flooding, the access point ignores ARP requests for destination end devices that are not in its ARP cache. You should only use this option if you have no IP devices in your wireless network.

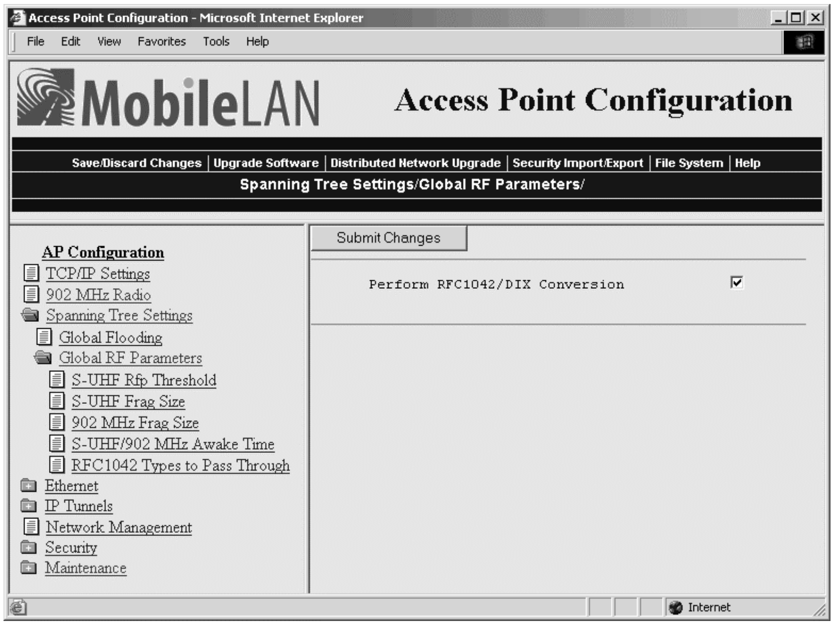
Configuring Global RF Parameters

Use global RF parameters to set various parameters on the access points. If you are configuring the root access point and you check the Set Globally check box, the value for that parameter is set globally for all access points and wireless end devices in the network. If you are configuring the root access point and you clear the Set Globally check box or if you are not configuring the root access point, each device uses its local setting.

To configure global RF parameters

1 From the menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.

2 Click Global RF Parameters. The Global RF Parameters screen appears.



Perform RFC1042/DIX Conversion ☑

Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Spanning Tree Settings/Global RF Parameters/
Submit Changes
AP Configuration
TCP/IP Settings
902 MHz Radio
Spanning Tree Settings
Global Flooding
Global RF Parameters
S-UHF Rfp Threshold
S-UHF Frag Size
902 MHz Frag Size
S-UHF/902 MHz Awake Time
RFC1042 Types to Pass Through
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Internet

3 Configure the global RF parameters. Click the links in the Global RF Parameters menu to set more parameters. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Global RF Parameter Descriptions

Parameter	Explanation
Perform RFC1042/DIX Conversion (802.11b or 802.11 radios only)	Determines how the access point will handle the conversion of RFC1042/DIX frames that are received on its 802.11b or 802.11a ports. Check this check box if the frames that are received and have a protocol type equal to a value in the “RFC1042 types to pass through” list are forwarded without conversion. If the frame has a protocol types that is not found in the list, it will be converted to DIX format before it is forwarded. Clear this check box if the frames that are received are forwarded without conversion; that is, when a SNAP frame is received from an 802.11b or 802.11a radio with an OUI (Organizationally Unique Identifier) equal to 000000, it will be forwarded without conversion.
S-UHF Rfp Threshold (S-UHF radios only)	Specifies the largest data frame 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 (S-UHF radios only)	Specifies the largest data frame that can be transmitted without fragmentation. On certain radios, fragmentation does not occur unless the radio detects interference. Larger frame sizes can improve throughput on a reliable connection, while smaller frame sizes can improve throughput on a poor connection.
902 MHz Frag Size (902 MHz radios only)	Specifies the largest data frame that can be transmitted without fragmentation. On certain radios, fragmentation does not occur unless the radio detects interference. Larger frame sizes can improve throughput on a reliable connection, while smaller frame sizes can improve throughput on a poor connection.
S-UHF/902 MHz Awake Time (S-UHF and 902 MHz radios only)	Specifies the amount of time that a wireless end device stays awake when radios are inactive. A sleeping device is less responsive to radio activity; however, the longer a device is kept fully awake, the larger the drain on the battery. You should set a device 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.
RFC1042 Types to Pass Through (802.11b or 802.11a radios only)	If the RFC1042/DIX Conversion field is Enabled, this parameter specifies values for protocol types that are to be passed without conversion. The list includes the Apple Talk protocol type, value 80F3. Values entered in this parameter represent the protocol types of frames that will be passed without conversion to DIX format.

6 Configuring Security

This chapter explains how to use different security solutions to ensure that you have a secure wireless network. This chapter covers these topics:

- About the different security features and solutions you can implement
- Enabling access methods
- Enabling secure IAPP and secure wireless hops
- Setting up logins
- (IEEE 802.11b or IEEE 802.11a radios) Configuring WEP 64/128 security
- Configuring an access control list (ACL)
- (IEEE 802.11b or IEEE 802.11a radios) Configuring IEEE 802.1x security

Understanding Security

MobileLAN access products provide many different security features and solutions that you can use to create a secure wireless network. To create a secure wireless network, you need to be concerned about

- securing your backbone. Only authorized users should be able to communicate with your network.
- keeping your data private. Make it difficult for an eavesdropper, such as a rogue access point, to monitor your data.
- authenticating wireless end devices. End devices must prove who they are before they are allowed to communicate with your network

Depending on the radios in the access point and the amount of security you need in your network, you can implement one or more of the security solutions in the following table.

MobileLAN access Security Solutions

Security Type	Secure Backbone	Data Privacy	Client Authentication
Change default parameters	X		
Disable access methods	X		
Enable secure IAPP	X		
Enable secure wireless hops	X		X
Use WEP 64/128 security/ Configure security ID		X	
Use a password server to control access point logins	X		
Use an access control list (ACL)			X
Use an 802.1x security solution	X	X	X

These security features and solutions are listed below in the order of amount of security and ease of use (most basic/least secure to most secure). Intermec recommends you at least change the default parameters, use basic security (WEP 64/128 security or security ID), and enable secure IAPP and secure wireless hops (Steps 1 through 4).

1 Change default parameters on access points and wireless end devices.

(802.11b/802.11a) Change the SSID from its default value of INTERMEC.

(OpenAir) Change the LAN ID from its default value of 0.

For help, see Chapter 4, “Configuring the Radios.”

2 Enable/disable access methods. For example, if you are not using Telnet sessions to configure or manage your access point, you can disable this access method. For help, see “Enabling Access Methods” in the next section.

3 Enable secure IAPP and secure wireless hops. Even if you are not configuring an 802.1x-enabled network, you can enable secure IAPP, which prevents unauthorized MobileLAN access products from joining the spanning tree. For help, see “Enabling Secure IAPP and Secure Wireless Hops” later in this chapter.

4 (802.11b/802.11a) Configure basic WEP 64/128 security. You can configure up to four different WEP keys on the access point and most wireless end devices, and then you specify which key is being used to encrypt data. You should periodically change which WEP key these devices use. For help, see “Configuring WEP 64/128 Security” later in this chapter.

(OpenAir) Use a security ID. For help, see “Configuring the WLI Forum OpenAir Radio” in Chapter 4.

5 Use a password server to maintain a list of authorized users who can configure and manage the access points. You can either use an external RADIUS server or you can use any access point’s embedded authentication server (EAS).

Or, change the default login for users who need to be able to configure or manage the access point.

For help, see “Setting Up Logins” later in this chapter.

6 Use a RADIUS server to maintain an access control list (ACL), which is a list of MAC addresses of end devices that can connect to the network through access point. You can either use an external RADIUS server or you can use any access point’s embedded authentication server (EAS). For help, see “Using an Access Control List (ACL)” later in this chapter.

7 (802.11b/802.11a) Use an 802.1x security solution. 802.1x security provides a framework to authenticate user traffic to a protected 802.11b or 802.11a network. Using 802.1x security provides secure data transmission by enabling secure IAPP, enabling secure wireless hops, and dynamically rotating the WEP keys. You configure the access point as an authenticator.

For the authentication server, you can either use an external RADIUS server or you can use a newer access point’s embedded authentication server (EAS).

For help, see “Configuring 802.1x Security” later in this chapter.

For help troubleshooting security, see “Troubleshooting Security” in Chapter 8.

Intermec is constantly evaluating new and more robust security solutions. For more information, contact your local Intermec representative.

Enabling Access Methods

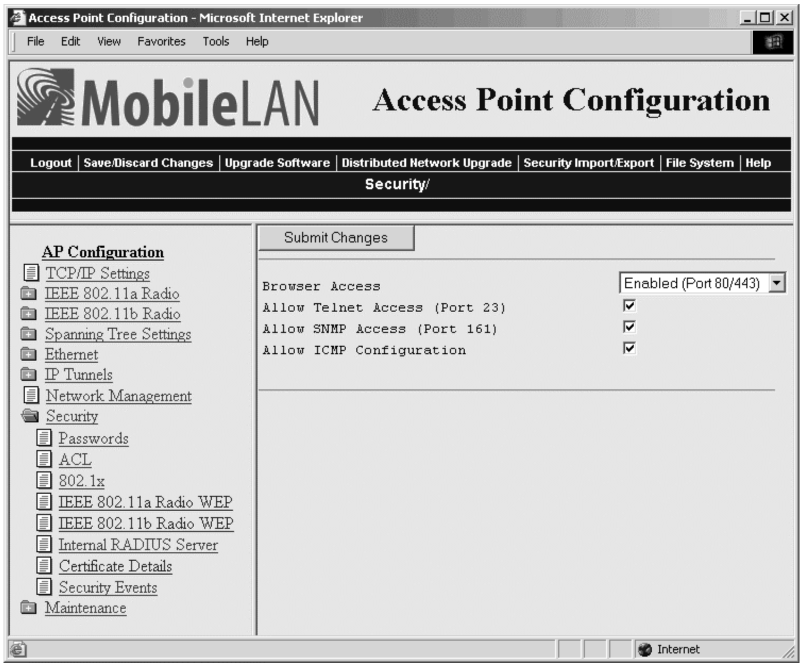
There are four access methods that you can enable or disable depending on how you want users to be able to configure or manage the access points:

- Web browser interface (HTTP or HTTPS)
- Telnet session
- MobileLAN manager or any other SNMP management station
- MobileLAN access Utility or any other program that uses ICMP echo

All access methods are enabled by default. You may want to disable any of these methods that you will not use to prevent access by an unauthorized method.

To enable or disable access methods

1 From the main menu, click Security. The Security screen appears.



Browser Access	Enabled (Port 80/443)
Allow Telnet Access (Port 23)	☑
Allow SNMP Access (Port 161)	☑
Allow ICMP Configuration	☑

2 Enable or disable the access methods that users can use to connect to the access point. For help, see the next table.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Security Parameter Descriptions

Parameter	Description
Browser Access	Determines if users can use a web browser to configure or manage this access point. Browser access is through either port 80 or port 443. Choose Secure-Only if you want to force users to log in using the secure web browser (HTTPS) interface. Secure-only access is through port 443. This feature is only available on the newer access points (WA22, 2101B, WA21, 2100D, and 2106).
Allow Telnet Access	Determines if users can use a telnet session (or a communications program) to configure or manage this access point. Telnet access is through port 23.
Allow SNMP Access	Determines if users can use MobileLAN manager or another SNMP management station to configure or manage this access point. SNMP access is through port 161.
Allow ICMP Configuration	Determines if users can use the MobileLAN access Utility or another program that uses ICMP echo (PING) to set the IP address or restore factory defaults on this access point.

Enabling Secure IAPP and Secure Wireless Hops

Secure IAPP prevents unauthorized MobileLAN access products from joining the spanning tree and it encrypts IAPP frames. If you enable secure IAPP, when access points communicate with each other through the radios, they will create secure wireless hops using the Secure Wireless Authentication Protocol (SWAP). SWAP forces access points to authenticate each other using an EAP-MD5 challenge.

By default, secure IAPP is disabled. All MobileLAN access products have the same IAPP secret key so they can communicate with each other. You can enable secure IAPP and secure wireless hops in any type of radio network.

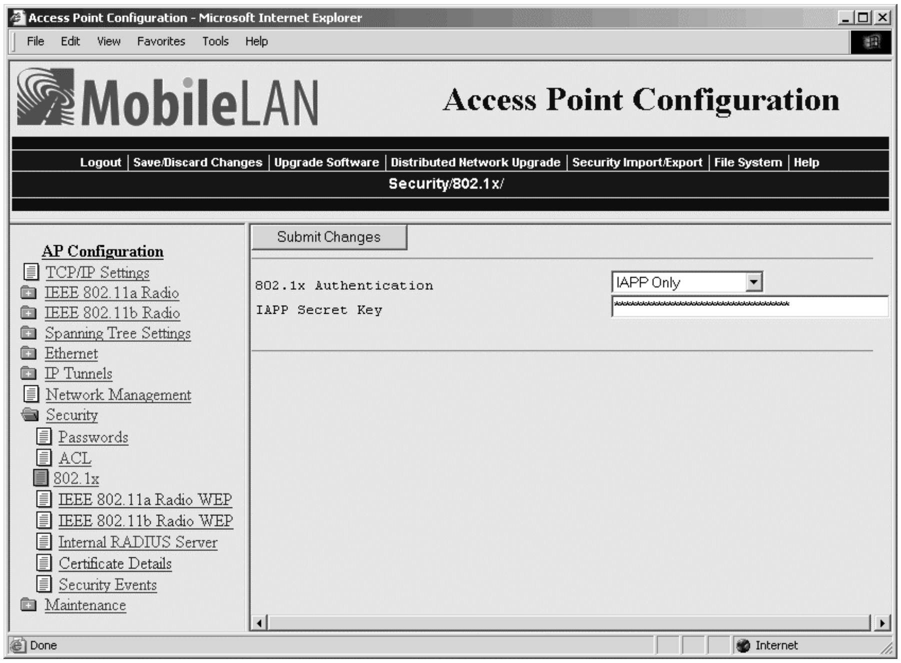
Note these potential problems:

- If you enable secure IAPP on a root access point that is running software release 1.80 or later and other access points in your network are running an earlier software release than 1.80, the access points with the earlier software release will not attach to the root. The access points with the earlier software release do not support secure IAPP. If you want to use secure IAPP, upgrade all access points to software release 1.80.
- If you enable secure IAPP on a non-root access point and the root access point has secure IAPP disabled, the access points will form separate spanning trees with the same LAN ID. If you want to use secure IAPP, enable secure IAPP on all access points.

To enable secure IAPP and secure wireless hops

Note: You do not need to perform this procedure if you are enabling 802.1x authentication in your network. Enabling 802.1x authentication automatically enables secure IAPP and secure wireless hops. See “Configuring 802.1x Security” later in this chapter.

1 From the main menu, click Security and then click 802.1x. The 802.1x screen appears.



802.1x Authentication: IAPP Only

IAPP Secret Key: ********************************

2 In the 802.1x Authentication field, click the down arrow on the right side of the field and choose IAPP Only.

3 In the IAPP Secret Key field, enter a secret key. This secret key must be between 16 and 32 bytes.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

5 Repeat Steps 1 through 4 for each access point in your spanning tree. All access points must have the same IAPP secret key to communicate with each other.

In the access point that contains the master radio, click Maintenance and then click AP Connections. The AP Connections screen lists the station radios (including ones in other access points) that are communicating with the master radio. For help, see “Viewing AP Connections” in Chapter 8.

Setting Up Logins

To ensure login security for configuring or maintaining the access points, you should either use a password server (typically an EAS or another RADIUS server) or immediately change the default user name and password.

To use the password server, you must have:

- a password server on the network that contains the user name/password database. For help, see “Configuring the Access Point to Use a Password Server” in the next section.

  You can either use an external RADIUS server or you can configure an EAS as a password server. For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS).”

- access points, which are the RADIUS clients.

If you enable RADIUS authorization, when a user uses a web browser or telnet to access the access point configuration screens, the user will need to enter a user name and password. This login is sent through the RADIUS client to the RADIUS server. The server compares the user name and password to its list of authorized user names and passwords. If a match is found, the server returns an access-accept frame and the user is logged into the access point with read/write privileges.

If neither RADIUS server #1 nor RADIUS server #2 is available when the user attempts a login and the Allow Service Password check box is checked, the service password is checked. If the login does not match the service password, the login fails.

Note: Each time the service password login attempt fails, the process may take up to eight seconds.

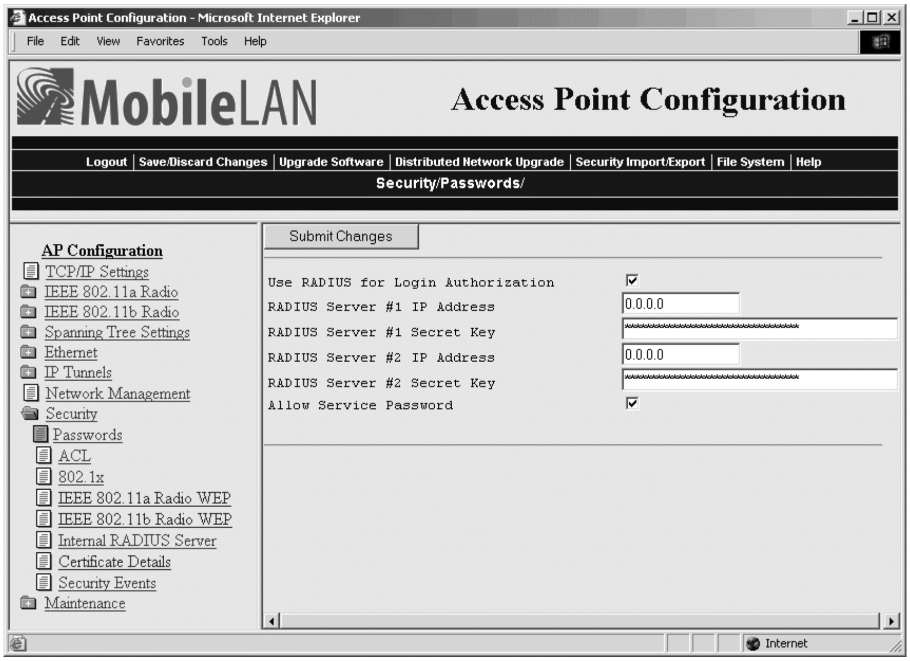
If you do not want to use RADIUS authorization, you should change the default login user name and password. You may also want to change the read-only password. For help, see “Changing the Default Login” later in this chapter.

Configuring the Access Point to Use a Password Server

If you use a password server to manage users who can log in to this access point, you need to tell this access point how to communicate with the password server and then you need to configure the password server. The password server can either be an external RADIUS server or you can use an EAS.

To configure the access point to use a password server

1 From the main menu, click Security, and then click Passwords. The Passwords screen appears.



```
Use RADIUS for Login Authorization      ☑
RADIUS Server #1 IP Address             0.0.0.0
RADIUS Server #1 Secret Key             ********************************
RADIUS Server #2 IP Address             0.0.0.0
RADIUS Server #2 Secret Key             ********************************
Allow Service Password                  ☑
```

2 Check the Use RADIUS for Login Authorization check box, and then click Submit Changes.

3 Configure the password parameters. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

5 Configure the password server.

a (Optional) If you change the default shared secret key, enter each access point as a RADIUS client and enter the shared secret key.

b Enter the user name and password for each user that is allowed to log in to this access point.

For help configuring an external RADIUS server, see the documentation that shipped with your server.

For help using an EAS, see Chapter 7, “Configuring the Embedded Authentication Server (EAS).”

Password Parameter Descriptions

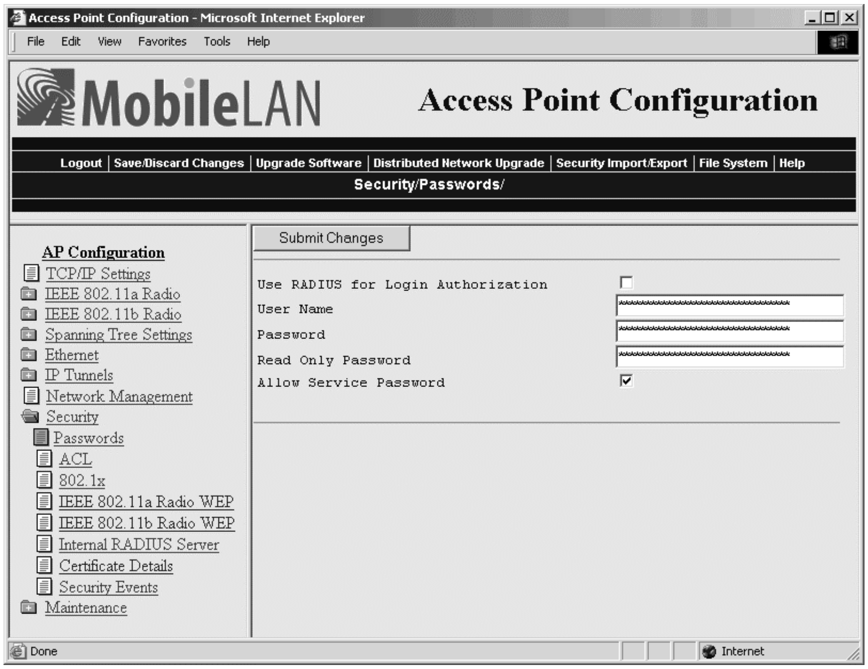
Parameter	Description
Use RADIUS for Login Authorization	Determines if you are using a password server to authenticate end devices that can communicate with this access point. Check this check box to use a password server .
RADIUS Server #1 IP Address	Enter the IP address of the password server that you want to use to authenticate user logins. If you are using an EAS, enter the IP address of the access point whose EAS you are using.
RADIUS Server #1 Secret Key	Enter the shared secret key for the password server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.
RADIUS Server #2 IP Address	Enter the IP address of the backup password server that you want to use to authenticate user logins if RADIUS server #1 is unavailable. If you are configuring an EAS, enter the IP address of the access point whose EAS you are using.
RADIUS Server #2 Secret Key	Enter the shared secret key for the backup password server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.
Allow Service Password	If RADIUS servers #1 and #2 are unavailable, check this check box to allow the login to be checked against the service password. Intermec Technical Support may use this service password if they need to troubleshoot this access point.

Changing the Default Login

If you are not using a password server to authorize user logins, you should change the default user name and password.

To set up logins

1. From the main menu, click Security, and then click Passwords. The Passwords screen appears.



Use RADIUS for Login Authorization □
User Name ********************************
Password ********************************
Read Only Password ********************************
Allow Service Password ☑

2. Clear the Use Radius for Login Authorization check box, and then click Submit Changes.
3. Configure the password parameters. For help, see the next table.
4. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

Once the changes are activated, you must enter these new values when you use a web browser or telnet to connect to this access point.

Password Parameter Descriptions

Parameter	Description
Use RADIUS for Login Authorization	Determines if you are using a password server to authenticate end devices that can communicate with this access point. Clear this check box.
User Name	Enter the user name you need to use to log in to this access point. This parameter can be from 0 to 16 characters long. If you leave the user name and password fields blank, a user will not need to log in to the access point.
Password	Enter the password you need to use to log in to this access point. This password gives you read and write access to the access point configuration. This parameter can be from 0 to 16 characters long. If you leave the user name and password fields blank, a user will not need to log in to the access point.
Read Only Password	Enter the password you need to use to log in to this access point. This password gives the user read-only access to the access point. This user is able to view the configuration and execute diagnostics but cannot perform any tasks that affect the operation of the access point, such as changing configuration options, rebooting, or downloading software. To disable this password, delete it.
Allow Service Password	If the user enters a login that does not match either the user name and password or the read only password, check this check box to allow the login to be checked against the service password. Intermec Technical Support may use this service password if they need to troubleshoot this access point.

Configuring WEP 64/128 Security

Note: If you configure WEP 64/128 security for a radio, you cannot also enable 802.1x authentication for that radio. 802.1x security uses rotating WEP keys that are automatically generated.

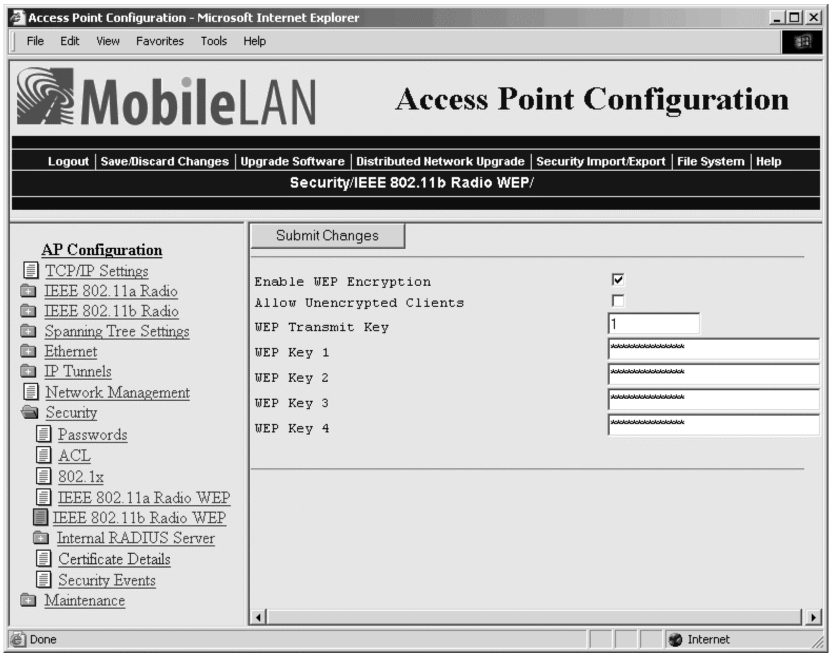
In your 802.11b or 802.11a network, you can configure static WEP keys (for WEP 64 or for WEP 128 security) to provide security between the access points and the wireless end devices. To use static WEP keys, your radios must support WEP encryption. All access points and wireless end devices on a particular network must use the same WEP encryption type and the same WEP transmit key. You should periodically change this WEP transmit key to prevent an unauthorized person with a sniffing tool from monitoring your network and discovering the WEP key.

Since, static WEP keys can be difficult to update, the MobileLAN access products and other Intermec products let you enter up to four WEP keys, and then pick a WEP transmit key (1-4). It is easier to rotate the WEP transmit key than to individually change all the WEP keys. For improved security, use 802.1x security.

WEP 64 has four 40-bit encryption keys and one 24-bit initialization vector (IV) key. To use WEP 64, you enter five ASCII characters or five hex pairs for the WEP keys. WEP 128 provides a higher degree of encryption protection. It has four 104-bit encryption keys and one 24-bit IV key. For WEP 128, you enter 13 ASCII characters or hex pairs.

To configure WEP 64/128 security

1 From the main menu, click Security, and then click IEEE 802.11b Radio or IEEE 802.11a Radio. The appropriate radio screen appears.



```
Enable WEP Encryption          ☑
Allow Unencrypted Clients      ☐
WEP Transmit Key               1
WEP Key 1                      **************
WEP Key 2                      **************
WEP Key 3                      **************
WEP Key 4                      **************
```

2 Check the Enable WEP Encryption check box, and then click Submit Changes.

3 Configure the parameters for WEP configuration. To ensure maximum security, configure each WEP key with a different WEP code. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

WEP Configuration Parameter Descriptions

Parameter	Explanation
Enable WEP Encryption	Determines if you are using WEP 64/128 security. Check this check box.
Allow Unencrypted Clients	Determines if the access point will receive transmissions from wireless end devices that are not using WEP encryption. Check this check box to accept transmissions from devices that are not using WEP encryption. Clear this check box to block transmissions from end devices that are not using WEP encryption.
WEP Transmit Key	Determines which of the four WEP keys this access point uses to transmit data.
WEP Key 1 through WEP Key 4	For WEP 64, you enter five ASCII characters or five hex pairs. For WEP 128, you enter 13 ASCII characters or hex pairs. To enter a hexadecimal key, prefix it with 0x. For example, the ASCII key ABCDE is equivalent to 0x4142434445.

Using an Access Control List (ACL)

You can use an access control list (ACL) to list the MAC addresses that are authorized to communicate with the network through the access point. The end devices do not need any special client software.

To use the ACL, you must have

- a RADIUS server on the network that contains the ACL.

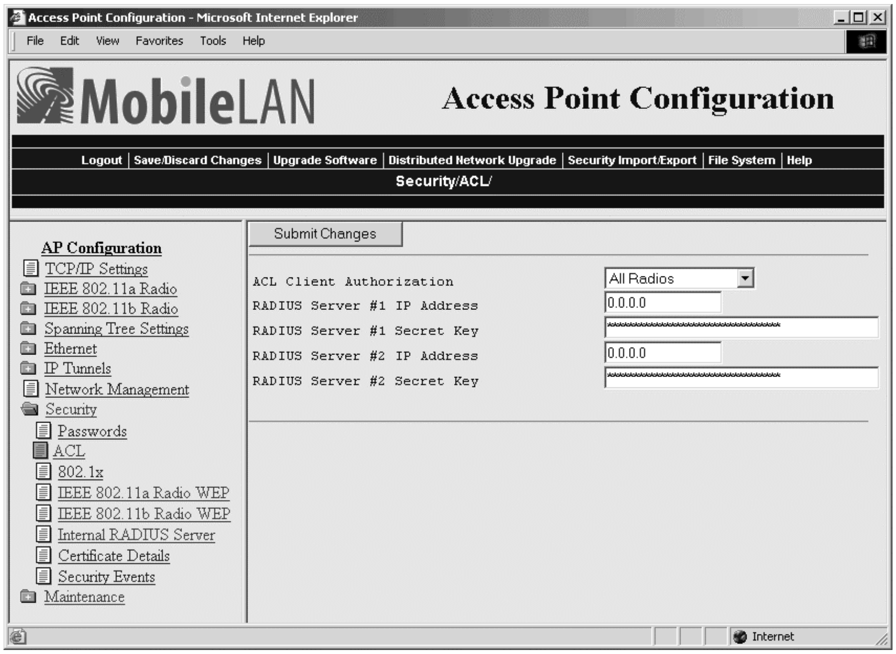
  You can either use an external RADIUS server or you can configure an EAS. For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS).”

- access points, which are the RADIUS clients.

If the access point has two radios, you can use an ACL for one radio and another type of security for the other radio. For example, you have some end devices that have an 802.1x supplicant and you have some end devices that do not have a supplicant. You can enable one radio to use 802.1x authorization and the other radio to use an ACL. You can also use one ACL for both radios. However, you cannot use a different ACL for each radio.

To use an ACL

1 From the main menu, click Security, and then click ACL. The ACL screen appears.



ACL Client Authorization	All Radios
RADIUS Server #1 IP Address	0.0.0.0
RADIUS Server #1 Secret Key	********************************
RADIUS Server #2 IP Address	0.0.0.0
RADIUS Server #2 Secret Key	********************************

2 In the ACL Client Authorization field, click the down arrow on the right side of the field. Choose which radio network will use the ACL or choose All Radios.

3 Configure the RADIUS server parameters. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

5 Configure the RADIUS server.

a (Optional) If you change the default shared secret key, enter each access point as a RADIUS client and enter the shared secret key.

b Enter the MAC address for each end device radio that is allowed to communicate to the network.

(902 MHz WAP only) Enter the Ethernet MAC address for each WAP that is allowed to communicate with the network.

For help configuring an external RADIUS server, see the documentation that shipped with your server.

For help using an EAS, see Chapter 7, “Configuring the Embedded Authentication Server (EAS).”

ACL Parameter Descriptions

Parameter	Description
ACL Client Authorization	Determines if this access point uses an ACL. Click the down arrow on the right side of the field and choose which radio uses an ACL to authenticate end devices.
RADIUS Server #1 IP Address	Enter the IP address of the RADIUS server that contains the ACL. If you are configuring an access point as a RADIUS server, enter the IP address of the access point.
RADIUS Server #1 Secret Key	Enter the shared secret key for the RADIUS server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.
RADIUS Server #2 IP Address	Enter the IP address of the backup RADIUS server that contains the ACL if RADIUS server #1 is unavailable. You cannot use this server to provide more ACL entries.
RADIUS Server #2 Secret Key	Enter the shared secret key for the backup RADIUS server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.

Configuring 802.1x Security

MobileLAN access products can help implement 802.1x security in an 802.11b or 802.11a network. The IEEE 802.1x standard provides an authentication protocol for 802.11 LANs. 802.1x provides strong authentication, access control, and key management, and lets wireless networks scale by allowing centralized authentication of wireless end devices. Intermec can provide a complete 802.1x security solution. For more information, see the *MobileLAN secure 802.1x Security Solution Installation Guide* (P/N 073134).

The 802.1x authentication process uses a RADIUS server, which is the authentication server, and access points, which are the authenticators, to manage the wireless end device authentication and wireless connection attributes. Extensible Authentication protocol (EAP) authentication types provide devices with secure connections to the network. They protect credentials and data privacy. Examples of EAP authentication types include Transport Layer Security (EAP-TLS) and Tunneled Transport Layer Security (EAP-TTLS).

To implement 802.1x security, you must have the following:

- A trusted certificate authority (CA), which issues digital authentication certificates. The authentication server must have a certificate installed on it. Also, if the end devices are using EAP-TLS, each one needs a client certificate.

  Intermec and others can provide the service of acting as a certificate authority and can issue certificates. For more information, contact your local Intermec representative.

- An authentication server (RADIUS server), which is software that is installed on a PC or server on your network or an EAS. The authentication server accepts or rejects requests from end devices that want to communicate with the 802.1x-enabled network.

  Note: If you use an EAS, you must use the EAS on a newer access point (WA22, 2101B, WA21, 2100D, or 2106) and your end devices must be running the EAP-TLS or EAP-TTLS supplicant.

  For help, see Chapter 7, "Configuring the Embedded Authentication Server (EAS)."

- An authenticator, which is an access point on your network. The authenticator receives requests from end devices that want to communicate with the network and forwards these requests to the authentication server. The authenticator also distributes the WEP keys to end devices that are communicating with it.

- End devices that are 802.1x-enabled. These end devices have an 802.11b or an 802.11a radio and a supplicant (EAP-TLS or EAP-TTLS) loaded on them. Supplicants allow your end devices to request communication with the authenticator using a specific EAP authentication type. For more information on the availability of 802.1x-enabled end devices, contact your local Intermec representative.

If the access point has two radios, you can implement 802.1x security on one radio network or both radio networks, as long as the radio supports 802.1x security. For example, you have some end devices that have a supplicant, but you also have some end devices that do not have a supplicant. You can enable one 802.11b radio to use 802.1x authorization and the other 802.11b radio to use an ACL.

About Secure IAPP and Secure Wireless Hops

Secure IAPP prevents unauthorized MobileLAN access products from joining the spanning tree and it encrypts IAPP frames. If you enable secure IAPP, when access points communicate with each other through the radios, they will create secure wireless hops using the Secure Wireless Authentication protocol (SWAP). SWAP forces access points to authenticate each other using an EAP-MD5 challenge. For more information, see “Enabling Secure IAPP and Secure Wireless Hops” earlier in this chapter.

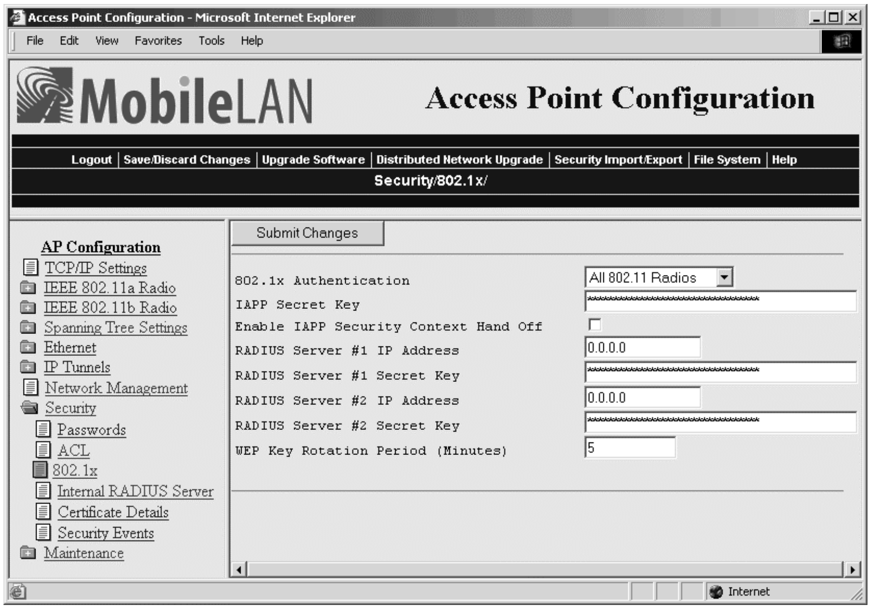
By default, secure IAPP is disabled. All MobileLAN access products have the same IAPP secret key so they can communicate with each other. When you configure the access point as an authenticator, you enable secure IAPP and secure wireless hops.

Configuring the Access Point as an Authenticator

The access point, when acting as an authenticator, receives requests from end devices that want to communicate with the network and forwards these requests to the authentication server. It also distributes the WEP keys to end devices that are communicating with it. Before you configure the access point as an authenticator, the access point should be installed and configured to communicate with the wireless end devices.

To configure the access point as an authenticator

1 From the main menu, click Security, and then click 802.1x. The 802.1x screen appears.



802.1x Authentication	All 802.11 Radios
IAPP Secret Key	********************************
Enable IAPP Security Context Hand Off	□
RADIUS Server #1 IP Address	0.0.0.0
RADIUS Server #1 Secret Key	********************************
RADIUS Server #2 IP Address	0.0.0.0
RADIUS Server #2 Secret Key	********************************
WEP Key Rotation Period (Minutes)	5

2 Click the down arrow on the right side of the 802.1x Authentication field, and then choose the radio networks that you want to implement 802.1x security, and then click Submit Changes.

3 Configure the parameters for 802.1x security. For help, see the next table.

4 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" in Chapter 1.

5 Configure the authentication server.

a (Optional) If you are using an EAS and you change the default shared secret key, enter each authenticator as a RADIUS client and enter the shared secret key. For help using an EAS, see Chapter 7, "Configuring the Embedded Authentication Server (EAS)."

b In the external RADIUS server, enter each authenticator's IP address and the shared secret key. For help configuring an external RADIUS server, see the documentation that shipped with your server.

802.1x Security Parameter Descriptions

Parameter	Explanation
802.1x Authentication	Determines if this access point uses 802.1x security. Click the down arrow on the right side of the field and choose which radio uses 802.1x security to authenticate end devices. Choose IAPP only if you only want to enable secure IAPP and secure wireless hops.
IAPP Secret Key	Enter a key that the access points use to encrypt and sign security context exchanges. This key must be the same in all access points and can contain from 16 to 32 characters. You can enter the key in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.
Enable IAPP Security Context Hand Off	Check this check box if you want to use IAPP for security context handoffs. This feature uses the advantages of the spanning tree for faster roaming. Devices do not have to perform a full reauthentication each time they roam between access points. Clear this check box if you want to use the 802.1x standard for reauthentication or if the supplicant functionality that is implemented on the end device does not support it. Currently, Trakker Antares terminals are the only end devices that support this feature.
Key Rotation Period	Enter how often (in minutes) the access point generates a new WEP key.

802.1x Security Parameter Descriptions (continued)

Parameter	Explanation
RADIUS Server #1 IP Address	Enter the IP address of the RADIUS server that you want to use to perform the 802.1x authentication.
RADIUS Server #1 Secret Key	Enter the shared secret key for the RADIUS server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.
RADIUS Server #2 IP Address	Enter the IP address of the backup RADIUS server that you want to perform the 802.1x authentication if RADIUS server #1 is unavailable. You cannot use this server to provide more entries.
RADIUS Server #2 Secret Key	Enter the shared secret key for the backup RADIUS server. You can enter the key from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x. For example, enter the ASCII key as ABCDE; enter the same hexadecimal key as 0x4142434445.

7 Configuring the Embedded Authentication Server (EAS)

This chapter explains how to configure the embedded authentication server (EAS) in your access point for different security solutions to ensure that you have a secure wireless network. This chapter covers these topics:

- About the EAS
- Installing certificates on the EAS
- Enabling the EAS
- Configuring the EAS database
- Managing the EAS database

About the Embedded Authentication Server (EAS)

The access point has an embedded authentication server (EAS), which is an internal RADIUS server. In your network, you can use the EAS on any access point. The EAS can act as

- a password server that maintains a list of logins of users who can configure and manage the access point.
- a RADIUS server that maintains an ACL, which is a list of MAC addresses that can connect to the network.
- a RADIUS server that maintains a list of RADIUS clients (usually access points) that are authorized to connect to the network.
- a RADIUS server that authorizes TLS and TTLS clients to connect to the network.

If you use the EAS, you may not need to buy an external RADIUS server. An EAS supports 128 clients. If you need to support more clients, you may be able to use the EAS on different access points for different purposes. For example, you can use the EAS on one access point as a password server and another EAS on another access point as the authentication server.

This table lists the maximum number of end devices that an EAS supports if you turn on the end devices **at the same time**. However, if you turn on the end devices in groups, the EAS supports 128 clients.

Maximum Number of Simultaneous Authentications

RADIUS Server Type	WA21, WA22, 2106	2101B, 2100D	All Other Access Points
Password server	70	70	70
ACL	128	128	128
802.1x authentication server (TTLS) and 700s	50	35	N/A
802.1x authentication server (TTLS) and Trakker Antares terminals	15	15	N/A

About Certificates

The access point needs a server certificate

- if you want to use the secure web browser interface (HTTPS).
- if this access point is an authentication server in your 802.1x-enabled network.

The certificate encrypts communication between the internal RADIUS server, RADIUS clients, and the supplicants and HTTPS clients. If you are configuring another access point as a backup RADIUS server, you should also install a unique certificate on it. Server certificates can be in either PKCS12 (*.P12/*.PFX) or *.PEM format.

If the access point supports clients running the TLS authentication type, it also needs a trusted certificate authority (CA) certificate. Trusted CA certificates can be in *.PEM format or *.CER format. They can contain several trusted CAs, but should be kept to a maximum file size of 2K.

How to Determine If You Need to Install a Certificate

Note: Certificates are only supported on newer access points (WA22, 2101B, WA21, 2100D, 2106). Older access points cannot use the secure web browser interface or be an authentication server.

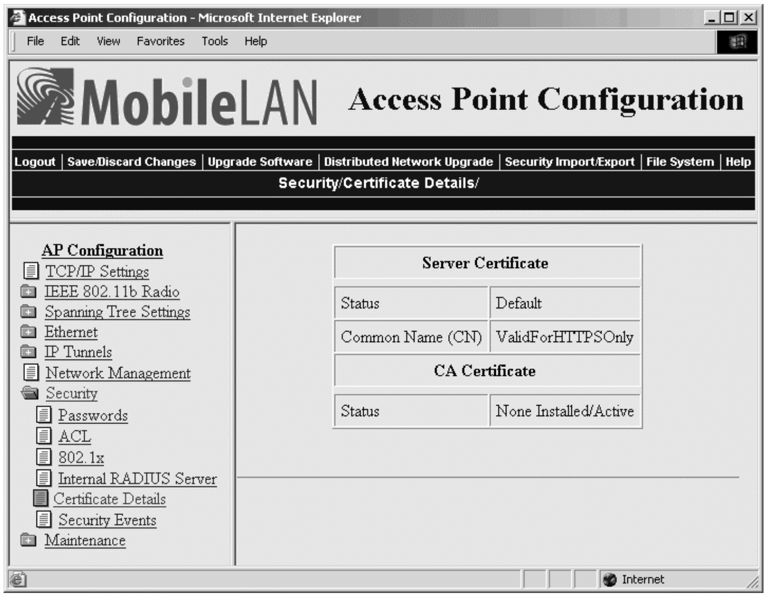
If your newer access point shipped from the factory with software release 1.80 or later preloaded on it, it has a unique server certificate (signed by Intermec) with a unique common name and passphrase. It also comes with an Intermec trusted CA certificate that supports clients running the TLS authentication type. These certificates support the secure web browser interface and provide basic security for all authentication types. You can also install certificates from a third-party certificate authority.

If you upgrade the access point to software release 1.80 or later, the software installs a default server certificate (ValidforHTTPSOnly). This certificate supports the secure web browser interface and it provides basic security for clients running the TTLS authentication type. If you use this access point as the authentication server, you should install a unique server certificate. Also, no trusted CA certificate is installed; therefore, it does not support clients running the TLS authentication type. Intermec can provide the service of acting as a certificate authority and can issue certificates. For more information, contact your local Intermec representative.

You can view the Certificate Details screen to determine which certificates are installed on the access point.

To view the certificates

- From the main menu, click Security, and then click Certificate Details.



Server Certificate	
Status	Default
Common Name (CN)	ValidForHTTPSOnly
CA Certificate	
Status	None Installed/Active

The Server Certificate lists the server certificate that is installed and the CA Certificate lists the trusted CA certificate that is installed.

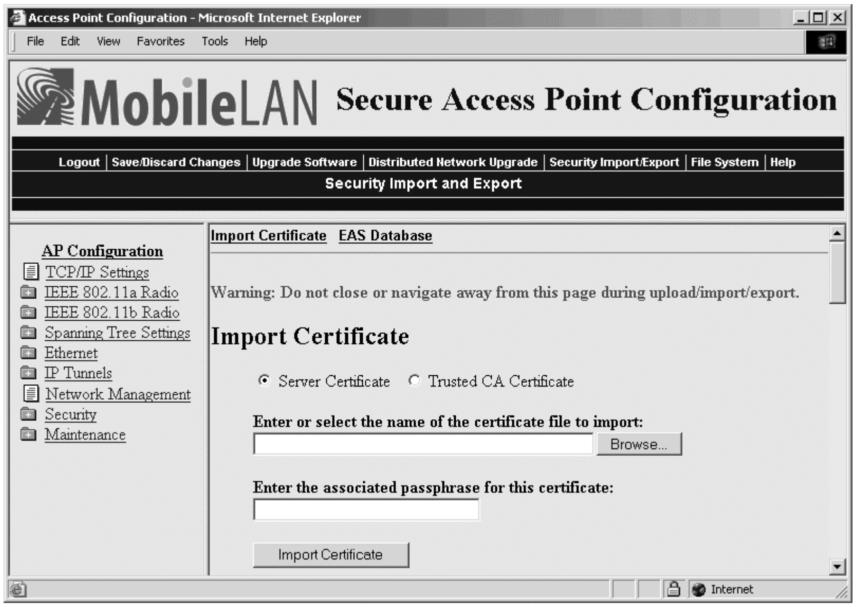
Installing and Uninstalling Certificates

Once you have determined that you need to install a certificate, use this procedure.

To install certificates

1. From the menu bar, click Security Import/Export, and then click Import Certificate. The Import Certificate screen appears.

2. If you are not using the secure web browser, click “A secure session is available” and log in to the access point using the secure web browser. Click Security Import/Export, and then click Import Certificate. The Import Certificate screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Secure Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Security Import and Export
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Import Certificate EAS Database
Browse...
Import Certificate
Internet

Warning: Do not close or navigate away from this page during upload/import/export.

Import Certificate

● Server Certificate ○ Trusted CA Certificate

Enter or select the name of the certificate file to import:

Enter the associated passphrase for this certificate:

3. Click Server Certificate or Trusted CA Certificate.

4. In the “Enter or select the name of the certificate file to import” field, enter the path and filename of the server certificate.

   Or, click Browse to locate the certificate.

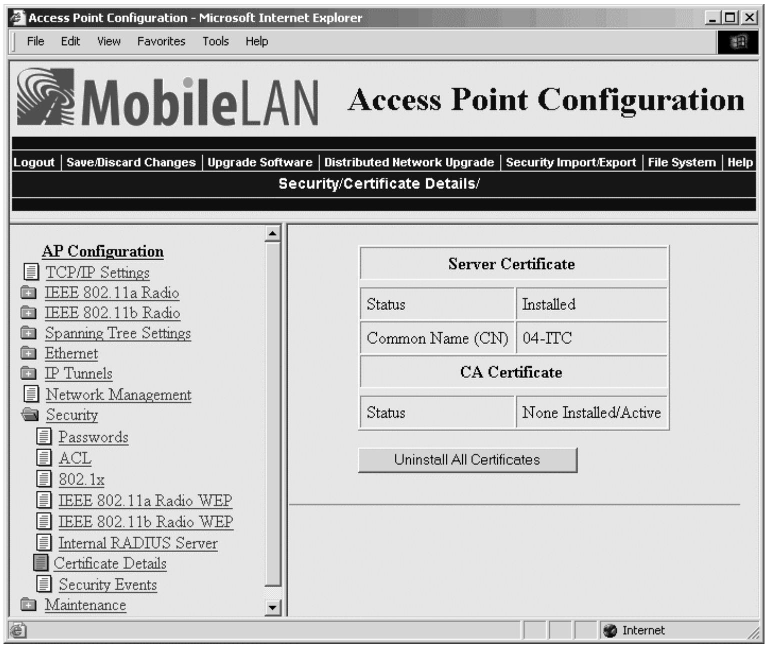
5. (Server Certificate only) In the “Enter the associated passphrase for this certificate” field, carefully enter the passphrase for the certificate.

6. Click Import Certificate.

To uninstall all certificates

Note: If you follow the procedure to uninstall all certificates, you will lose the unique server certificate and the trusted CA certificate. You will need to contact your local Intermec representative to purchase new certificates.

1 From the main menu, click Security, and then click Certificate Details.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Security/Certificate Details/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Passwords
ACL
802.1x
IEEE 802.11a Radio WEP
IEEE 802.11b Radio WEP
Internal RADIUS Server
Certificate Details
Security Events
Maintenance
Uninstall All Certificates
Internet

Server Certificate	
Status	Installed
Common Name (CN)	04-ITC
CA Certificate	
Status	None Installed/Active

2 Click Uninstall All Certificates. The unique server certificate and the trusted CA certificate are deleted.

You can still use the secure web browser interface and install new certificates using the default certificate (ValidforHTTPSOnly).

Configuring the EAS

Once you decide which access point will be configured to use its EAS, you need to enable the EAS on that access point and configure its database.

To configure the EAS

1 Install any certificates. For help, see “Installing and Uninstalling Certificates” earlier in this chapter.

2 On the access point that will contain the EAS, enable the EAS. For help, see “Enabling the EAS” in the next section.

3 Configure the EAS database. For help, see “Configuring the Database” later in this chapter.

4 Make sure that all access points that are using this EAS (as a password server, ACL, authentication server, etc.) are configured with this access point’s IP address in the appropriate RADIUS server IP Address field. For help, see

- “Configuring the Access Point to Use a Password Server” in Chapter 6.
- “Using an Access Control List (ACL)” in Chapter 6.
- “Configuring the Access Point as an Authenticator” in Chapter 6.

Enabling the EAS

In all MobileLAN access products, the default secret key is the same. By having the same default secret key, you can verify that all access points can communicate with the EAS. Then, for more security, you may want to change the secret key to prevent unauthorized access points from communicating with your network.

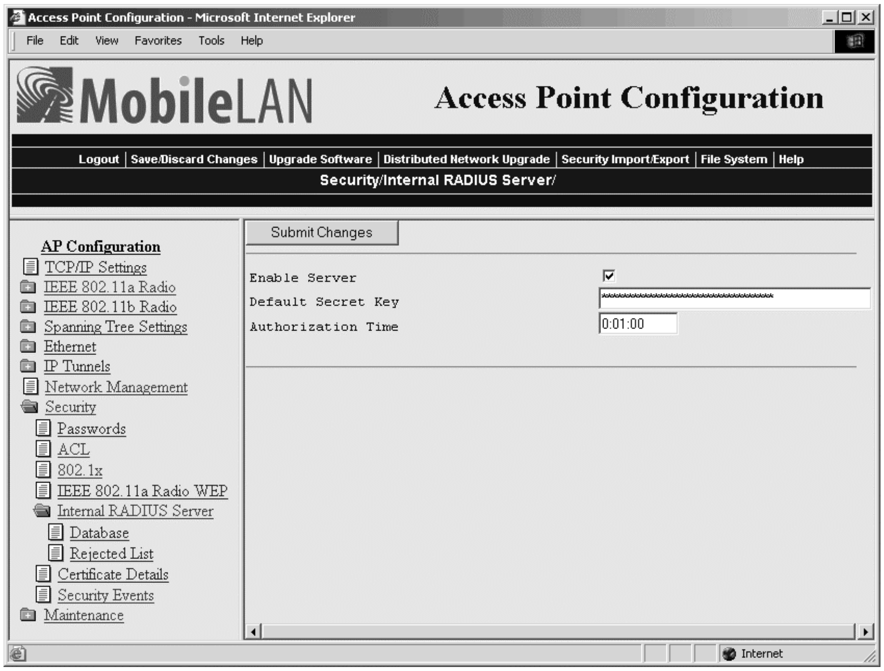
If you want to use the same secret key for communications between the EAS and all access points, in the Internal RADIUS Server screen, enter a new default secret key. Then, enter this same secret key into all appropriate RADIUS Server Secret Key fields.

If you want to use a unique secret key for communications between the EAS and each access point, you need to add each access point in your network to the EAS as a RADIUS client. Then, enter the unique secret key into each RADIUS Server Secret Key field. For help, see “Configuring the Database” in the next section.

To enable the EAS

1 Log in to the access point whose EAS you are enabling.

2 From the main menu, click Security, and then click Internal RADIUS Server. The Internal RADIUS Server screen appears.



Enable Server ☑

Default Secret Key ********************************

Authorization Time 0:01:00

3 Check the Enable Server check box, and then click Submit Changes.

4 (Optional) In the Default Secret Key field, enter a default secret key that is used between the EAS and the access points. This secret key can be from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x.

5 In the Authorization Time field, enter the amount of time that RADIUS clients (access points) remain authorized by the server before they need to be reauthorized. The format is `d:hh:mm`, where *d* is days, *hh* is hours, and *mm* is minutes.

If you enter 0s, the RADIUS server will only authenticate a RADIUS client the first time it connects.

6 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

7 If you entered a new secret key in Step 4 and you want to use this secret key for communications between the EAS and all access points, enter this secret key in all appropriate RADIUS Server Secret Key fields.

Configuring the Database

The EAS database contains up to 128 clients that this access point authorizes for logins, RADIUS clients, ACL clients, and 802.1x clients. This screen is hot settable; that is, to activate a change, you click Save/Discard changes, and then click Save Changes without Reboot.

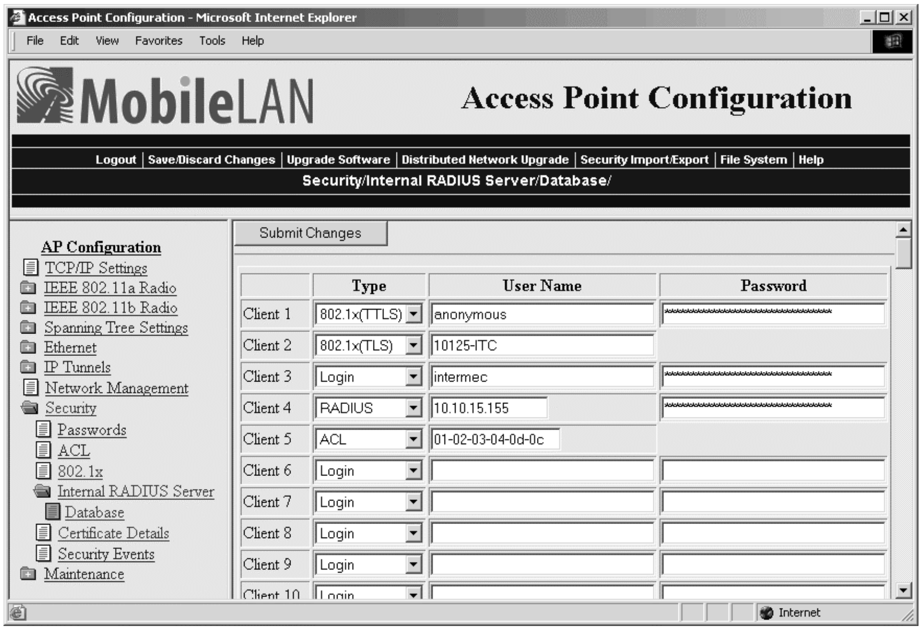
You can also create a database (using Microsoft Excel or Notepad) and then import it. Or, you can configure one database, export it, and import it to an EAS in the backup RADIUS server. For help, see "Exporting and Importing Databases" later in this chapter.

Note: Intermec recommends that when you are done configuring the database, you export it and save the file in a safe place. If you restore the access point to its default configuration, the database is not saved. For help, see "Exporting and Importing Databases" later in this chapter.

To configure the database

1 From the main menu, click Security, and then click Internal RADIUS Server.

2 Click Database. The Database screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Security/Internal RADIUS Server/Database/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Passwords
ACL
802.1x
Internal RADIUS Server
Database
Certificate Details
Security Events
Maintenance
Submit Changes
Internet

	Type	User Name	Password
Client 1	802.1x(TTLS)	anonymous	********************************
Client 2	802.1x(TLS)	10125-ITC	
Client 3	Login	intermec	********************************
Client 4	RADIUS	10.10.15.155	********************************
Client 5	ACL	01-02-03-04-0d-0c	
Client 6	Login		
Client 7	Login		
Client 8	Login		
Client 9	Login		
Client 10	Login		

3 In the Type field, click the down arrow on the right side of the field and choose the type of client you are entering in the database. For help, see the next table.

4 Click Submit Changes.

5 Enter the appropriate user name and password. User names and passwords can be from 1 to 32 characters. For help, see the next table.

6 Click Submit Changes.

7 Repeat Steps 3 through 6 for each client.

8 Click Save/Discard changes, and then click Save Changes without Reboot.

Internal RADIUS Server Entry Descriptions

Type	Description	User Name	Password
Login	Enter user names and passwords for users who are authorized to configure and maintain access points using the password server.	User name	User password
RADIUS	Enter a secret key that is shared by the RADIUS client (access point) and the RADIUS server. You do not need to enter any RADIUS clients if you do not change the default secret key. For more security, you should change the default secret key.	RADIUS client IP address	Secret key
ACL	Enter the end device radio MAC address for all end devices that are authorized to communicate with the network. (902 MHz WAP only) Enter the Ethernet MAC address for all WAPs that are authorized to communicate with the network.	MAC address	None
802.1x (TTLS)	Enter the login name and password of all end devices that are authorized to communicate with the 802.1x-enabled network. For more security, you should delete the user name “anonymous” and the password “anonymous.”	End device login name	End device login password
802.1x (TLS)	Enter the client certificate common name of all end devices that are authorized to communicate with the 802.1x-enabled network.	Client certificate common name	None

Using the Rejected List

The Rejected List screen displays the users and devices that have been rejected by the EAS. You can use this list to discover which users and devices may need to be added to the database. When using the web browser interface, you can immediately add previously rejected end devices to the database. You do not need to click Submit Changes or reboot the access point.

Note: When you reboot the access point, the rejected list is cleared.

To view the rejected list

1. From the main menu, click Security, and then click Internal RADIUS server.
2. Click Rejected List. The Rejected List screen appears.
3. Determine which users and devices you need to add to the database. For help understanding the list, see the next table.
4. Add users and devices to the database. For help see “Adding Entries to the Database” in the next section.

Rejected List Values

Column	Description
Type	Lists the type of authentication that failed. The type can be: Login, ACL, TTLS/PAP, TTLS/CHAP, TTLS/EAP, TTLS/MSCHAP, TTLS/MSCHAP-V2, or TLS.
User Name	Lists the value that was passed in the User Name field of the RADIUS server database during the failed attempt.
Last Time	Indicates how long ago the last authentication was attempted.
Count	Indicates how many times the authentication failed.
NAS IP Address	Displays the IP address of the RADIUS server that rejected the client.

Adding Entries to the Database

When you accept Login, ACL, TLS, and TTLS/PAP entries, they are added to the database and require no further configuration.

If the authentication type does not allow the EAS to learn the password of the rejected client (such as TTLS/CHAP), only the user name is added to the database. You need to manually enter the password into the database, click Submit Changes, click Save/Discard Changes, and then click Save Changes without Reboot.

To add all entries to the database

1 Click Select All Entries. A check box appears next to all entries.

2 Click Accept Selected Entries.

To add one entry to the database

1 Check the check box next to the entry you want to add to the database.

2 Click Accept Selected Entries.

Clearing the Rejected List

1 Click Select All Entries. A check box appears next to all entries.

2 Click Clear Selected Entries

Rebooting the access point will also clear the rejected list.

Exporting and Importing Databases

Note: Intermec recommends that you use the secure web browser interface (HTTPS) when you export and import databases. Otherwise, the information in the databases is sent in the clear.

The EAS database is simply a comma-separated text file. You can create the database offline (using Microsoft Excel or Notepad) and then import it. The file must have the following format:

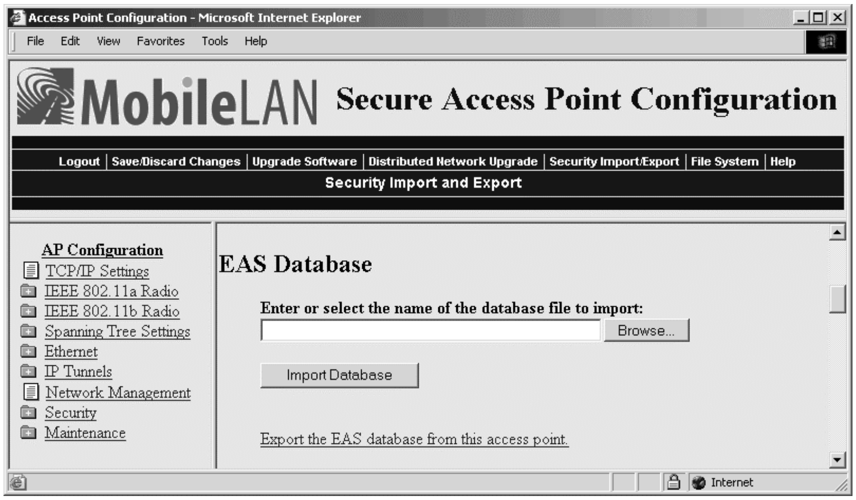
```
ACL, 11-22-33-44-55-66
TTLS, username, password
TLS, commonname
LOGIN, username, password
RADIUS, 0.0.0.0, secretkey
```

You should export the database so you have a backup version. You may also want to create the database in the primary RADIUS server, and then export it to a file that you can import to a backup RADIUS server.

To export a database

1 From the menu bar, click Security Import/Export, and then click EAS Database. The EAS Database screen appears.

2 If you are not using the secure web browser, click “A secure session is available” and log in to the access point using the secure web browser. Click Security Import/Export, and then click EAS Database. The EAS Database screen appears.

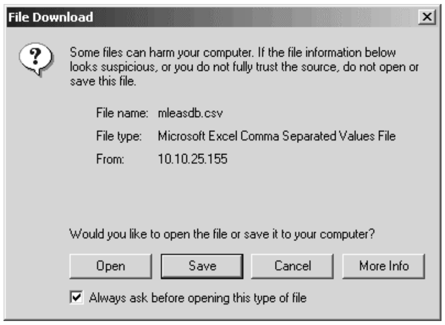

Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Secure Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Security Import and Export
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Browse...
Import Database
Internet

EAS Database

Enter or select the name of the database file to import:

Export the EAS database from this access point.

3 Click Export the EAS database from this access point. A File Download dialog box appears.



Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: mleasdb.csv

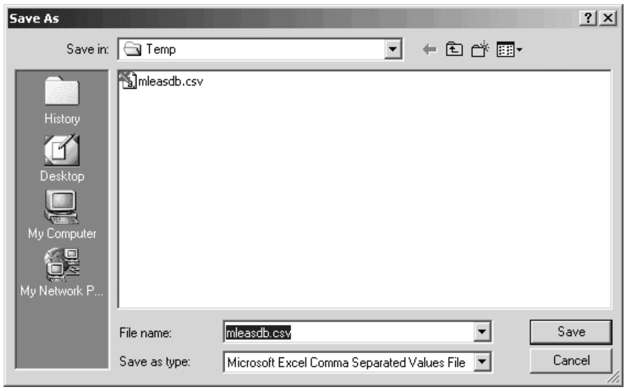
File type: Microsoft Excel Comma Separated Values File

From: 10.10.25.155

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

4 Click Save. The Save As dialog box appears.



Save in: Temp

File name: mleasdb.csv

Save as type: Microsoft Excel Comma Separated Values File

5 Choose the location and filename of the database. If you use the *.CSV extension, you can import it into Microsoft Excel, which recognizes it as a comma separated text file.

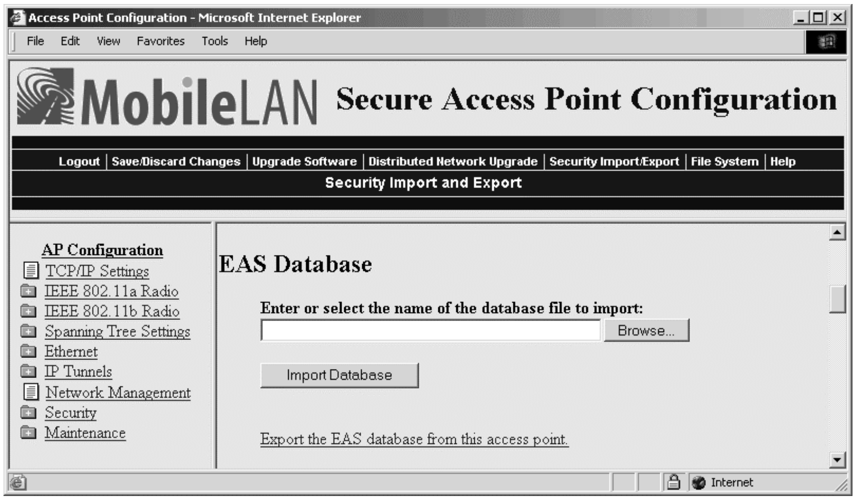
6 Click Save.

To import a database

Note: As soon as you import the database, it is active.

1 From the menu bar, click Security Import/Export. The EAS Database screen appears.

2 If you are not using the secure web browser, click “A secure session is available” and log in to the access point using the secure web browser. Click Security Import/Export. The EAS Database screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Secure Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Security Import and Export
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
EAS Database
Enter or select the name of the database file to import:
Browse...
Import Database
Export the EAS database from this access point.
Internet

3 Enter the path and filename of the database.

Or, click Browse to locate the file.

4 Click Import Database.

8 Managing, Troubleshooting, and Upgrading Access Points

This chapter explains how to manage, maintain, troubleshoot, and upgrade the MobileLAN access products. This chapter covers these topics:

- Managing the access points using an SNMP management station. You can also manage the access point using MobileLAN manager, a web browser, a communications program, or a telnet session.
- Maintaining the access points by using the LEDs and by understanding various maintenance screens. This section also explains how to restore the access point to its default configuration.
- Troubleshooting the access points. This section also explains how to recover a failed access point.
- Upgrading the access points using the MobileLAN access utility or a web browser.

Managing the Access Points

There are several methods that you can use to manage the access points. You can use

- MobileLAN™manager. You can purchase this software to make it easy for you to support your wireless network without having expert knowledge of access points or MIBs. It works with the access point's event-driven notification method (instead of traditional polling processes) to maintain real-time status on all access points. It also helps you troubleshoot your network by providing you with multiple views of your network, including what end devices are connected to which access point. For more information, go to mobilelan.intermec.com.
- a web browser. For help, see "Using a Web Browser Interface" in Chapter 1.
- a communications program, such as HyperTerminal. For help, see "Using a Communications Program" in Chapter 1.
- a telnet session. Go to an MS-DOS prompt and type `telnet` *`IPaddress`*, where *IPaddress* has the form *x.x.x.x* and *x* is a number from 0 to 255. For more help, see "Using a Communications Program" in Chapter 1. The interface looks similar.
- an SNMP management station. For help, see "Using Simple Network Management Protocol (SNMP)" in the next section.

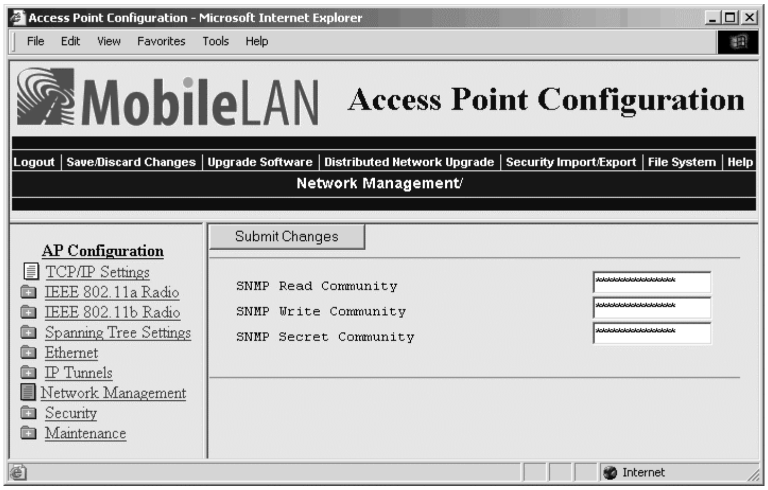
Using Simple Network Management Protocol (SNMP)

The access point can be managed using Simple Network Management Protocol (SNMP); that is, you access the access point from an SNMP management station. Contact your Intermec representative if you need to obtain a copy of the MIB.

Before you can use an SNMP management station, you must define the access point's SNMP community strings.

To configure the SNMP community strings

1 From the menu, click Network Management. The Network Management screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Network Management/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Submit Changes
Internet

SNMP Read Community ***************
SNMP Write Community ***************
SNMP Secret Community ***************

2 Configure the SNMP community parameters. For help, see the next table.

3 Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” in Chapter 1.

SNMP Community Parameter Descriptions

Parameter	Description
SNMP Read Community	Specify a password that provides read-only access. This password can be from 1 to 15 characters and is case sensitive.
SNMP Write Community	Specify a password that provides read and write access. This password can be from 1 to 15 characters and is case sensitive.
SNMP Secret Community	Specify a password that provides read and write access and lets the user change the community strings. This password can be from 1 to 15 characters and is case sensitive.

Maintaining the Access Points

The access point LEDs tell you with the status of the access point as it boots. They can also help you troubleshoot any internal problems.

The Maintenance menu lets you can view different parameters configured for the access point, including connections, port statistics, and a configuration summary. This information may be needed when you call Intermec Technical Support.

Understanding the LEDs Lighting Sequence

When the access point boots, the LEDs flash as it performs internal diagnostics. This table describes the LED activity during the boot process.

MobileLAN access LED Boot Sequence

Power	Wireless #1	Wireless #2	Wired LAN	Root/ Error	Description
○	●	●	●	○	Flash checksum being calculated
○	○	●	●	○	Flash checksum failure
○	●	●	○	●	RAM test in progress
○	○	●	○	●	RAM test failure
○	●	○	●	●	Monitor loading in progress
○	●	○	●	○	Ethernet test in progress
○	○	○	●	○	Ethernet test failure
○	●	☼	○	☼	Only Boot ROM code is available on access point. Load new files.

○ = On ● = Off ☼ = Flashing

After the access point successfully boots, the LEDs display the following pattern:

Power	Wireless #1	Wireless #2	Wired LAN	Root/Error
○	☼	☼ (if radio installed)	☼	☼ (if the access point is configured as the root)

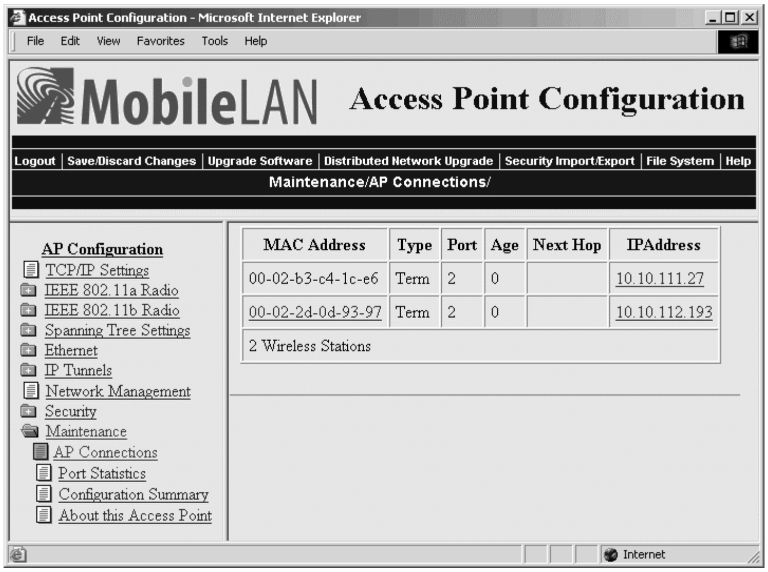
Viewing AP Connections

The AP Connections screen shows information about the devices (access points (AP) and end devices (Term)) that are connected through the spanning tree.

It also shows which devices are passed or blocked if you are using an ACL or if you implemented 802.1x security. In the ACL or 802.1x column, you will see a Pass or a Blocked. If an access point is connected to this access point, you will see the Ethernet MAC address. If a WAP is connected to this access point, you will see the radio MAC address. If an access point or WAP was blocked and should have been allowed to pass, re-enter the IAPP secret key in both devices.

To view AP connections

- From the menu, click Maintenance, and then click AP Connections. The AP Connections screen appears. This screen is read-only.



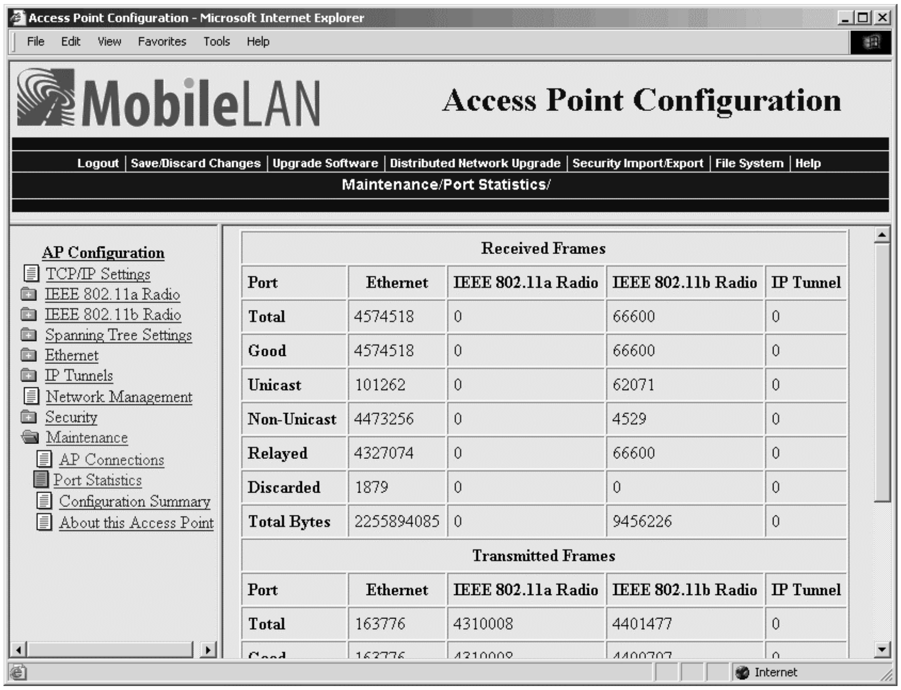
MAC Address	Type	Port	Age	Next Hop	IPAddress
00-02-b3-c4-1c-e6	Term	2	0		10.10.111.27
00-02-2d-0d-93-97	Term	2	0		10.10.112.193
2 Wireless Stations					

Viewing Port Statistics

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

To view port statistics

- From the menu, click Maintenance, and then click Port Statistics. The Port Statistics screen appears. This screen is read-only.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Maintenance/Port Statistics/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
AP Connections
Port Statistics
Configuration Summary
About this Access Point
Internet

Received Frames

Port	Ethernet	IEEE 802.11a Radio	IEEE 802.11b Radio	IP Tunnel
Total	4574518	0	66600	0
Good	4574518	0	66600	0
Unicast	101262	0	62071	0
Non-Unicast	4473256	0	4529	0
Relayed	4327074	0	66600	0
Discarded	1879	0	0	0
Total Bytes	2255894085	0	9456226	0

Transmitted Frames

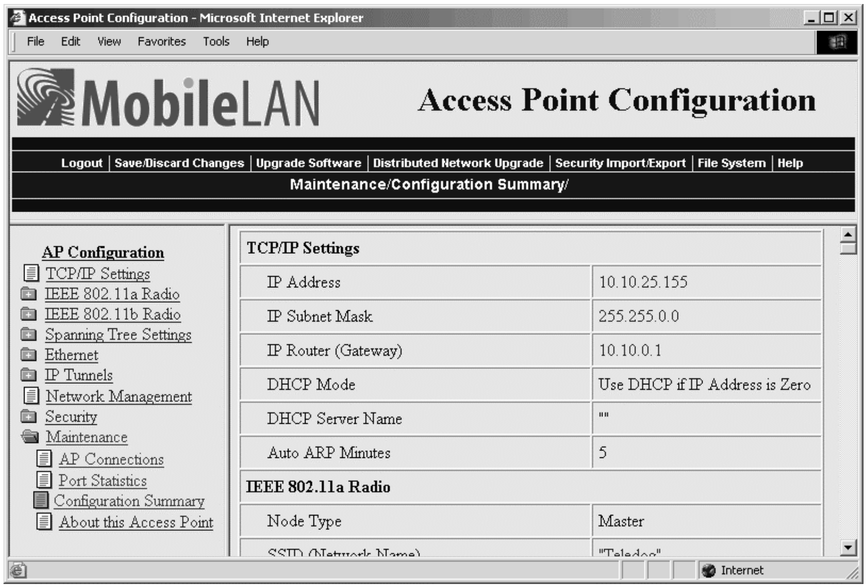
Port	Ethernet	IEEE 802.11a Radio	IEEE 802.11b Radio	IP Tunnel
Total	163776	4310008	4401477	0
Good	163776	4310008	4400707	0

Viewing the Configuration Summary

The Configuration Summary screen summarizes the configuration settings for the access point. Any changes from the default configuration that have been made to this access point are blue.

To view the configuration summary

- From the menu, click Maintenance, and then click Configuration Summary. The Configuration Summary screen appears. This screen is read-only.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Maintenance/Configuration Summary/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
AP Connections
Port Statistics
Configuration Summary
About this Access Point
Internet

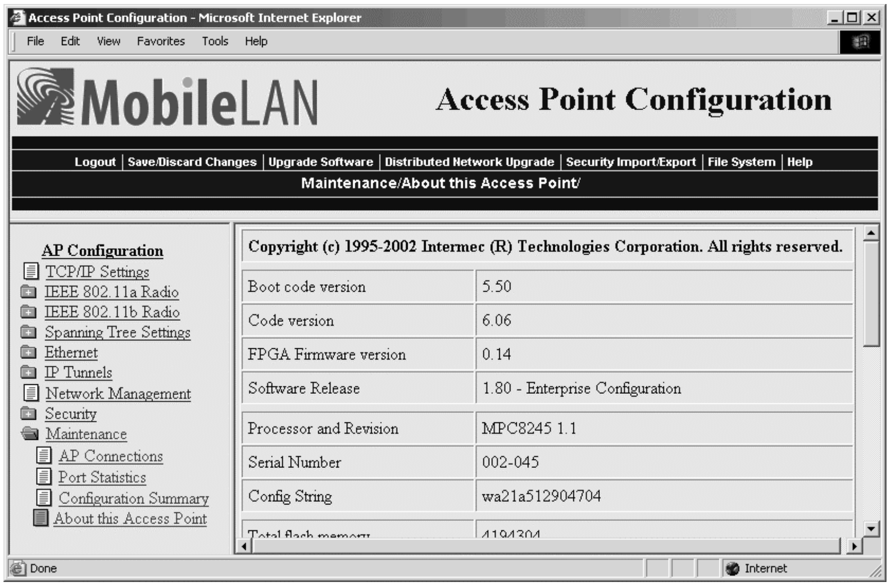
TCP/IP Settings	
IP Address	10.10.25.155
IP Subnet Mask	255.255.0.0
IP Router (Gateway)	10.10.0.1
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	""
Auto ARP Minutes	5
IEEE 802.11a Radio	
Node Type	Master
SSID (Network Name)	"Teledoc"

Viewing the About This Access Point Screen

This screen shows information about the access point including software versions, radio versions, and MAC addresses.

To view About this Access Point

- From the menu, click Maintenance, and then click About this Access Point. The About this Access Point screen appears. This screen is read-only.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Maintenance/About this Access Point/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
AP Connections
Port Statistics
Configuration Summary
About this Access Point
Done
Internet

Copyright (c) 1995-2002 Intermec (R) Technologies Corporation. All rights reserved.

Boot code version	5.50
Code version	6.06
FPGA Firmware version	0.14
Software Release	1.80 - Enterprise Configuration
Processor and Revision	MPC8245 1.1
Serial Number	002-045
Config String	wa21a512904704
Total flash memory	4194304

Restoring the Access Point to the Default Configuration

You may need to restore the access point to the factory default configuration. For a list of the default settings, see “Default Settings” in Appendix A. To restore the access point to the default configuration, you can use:

- MobileLAN access Utility. For help, see “Using the MobileLAN access Utility” in the next section.
- Web browser interface. For help, see “Using the Web Browser Interface” later in this section.

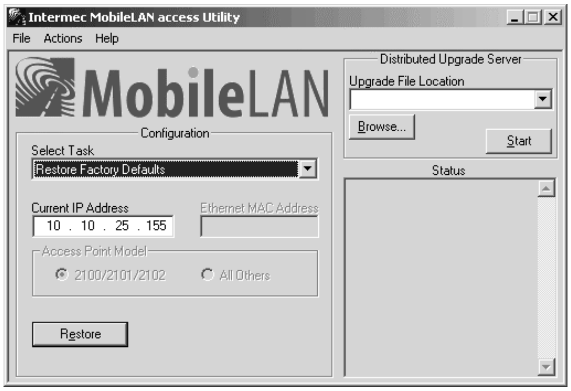
Using the MobileLAN access Utility

For help installing the MobileLAN access utility, see “Using the MobileLAN access Utility” in Chapter 1.

To restore the access point to the default configuration

1 Start the utility.

2 Click the down arrow on the right side of the Select Task field and choose Restore Factory Defaults.



Select Task: Restore Factory Defaults

Current IP Address: 10 . 10 . 25 . 155

Access Point Model: ● 2100/2101/2102 ○ All Others

3 In the Current IP Address field, enter the IP address of the access point you want to restore to factory defaults.

4 Disconnect and reconnect the power cable to the access point. The access point has no On/Off switch, so it boots as soon as you apply power.

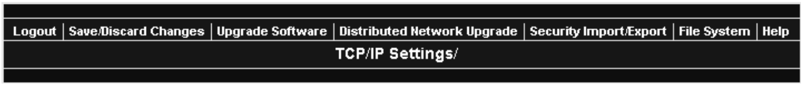
5 Immediately click Restore. The Status box lets you know when the default configuration has been restored. You will need to reconfigure your network settings.

6 To close the utility, from the File menu choose Exit.

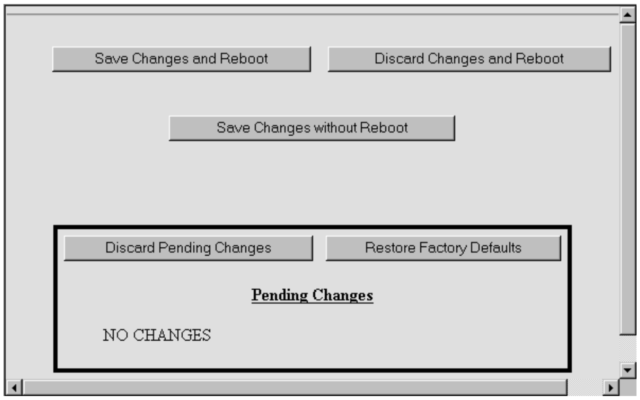
For more help using the utility, from the Help menu choose Contents.

Using the Web Browser Interface

1 In the menu bar, click Save/Discard Changes.


Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
TCP/IP Settings/

This screen appears.



Pending Changes

NO CHANGES

2 Click Restore Factory Defaults. Under Pending Changes, you will see a list of what parameters need to be changed.

3 Click Save Changes and Reboot. When the access point is done rebooting, it will use the factory default settings as its active configuration. You may need to reset the IP address and other network parameters.

Troubleshooting the Access Point

This section provides you with information on getting help with your installation and some general problems and solutions.

Getting Help With Your Installation

The access points are 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 access point firmware are you using? For help, see “Viewing the About This Access Point Screen” earlier in this chapter.

You should have the information on the About this Access Point screen available when you call Intermec Technical Support. In the U.S.A., call Intermec Technical Support at 1-800-755-5505. In Canada, call 1-800-668-7043. Outside the U.S.A. or Canada, call your local Intermec representative.

General Troubleshooting

Problem/Question	Possible Solution/Answer
Is the access point fully booted?	It takes about 30 seconds for an access point to boot. When the access point is done booting, the Power LED remains steady green, the Wired LAN #1 LED flashes green, and • if the access point is connected to the Ethernet network, the Wired LAN LED flashes green. • if there is a radio in radio slot #2, the Wired LAN #2 LED flashes green. • if the access point is configured as a root access point, the Root/Error LED remains steady green.
The Power LED is not on.	1. Make sure the power cable is firmly plugged into the access point and the power source. 2. Unplug the access point, and then plug it back into the power source. After the access point boots, verify that the Power LED remains on. 3. The access point may have a hardware problem. Call Intermec Technical Support.
The Wireless #2 LED and the Root LED are flashing at the same time.	You may only have the boot ROM code it; you have lost all the access point files. You need to use the MobileLAN access Utility to recover the access point. For help, see “Recovering a Failed Access Point” later in this chapter.
You cannot connect to the access point using the serial port.	1. Verify that you are using a null-modem cable to connect the access point to your terminal or PC. 2. Verify that you are communicating through the correct serial port. 3. Verify that your terminal or PC is set to 9600, N, 8, 1, no flow control. (Verify that the baud rate is not 115200.) 4. Your system may be in autobaud mode. Reboot and press a key once per second until the signon screen appears.
You cannot connect to the access point using a web browser.	1. Verify that you did not disable the Browser Access field in the Security screen. 2. If you access the Internet through a proxy server, be sure you have added the IP address of the access point to the Exceptions list.
You cannot ping or telnet to an access point.	1. You must set an IP address and subnet mask using the MobileLAN access Utility or a communications program before you can remotely connect to the access point. 2. Verify that you did not disable the Telnet Access field in the Security screen. 3. The access point may have lost its files. For help, see “Recovering a Failed Access Point” later in this chapter.

General Troubleshooting (continued)

Problem/Question	Possible Solution/Answer
The Ping Utility screen does not appear when you click a MAC address or an IP address in the AP Connections screen.	The web browser you are using does not have Java support. Intermec recommends that you use Internet Explorer v3.0 or later or Netscape Communicator v4.0 or later.
You cannot connect to the access point using MobileLAN manager or another SNMP management station.	Verify that you did not disable the SNMP Access field in the Security screen.
The end device cannot connect to the network.	• From the Maintenance menu, choose AP Connections and verify that the MAC address of your end device appears on your PC screen. If it does not appear, your end device is not communicating with the access point. Check your radio configuration settings. • Verify that the access point is not filtering out the type of traffic you are trying to pass through it.
The end device cannot synch to the access point.	If you are using 802.11b or 802.11a radios: • Verify that the end device and the access point have the same SSID (network name) and security. If you are using OpenAir radios: • Verify that the end device and access point have the same LAN ID, security ID, channel, and subchannel. • Verify that the access point is configured as a master and that the end device is configured as a station. If you are using 902 MHz radios: • Verify that the end device and the access point have the same LAN ID and mode-channel. If you are using S-UHF radios: • Verify that the end device and the access point have the same frequency.
The end devices are unable to roam from one access point to another.	The switches in your network may not support backward learning. Use data link tunneling to force all wireless traffic through a fixed point so that roaming is transparent to the bridges or switches. The end devices must have IP addresses from the root IP subnet. For more information, see “About Data Link Tunneling” in Chapter 5.
The end devices are unable to roam between a MobileLAN access product and 011X devices.	Set the Unicast Flood Mode to Hierarchical. For more information, see “Configuring Global Flooding” in Chapter 5.

General Troubleshooting (continued)

Problem/Question	Possible Solution/Answer
You cannot originate an IP tunnel to an access point on a remote IP subnet.	1. Verify that the IP Router (Gateway) address is correct. 2. Verify that the access points on the ends of the tunnel have the same LAN ID. 3. On the root access point verify that the IP address of the access point at the endpoint of the IP tunnel appears in the IP Addresses list.
You need to verify the static 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 access points and end devices to reset the WEP keys.
The filters are not filtering properly.	Check all of your filter settings. Conflicts may exist between the various filters.
You need to confirm which master radio a WAP is connected to.	To verify that a WAP is communicating with a particular radio, view the AP Connections screen for the access point. Click Maintenance, and then click AP Connections.
The throughput seems slow.	• Verify that your antennas are well placed and that metal or other obstacles do not block them. • You may want to add a second access point 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 network. For more information about filters, see "Configuring IP Tunnel Filters" in Chapter 5.
The radio coverage is less than you expected it to be.	Verify that the antennas or antenna cables are plugged into the correct connectors by reading the label on the access point. The connectors for the WA21 and WA22 are different than the ones for the 2100 and the 2101.

Troubleshooting the Radios

If you are having problems communicating with your wireless network, you can use the access point LEDs, a serial connection, or the access point to help you troubleshoot any radio problems.

Using LEDs

If the access point LEDs show the following pattern after it boots, the radio may be faulty or the configuration matrix string is incorrect. Contact your local Intermec representative to help you correct the problem.

Power	Wireless #1	Wireless #2	Wired LAN	Root/Error
○	●	●	○	○

○ = On ● = Off

Using a Communications Program or a Telnet Session

If you are communicating with the access point using a communications program or a telnet session, an error message may appear on your PC after the access point reboots or when a session is saved. The error messages are described in the following table. In this 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. You will need to contact your local Intermec representative to correct the problem.

Radio Error Messages

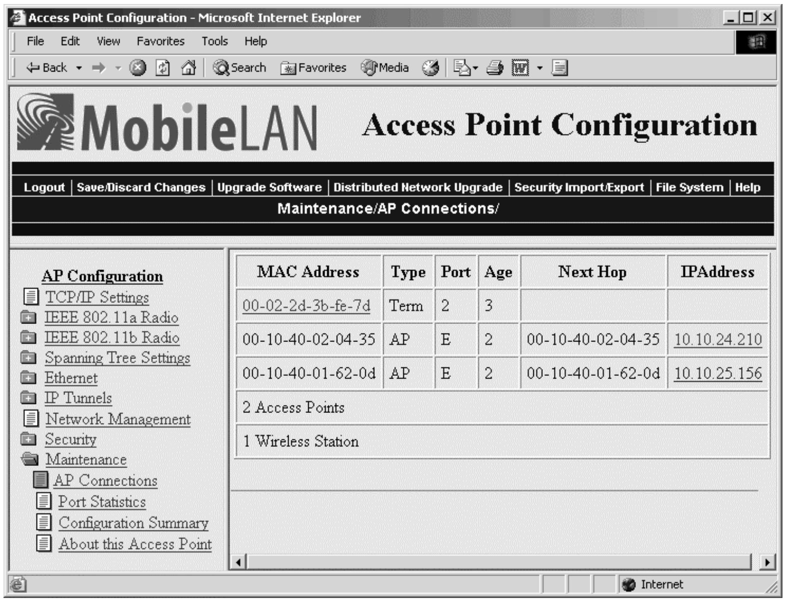
Error Message	Explanation
Couldn’t read country code from radio A	The radio may be faulty.
Invalid country code in string for radio A	The country code in the configuration matrix string does not match the country code in the radio in the access point.
Radio A has unknown country code	The radio may have been configured incorrectly at the factory.
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.

Using Radio MAC Ping (802.11b Radios)

Radio MAC Ping runs at the MAC sublayer of the Data Link layer, thus allowing you to ping any 802.11b device that is connected to the access point. Radio MAC Ping can help you determine the connectivity and signal strength of an 802.11b radio.

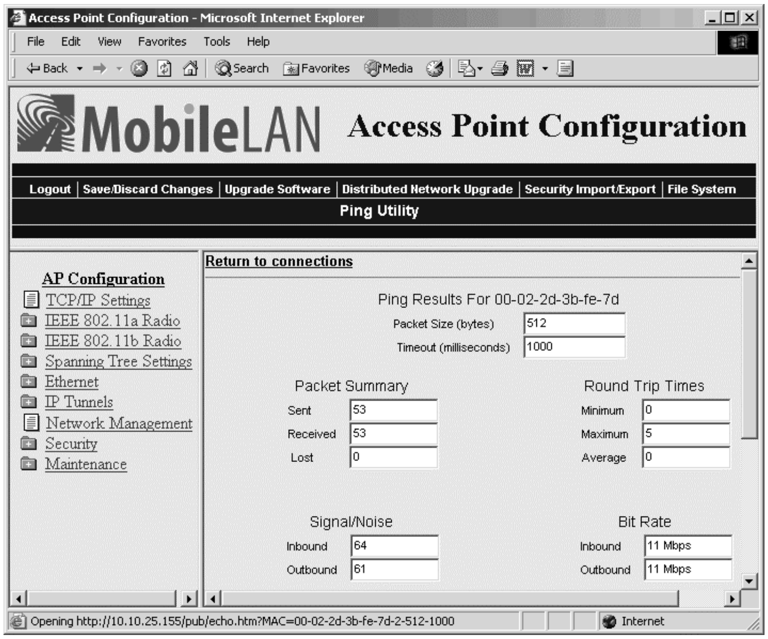
To use radio MAC ping

1 From the menu, click Maintenance, and then click AP Connections. The AP Connections screen appears. All devices that support a radio MAC ping will have their MAC address listed with a hyperlink.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Maintenance/AP Connections/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
AP Connections
Port Statistics
Configuration Summary
About this Access Point
Internet

MAC Address	Type	Port	Age	Next Hop	IPAddress
00-02-2d-3b-fe-7d	Term	2	3		
00-10-40-02-04-35	AP	E	2	00-10-40-02-04-35	10.10.24.210
00-10-40-01-62-0d	AP	E	2	00-10-40-01-62-0d	10.10.25.156
2 Access Points					
1 Wireless Station					

2 Click a MAC address hyperlink. The access point pings the device, and then the Ping Utility screen appears showing the results.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System
Ping Utility
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Return to connections
Internet

Ping Results For 00-02-2d-3b-fe-7d

Packet Size (bytes): 512

Timeout (milliseconds): 1000

Packet Summary

- Sent: 53
- Received: 53
- Lost: 0

Round Trip Times

- Minimum: 0
- Maximum: 5
- Average: 0

Signal/Noise

- Inbound: 64
- Outbound: 61

Bit Rate

- Inbound: 11 Mbps
- Outbound: 11 Mbps

Opening http://10.10.25.155/pub/echo.htm?MAC=00-02-2d-3b-fe-7d-2-512-1000

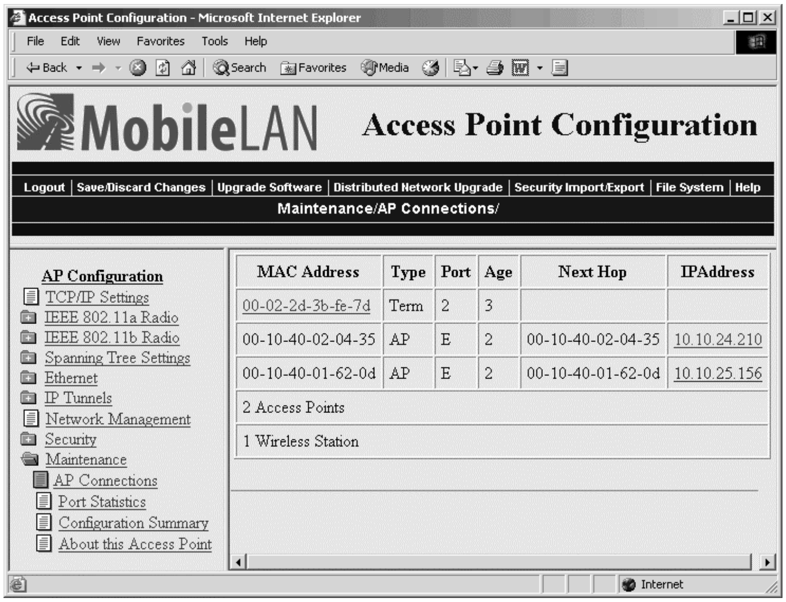
3 Click Return to connections to return to the AP Connections screen.

Using ICMP Echo

ICMP (Internet Control Message Protocol) echo lets you ping devices using their IP address. ICMP echo can only be used if the access point has determined the IP address of the end device or another access point. If the access point is acting as an ARP server, it will determine the IP addresses of the end devices that are attached to it and allow you to use ICMP echo on the wireless network. The access point always knows the IP address of all access points in the spanning tree.

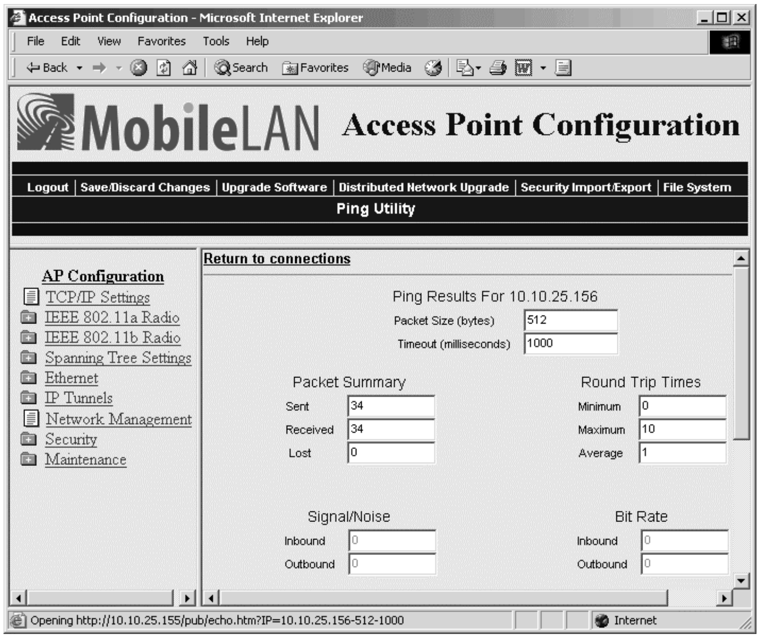
To use ICMP echo

1 From the menu, click Maintenance, and then click AP Connections. The AP Connections screen appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Maintenance/AP Connections/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
AP Connections
Port Statistics
Configuration Summary
About this Access Point
Internet

MAC Address	Type	Port	Age	Next Hop	IPAddress
00-02-2d-3b-fe-7d	Term	2	3		
00-10-40-02-04-35	AP	E	2	00-10-40-02-04-35	10.10.24.210
00-10-40-01-62-0d	AP	E	2	00-10-40-01-62-0d	10.10.25.156
2 Access Points					
1 Wireless Station					

2 Click an IP address link. The access point pings the device, and then the Ping Utility screen appears showing the results.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System
Ping Utility
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Maintenance
Return to connections
Internet

Ping Results For 10.10.25.156

Packet Size (bytes) 512

Timeout (milliseconds) 1000

Packet Summary

Sent 34

Received 34

Lost 0

Round Trip Times

Minimum 0

Maximum 10

Average 1

Signal/Noise

Inbound 0

Outbound 0

Bit Rate

Inbound 0

Outbound 0

Opening http://10.10.25.155/pub/echo.htm?IP=10.10.25.156-512-1000

3 Click Return to connections to return to the AP Connections screen.

Troubleshooting Security

This section helps you troubleshoot problems you may have while installing and configuring security in your network. For more help troubleshooting 802.1x security, refer to the documentation for the MobileLAN secure 802.1x security solution, the Odyssey server, and the end devices.

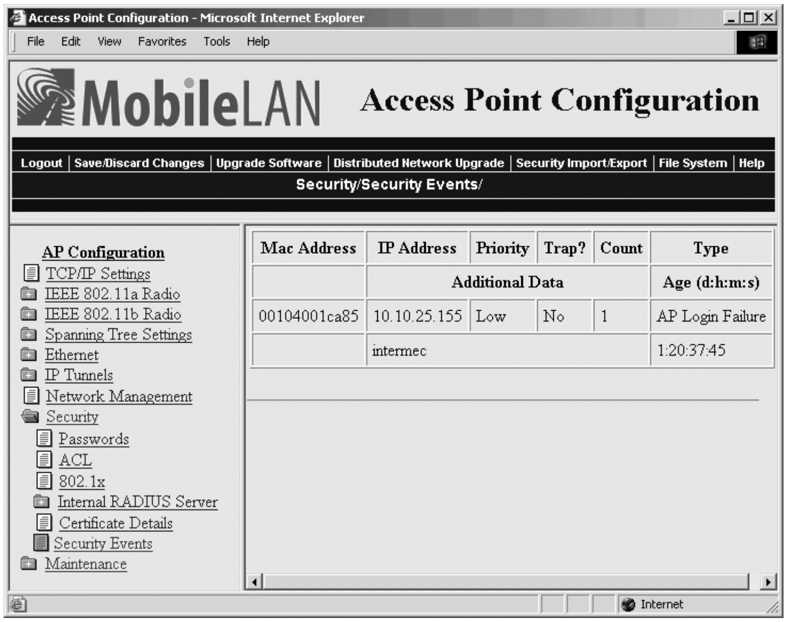
Viewing the Security Events Log

The access point logs a variety of 802.1x events in its Security Events log. Only the access point that generates the security event displays it in its Security Events log.

To see all the 802.1x events in your network, you need to use MobileLAN manager or another SNMP management station or network management tool.

To view the Security Events log

- From the menu, click Security and then click Security Events. The Security Events log appears.


Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Security/Security Events/
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Network Management
Security
Passwords
ACL
802.1x
Internal RADIUS Server
Certificate Details
Security Events
Maintenance
Internet

Mac Address	IP Address	Priority	Trap?	Count	Type
	Additional Data				Age (d:h:m:s)
00104001ca85	10.10.25.155	Low	No	1	AP Login Failure
	intermec				1:20:37:45

For help understanding the events, see the next table.

Security Events Log Description

Column	Description
MAC Address	Ethernet MAC address of the device that caused the event.
IP Address	IP address of the device that caused the event.
Priority	Priority of the event (critical, high, low, informative).
Trap	Specifies if the event generated an SNMP-reliable trap. Any event with a priority of critical or high will generate an SNMP reliable trap.
Count	Number of times the event occurred.
Type	Details of the event that occurred.
Age	Amount of time that has passed since the event occurred.

Note: If you use an SNMP management station or another network management tool, the age represents how much time has passed since the access point was booted that this event occurred.

General Security Troubleshooting

This section provides you with information on getting help with your secure network and some problems and solutions.

Problem/Question	Possible Solution/Answer
You enabled secure IAPP in your network, but the access points do not communicate with the root access point.	• The root access point is running software release 1.80 or later. All access points must also be running software release 1.80 or later. Upgrade all access points to the same software release as the root access point. • Verify that you enabled secure IAPP on all access points. • In the root access point, click Maintenance, and then click AP Connections. If any access point station radios are blocked, re-enter the IAPP secret key in all access points.
You are implementing 802.1x security and you cannot get an end device to authenticate with a RADIUS server.	• Verify that the RADIUS server IP address is correct. Re-enter the RADIUS server secret key in both the access point and the RADIUS server. • Verify that the IAPP secret key is the same in all access points. • Verify that the access point that the end device is communicating with has the 802.1x Authentication field set to authenticate the radio that is in the end device. • Verify that the root access point is running software release 1.72 or later. • Verify that your end device is configured properly for 802.1x security. For help, see the end device user's manual.

Recovering a Failed Access Point

Note: Do not use this procedure to upgrade your access point software. For upgrading instructions, see “Upgrading the Access Points” in the next section.

You should never need to use this procedure. However, if your access point is not functioning, you may need to download an entirely new file system. If the access point loses all its files except the boot ROM code, the Wireless #2 LED and the Root LED are flashing at the same time. You will not be able to ping the access point and you cannot establish a telnet session to the access point.

You can recover a failed access point using

- the MobileLAN access Utility. For more information, see the next section “Using the MobileLAN access Utility.”
- a Windows NT 4.0/2000/XP PC

Using the MobileLAN access Utility

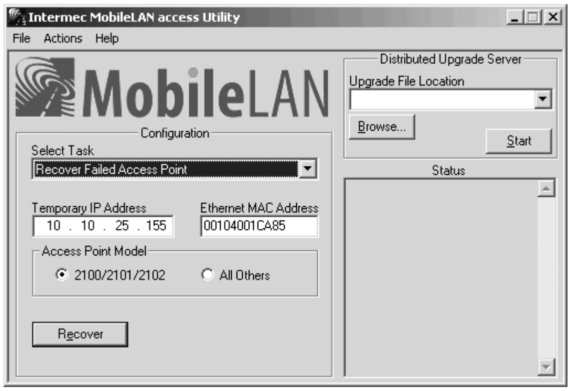
The MobileLAN access Utility enables your PC to recover an access point that is not functioning. For help installing the MobileLAN access utility, see “Using the MobileLAN access Utility” in Chapter 1.

To recover a failed access point

1 Download the upgrade software to your PC.

2 Start the utility.

3 Click the down arrow on the right side of the Select Task field and choose Recover Failed Access Point.



Select Task: Recover Failed Access Point

Temporary IP Address: 10 . 10 . 25 . 155

Ethernet MAC Address: 00104001CA85

Access Point Model: ● 2100/2101/2102 ○ All Others

4 In the Temporary IP Address field, enter a temporary IP address for the access point you need to recover. You can use any IP address that is valid on your network.

5 In the Ethernet MAC Address field, enter the MAC address of the access point you need to recover. This MAC address is printed on a label that is on the bottom of the access point.

Note: If you are only recovering one access point, you can enter 00:10:40:FF:FF:FF. This special MAC address works with all access points.

6 In the Access Point Model box, choose the model of the access point you are recovering.

7 In the Upgrade File Location field, enter the pathname and filename of the upgrade software. The upgrade software must be a .BIN file.

8 Click Start.

9 Disconnect and reconnect the power cable (or Ethernet cable, if you are using power over Ethernet) to the access point. The access point has no On/Off switch, so it boots as soon as you apply power.

10 Click Recover. The Status box lets you know when the access point is successfully recovered.

You will need to reconfigure the access point.

Using a Windows NT 4.0/2000/XP PC

If you do not have the MobileLAN access Utility, you can use a Windows NT 4.0/2000/XP PC and a command prompt to recover a failed access point. To access a command prompt, see your Windows documentation. For this procedure you will need to contact Intermec Technical Support to obtain the appropriate .DNL file.

MobileLAN access DNL File

Access Point	Upgrade File
WA22, WA21, 2106	AP824X.DNL
2100D, 2101B	AP855.DNL
2100A, 2100B, 2100C, 2101A, 2102	UAP.DNL

To recover a failed access point

1 From a command prompt, type this command to create a static ARP cache entry for the netloader.

```
arp -s x.x.x.x yy-yy-yy-yy-yy-yy
```

where:

x.x.x.x is the IP address that you want to assign the access point

yy-yy-yy-yy-yy-yy is the MAC address of the access point. This MAC address is printed on a label that is on the bottom of the access point.

Note: If you are only recovering one access point, you can enter 00:10:40:FF:FF:FF. This special MAC address works with all access points.

2 Type this command to continuously ping the access point while you boot the access point.

```
ping –t –l 100 IPaddress
```

where *IPaddress* is the access point IP address you assigned in Step 1.

3 Disconnect and reconnect the power cable (or Ethernet cable, if you are using power over Ethernet) to the access point. The access point has no On/Off switch, so it boots as soon as you apply power.

4 When the access point responds to the ping, use any TFTP client to transfer the appropriate .DNL file to the access point. Make sure the Transfer mode is binary.

```
tftp –i IPaddress put filename.dnl
```

where:

IPaddress	is the access point IP address you assigned in Step 1.
filename	is the name of the appropriate .DNL file.

Once the TFTP transfer is complete, the access point will begin booting the image that was just passed to it. This image is only resident in RAM. If you reboot the access point or if the access point loses power, the .DNL image will be lost.

5 Type this command to remove the static ARP cache entry from your PC.

```
arp –d IPaddress
```

where *IPaddress* is the access point IP address you assigned in Step 1.

When the access point is done booting, all access point services are available. You can now telnet to the access point to upgrade it with a permanent image and configure it.

Note: You may be unable to access the web browser interface if the support files for this interface still need to be recovered. If so, use telnet to upgrade the access point, and then use the web browser interface to configure it.

Upgrading the Access Points

Note: If the access point that you are upgrading is running a software release earlier than 1.50, first upgrade it to 1.50. Then, use the MobileLAN access Utility or the web browser interface to upgrade it to the desired software release.

For optimal performance, you should install the most current software version on all the access points in your network. To upgrade the software, you must copy the software release to your PC, and then you can upload the release to your root access point and other access points. However, you can also configure the root access point to copy the release to all other access points in its spanning tree.

You can upgrade the access point software using

- the MobileLAN access Utility as a distributed upgrade server. For help, see the next section “Using the MobileLAN access Utility” and the online help.
- a web browser interface. For help, see “Using a Web Browser Interface” later in this section.

To copy the software release to your PC

1. Using a web browser, navigate to www.intermec.com.
2. From the Support menu, choose Software Downloads.
3. Click MobileLAN and then click access Software.
4. Click the software link to save the upgrade file on your PC.

Using the MobileLAN access Utility

The MobileLAN access Utility enables your PC to act as a distributed upgrade server. That is, the PC stores the upgrade software and you configure the root access point to retrieve the software at a specified time. You can also configure the root access point to inform other access points in its spanning tree where they can get the software so they can be upgraded.

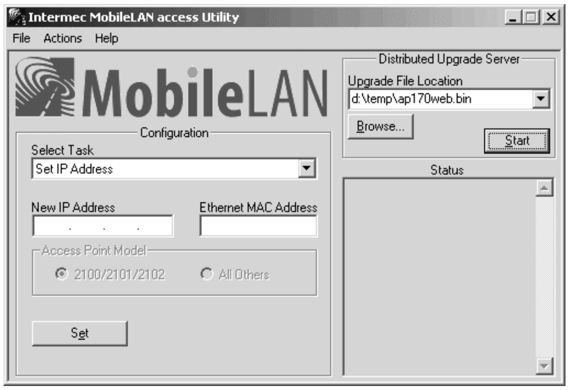
If you use this utility, you only need to configure the root access point and all access points will be upgraded. However, when the access points request the upgrade software, the utility must be active.

Note: The PC that is running the MobileLAN access Utility does not need to be on the same IP subnet as the access points.

To upgrade the access point software

1 Start the utility.

2 In the Upgrade File Location field, enter the path and filename of the upgrade file (AP*WEB.BIN) or click Browse to find the file. For example, AP180WEB.BIN.



Upgrade File Location: d:\temp\ap170web.bin

Select Task: Set IP Address

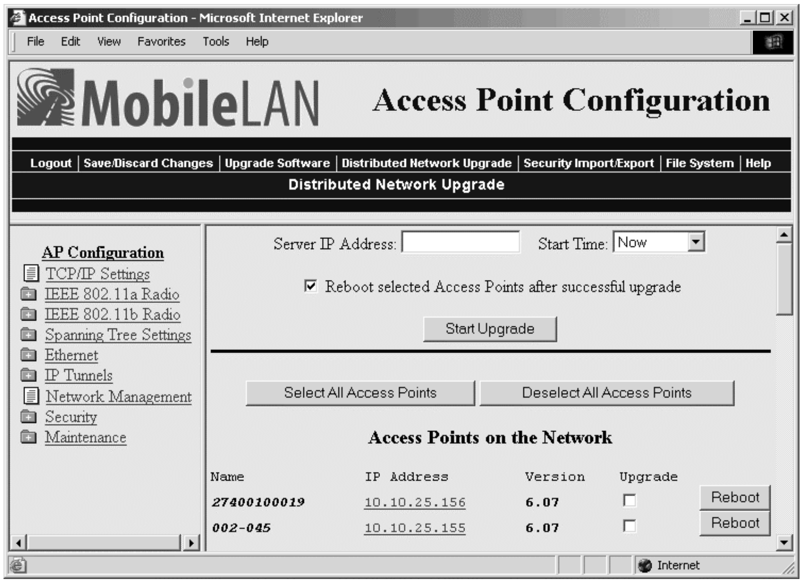
Access Point Model: ● 2100/2101/2102 ○ All Others

3 Click Start. The utility must remain active until the upgrade procedure is complete; do not close the utility.

4 Configure the root access point to retrieve the software.

a From the Actions menu, click Configure Access Point, and then enter the IP address of the root access point. A web browser session is established.

b From the menu bar, click Distributed Network Upgrade. The Distributed Network Upgrade screen appears.



Server IP Address: Start Time: Now

☑ Reboot selected Access Points after successful upgrade

Access Points on the Network

Name	IP Address	Version	Upgrade	
27400100019	10.10.25.156	6.07	□	Reboot
002-045	10.10.25.155	6.07	□	Reboot

c In the Server IP Address field, enter the IP address of the PC contains the software release and that is running the utility.

d Click the down arrow on the right side of the Start Time field and choose when you want the upgrade to start.

e Check the Reboot selected Access Points after successful upgrade check box if you want to access points to run the upgraded software after it is downloaded.

If clear this check box, you will need to reboot the access points when you want them to run the upgraded software.

5 Configure the root access point to tell the other access points where to get the upgrade software.

a Under the Access Points on the Network title, you can see a list of all the access points in the spanning tree.

b Check the Upgrade check box of all access points you want to upgrade.

To select all access points that are listed, click the Select All Access Points button.

To deselect all access points that are selected, click the Deselect All Access Points button.

When the start time expires, the root access point retrieves the upgrade software and reboots. When it is done rebooting, it will be running the new software. The other access points that you configured to be upgraded will also retrieve the upgrade software. If you checked the Reboot selected Access Points after successful upgrade check box, they will also reboot, and then they will be running the new software.

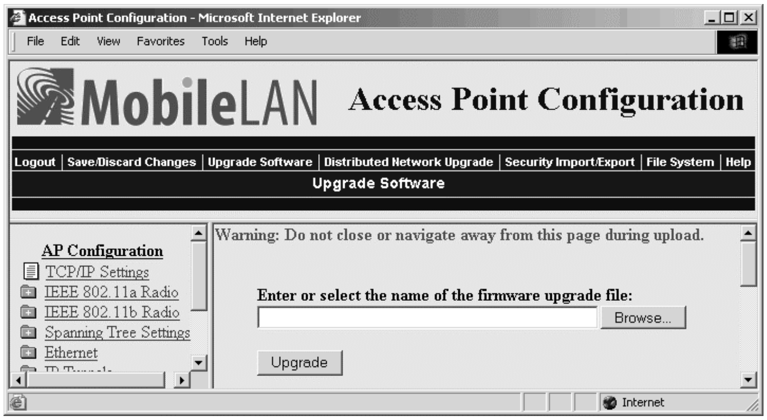
Using a Web Browser Interface

You can use a web browser interface to upgrade the access points one at a time. In other words, for each access point you want to upgrade, you will need to establish a web browser session with it, upgrade its software, save the new configuration, and reboot it.

To upgrade the access point software

1 Establish a web browser session with the access point you want to upgrade.

2 From the menu bar, click Upgrade Software. The Upgrade Software screen appears.



Access Point Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
MobileLAN
Access Point Configuration
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | Security Import/Export | File System | Help
Upgrade Software
AP Configuration
TCP/IP Settings
IEEE 802.11a Radio
IEEE 802.11b Radio
Spanning Tree Settings
Ethernet
Browse...
Upgrade
Internet

Warning: Do not close or navigate away from this page during upload.

Enter or select the name of the firmware upgrade file:

3 Enter the path and filename of the upgrade file (AP*WEB.BIN) or click Browse to find the file on your PC. For example, AP180WEB.BIN.

4 Click Upgrade to start the upgrade. The upgrade may take up to three minutes to complete.

5 When the upgrade is complete, click Save Changes and Reboot.

When the access point is done rebooting, it is upgraded to the new software. Repeat this procedure for each access point you want to upgrade.

Troubleshooting the Upgrade

Each access point on a wired LAN requires approximately three minutes to upgrade (it takes slightly longer for wireless access points). The web browser screen updates every 30 seconds as the upgrade progresses and shows the final status when all upgrades are complete. If you checked the Reboot selected Access Points after successful upgrade check box, the web browser disconnects. Click the Refresh button to log in again.

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

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

1 Recheck the access points where the error occurred.

2 Click Start Upgrade to attempt the upgrade again. If the upgrade is successful and you checked the Reboot selected Access Points after successful upgrade check box, the access points will reboot.

If an error occurs during the final reboot, you should

1 Wait five minutes for the access points that did not reboot to refresh.

2 Refresh your web 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 and you checked the Reboot selected Access Points after successful upgrade check box, the access points will reboot according to your Reboot selection.

If you need to downgrade an access point to an earlier release, contact Intermec Technical Support.

9 Additional Access Point Features

This chapter explains some of the more advanced ways that you can maintain the MobileLAN access products. This chapter covers these topics:

- Understanding the Access Point Segments
- Using the AP Monitor
- Using Console Command mode
- Creating script files

Understanding the Access Point Segments

The 2101, 2100, and 2102 have these four segments in their 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)

You can enter commands to manipulate the boot and data segments. For instance, you typically download new access point software into an inactive segment, and then make that segment active the next time the access point boots.

The WA22, WA21, and 2106 have only one segment.

Using the AP Monitor

The AP (access point ROM) monitor is system software that lets you manipulate the access point files and file segments. You can only access the AP monitor through the serial port using a communications program. Therefore, you cannot use this feature with the 2106.

Note: Certain functions available through the AP monitor can erase the access point configuration. Intermec strongly recommends that you only use the AP monitor when absolutely necessary. For example, you might use the AP monitor to upgrade the access point software or when instructed to do so by Intermec Technical Support.

Entering the AP Monitor

1. Use a communications program to start a session with the access point.
2. Reboot the access point.
3. When you see the message <Press any key within 5 seconds to enter the AP monitor> during the boot process, press Enter.

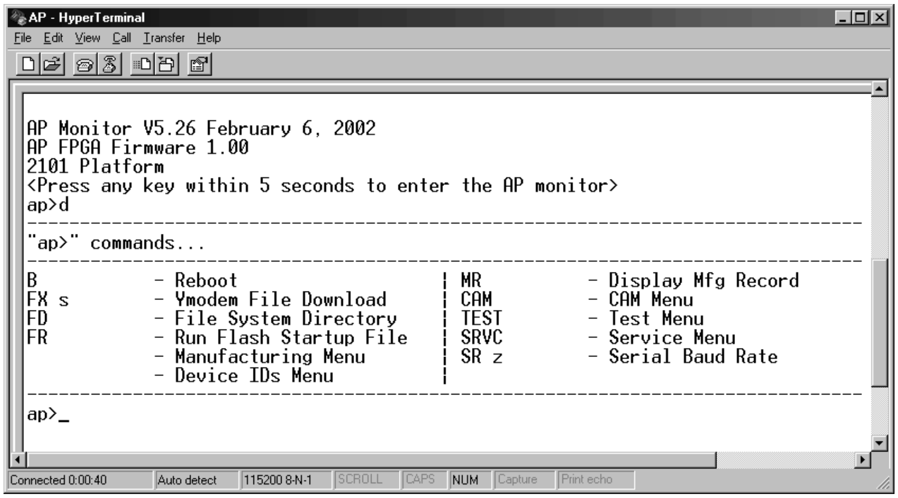
The ap prompt (ap>) appears.

Using AP Monitor Commands

You can display a list of AP monitor commands on the screen anytime you see the ap prompt.

To list AP monitor commands

- Press any key (except the letter B, which reboots the access point), and then press **Enter**. A list of AP monitor commands appears.



```
AP Monitor V5.26 February 6, 2002
AP FPGA Firmware 1.00
2101 Platform
<Press any key within 5 seconds to enter the AP monitor>
ap>d
-------------------------------------------------------------------------------
"ap>" commands...
-------------------------------------------------------------------------------
B           - Reboot                   | MR          - Display Mfg Record
FX s        - Ymodem File Download     | CAM         - CAM Menu
FD          - File System Directory    | TEST        - Test Menu
FR          - Run Flash Startup File   | SRVC        - Service Menu
            - Manufacturing Menu       | SR z        - Serial Baud Rate
            - Device IDs Menu          |
-------------------------------------------------------------------------------
ap>_
```

B

Purpose: Reboots the access point.

Syntax: `B`

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 access point boot segment and tries to run it; therefore, the first executable file in the access point boot segment must be the boot file.

Syntax: `FR`

FX

Purpose: Downloads a file using Ymodem batch protocol into the flash segment that is specified by *s*.

Syntax: `FX s`

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

MR

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

Syntax: `MR`

SR

Purpose: Sets the baud rate of the access point.

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`.

You can also set the baud rate to autobaud, which lets the access point set its baud rate to match the baud rate of your terminal. Type `SR 0` and press Enter twice.

Using Content Addressable Memory (CAM) Mode Commands

You may need to use CAM commands to perform certain functions. Since the Ethernet port on the access points (except the 2102) supports data rates significantly higher than the radio ports, all frames cannot be forwarded form the Ethernet network to the radios. CAM, which is controlled by the Field Programmable Gate Array (FPGA), filters frames based on the radio's capability.

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.

To enter CAM mode

1. Type `CAM` and press Enter.
2. Enter a password. The default password is `EV98203C` (case sensitive).

When you are in CAM mode, the CAM prompt (CAM>) appears.

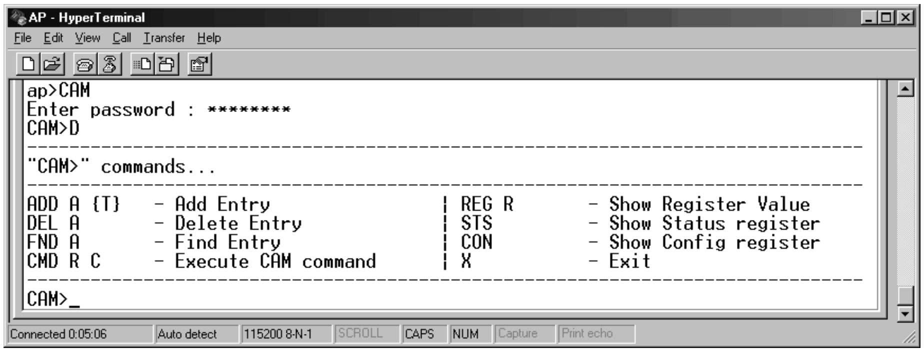
To exit CAM mode

- At the test prompt, type X and press **Enter**.

You return the ap prompt.

To display CAM commands

- Type any letter or number other than B and press **Enter**. The CAM commands appear on the screen.



```
ap>CAM
Enter password : ********
CAM>D
-------------------------------------------------------------------------------
"CAM>" commands...
-------------------------------------------------------------------------------
ADD A {T}   - Add Entry              | REG R      - Show Register Value
DEL A       - Delete Entry           | STS        - Show Status register
FND A       - Find Entry             | CON        - Show Config register
CMD R C     - Execute CAM command    | X          - Exit
-------------------------------------------------------------------------------
CAM>_
```

Using Test Mode Commands

Within the AP monitor, Test mode lets you 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.

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.

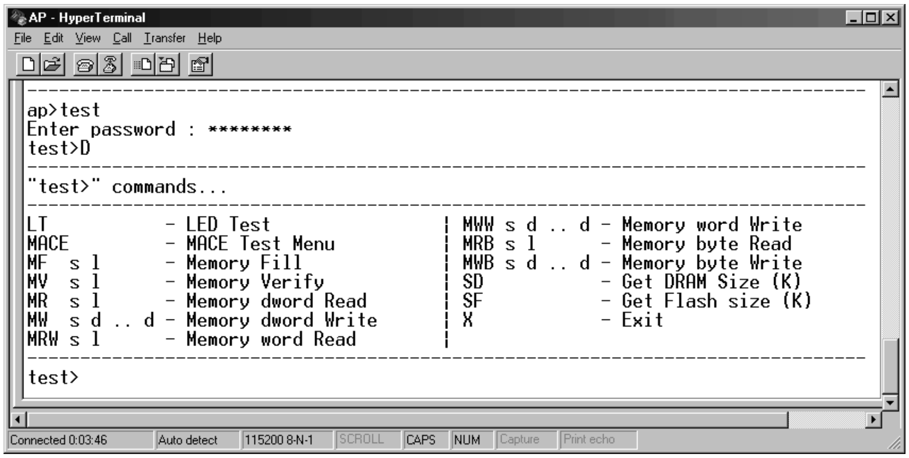
To exit Test mode

- At the test prompt, type X and press **Enter**.

You return the ap prompt.

To display test commands

- Type any letter or number other than B and press **Enter**. The test commands appear on the screen.



```
-----------------------------------------------------------------------------
ap>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 l      - 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 Service Mode Commands

In Service mode, you can perform file functions and segment functions such as deleting a file, downloading a file using the Ymodem protocol, and erasing a segment.

To enter Service mode

1. At the ap prompt, type `SRVC` and press **Enter**.
2. Enter the service password. The default password is `EV98203S` (case sensitive).

The service prompt (service>) appears.

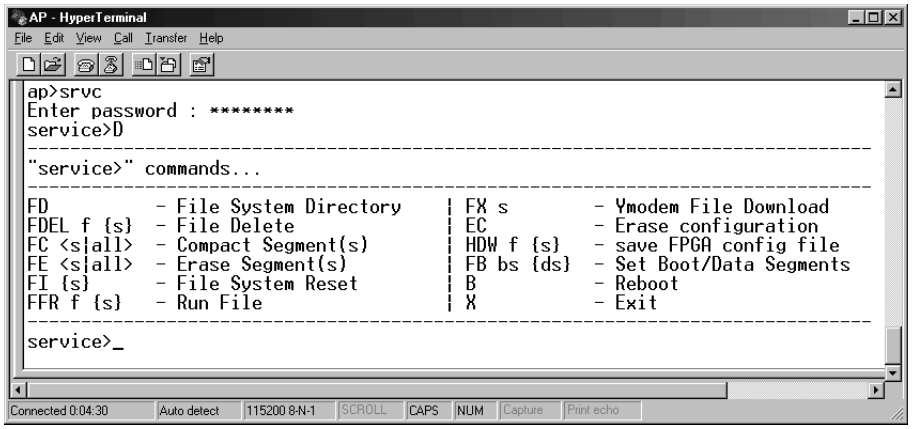
To exit Service mode

- At the service prompt, type `X` and press **Enter**.

You return the ap prompt.

To list service commands

- Press any key (except the letter B, which reboots the access point), and then press **Enter**. The service commands appear on the screen.



```
ap>srvc
Enter password : ********
service>D
--------------------------------------------------------------------------------
"service>" commands...
--------------------------------------------------------------------------------
FD            - File System Directory    | FX s         - Ymodem File Download
FDEL f {s}    - File Delete              | EC           - Erase configuration
FC <s|all>    - Compact Segment(s)       | HDW f {s}    - save FPGA config file
FE <s|all>    - Erase Segment(s)         | FB bs {ds}   - Set Boot/Data Segments
FI {s}        - File System Reset        | B            - Reboot
FFR f {s}     - Run File                 | X            - Exit
--------------------------------------------------------------------------------
service>_
```

Many of the commands that are available in Service mode are also available in the AP monitor or Console Command mode.

B

Purpose: Reboots the access point.

Syntax: `B`

FB

Purpose: Makes an inactive segment the active segment.

Syntax: `FB` *`bootsegment (datasegment)`*

where:

bootsegment is the name or number of the boot segment to be activated.

datasegment is the optional 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 access point a common task is to activate the new software. To activate the new software, enter:

```
FB IB: ID:
```

FB (continued)

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.

FC

Purpose: Compacts the files in a particular segment.

Syntax:

```
FC s
```

where *s* is the name or number of the segment to be compacted. You can enter `ALL` instead of a segment name or number if you want to erase all segments.

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

```
FC 1
```

To compact the contents of the inactive boot segment, enter:

```
FC IB:
```

FD

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

Syntax:

```
FD
```

FDEL

Purpose: Deletes a particular file from a segment.

Syntax:

```
FDEL f (s)
```

where:

f is the name of the file to be deleted.

s is the optional segment location of the file.

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.

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

Syntax: `FE s`

where *s* is the name or number of the segment to be erased. You can enter `ALL` instead of a segment name or number if you want to erase all segments.

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

```
FE 1
```

To erase the contents of the inactive boot segment, enter:

```
FE IB:
```

FFR

Purpose: Runs a program *`f`*`,` from a location *`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
```

FI

Purpose: Reinitializes the access point file system. If the access point file system or a file segment becomes corrupt, use this command to reset it.

Syntax: `FI (s)`

where *s* is the optional number of the segment to be reinitialized.

FX

Purpose: Downloads a file using Ymodem batch protocol into the flash segment that is specified by *`s`*.

Syntax: `FX s`

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

HDW

Purpose: Loads the FPGA configuration file into the access point. If you are directed to change the FPGA firmware in the access point, use this command.

Syntax: `HDW f (s)`

where:

f is the FPGA configuration filename.

s is the optional segment where you want to load the configuration file.

Using Command Console Mode

You can use the Command Console mode to manipulate some access point files and file segments. You can also use Command Console mode to upgrade access points using TFTP and script files.

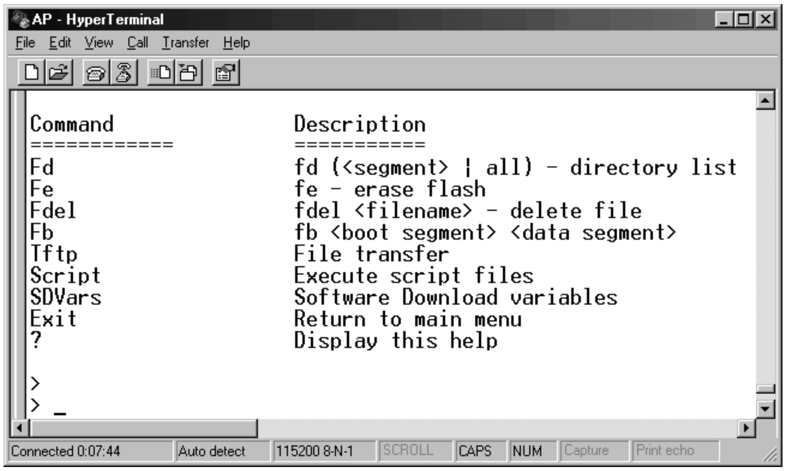
You access the Command Console mode through the serial port using a communications program or over the network using a telnet session. You cannot access Command Console mode using a web browser interface.

Entering Command Console Mode

1 Use a communications program or telnet to start a session with the access point. For help, see “Using a Communications Program” in Chapter 1.

2 From the Access Point Configuration menu, choose Maintenance.

3 From the Maintenance menu, choose Command Console. The list of commands appears.



```
Command                Description
============           ===========
Fd                     fd (<segment> | all) - directory list
Fe                     fe - erase flash
Fdel                   fdel <filename> - delete file
Fb                     fb <boot segment> <data segment>
Tftp                   File transfer
Script                 Execute script files
SDVars                 Software Download variables
Exit                   Return to main menu
?                      Display this help

>
> _
```

To exit Command Console mode

- At the prompt, type `exit`.

You return to the Maintenance menu.

Using the Commands

Several of these commands require that you enter filenames. To indicate the segment where the file is located, precede the filename 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 access point searches the segments in the following order until it finds a file that matches the file name RAM, 1, 2, 3, 4.

FB

Purpose: Makes an inactive segment the active segment.

Syntax:

```
FB bootsegment datasegment
```

where:

bootsegment is the name or number of the boot segment to be activated.

datasegment 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 access point 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: Displays the flash file system directory, which includes information about the boot file. Use this command to ensure that the correct version of the file is in the active boot segment.

Syntax:

```
FD
```

Example: To show only the files loaded in the active boot segment., enter:

```
FD ab:
```

Note: If the active segment contains no files when you reboot the access point, the access point enters the AP monitor and you will no longer be able to telnet to it during this session. If this occurs, you must access the access point through its serial port to correct the problem.

FDEL

Purpose: Deletes a particular file from a segment.

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.

Syntax:

```
FDEL f
```

where *f* 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
```

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.

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

Syntax:

```
FE s
```

where *s* is the name or number of the segment to be erased. You can enter `ALL` instead of a segment name or number if you want to erase segments 1 through 4.

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

```
FE 1
```

To erase the contents of the inactive boot segment, enter:

```
FE IB:
```

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 f`

where *f* is the name of the script file to be executed.

For more information about using the script command, see "Creating Script Files" later in this chapter.

Using TFTP Commands

TFTP commands are file transfer commands. An access point can act as either a client or server in the TFTP environment. As a server, the access point can service read and write requests from an access point client. As a client, the access point 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 access point retries TFTP client commands get and put until the command is successfully completed. If the first attempt fails, the access point 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 access point backoff algorithm should prevent excessive network traffic when many access points are trying to contact a TFTP server.

TFTP GET

Purpose: TFTP client requests a file from the TFTP server.

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.

TFTP GET (continued)

Syntax: `TFTP GET IPaddress foreignfilename localfilename`

where:

IPaddress is the IP address of the server. You can use an asterisk (*) here if you want to use the value in serveripaddress.

foreignfilename 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 access point.

localfilename is the name you wish to call the file on the access point. 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.

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 access point.

```
TFTP GET 1.2.3.4 C:\STARTUP\UAP.DNL IB:
```

The access point may generate these error messages when it issues a TFTP GET command. Other error messages may be returned from the server and displayed by the access point. 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 access point 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 TFTP client to the TFTP server or to another access point.

Syntax:

```
TFTP PUT IPaddress foreignfilename localfilename
```

where:

IPaddress	is the IP address of the server. You can use an asterisk (*) here if you want to use the value in the serveripaddress.
foreignfilename	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.
localfilename	is the name of the file to be sent from the access point.

Example: The following command takes file UAP.PRG that is saved in the active boot drive on the access point client and stores it in the inactive boot segment on the access point server that has IP address 1.2.3.4.

```
TFTP PUT 1.2.3.4 IB:UAP.PRG AB:UAP.PRG
```

The access point may generate these error messages when it issues a TFTP PUT command. Other error messages may be returned from the server and displayed by the access point. See your server documentation for additional information.

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: The access point can function as a TFTP server. You can use the TFTP server log command to save a history of TFTP client requests. The TFTP server log contains useful TFTP server status information. The log begins when you set up the server. To clear the log, reboot the access point.

Syntax:

```
TFTP SERVER LOG
```

TFTP SERVER START

Purpose: Use this command to enable the access point to act as a server. You can enable one access point to act as a TFTP server and download files to additional access points.

Syntax: `TFTP SERVER START`

After you issue this command, the access point responds to TFTP client requests that are directed to its IP address. When acting as a server, the access point supports up to four concurrent TFTP sessions.

TFTP SERVER STOP

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

Syntax: `TFTP SERVER STOP`

After you issue this command, the access point no longer responds to TFTP client requests; however, current TFTP sessions with the server are allowed to complete. This 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 access point 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 access point file header, or the file name may be incorrectly formed.
Can’t read remote file	The server returns this message if the access point 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 access point 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.

Using sdvars Commands

Use sdvars commands 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.

This section describes the sdvars commands 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.

Syntax:

```
sdvars set serveripaddress ipaddress
```

where *ipaddress* is the address of the TFTP 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 foreignfilename
```

where *foreignfilename* 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; that is, when zero is reached, the software download process begins. Set this variable to reflect how far into the future the access point is to begin downloading and executing the script file from the TFTP server. When the timer reaches 0, the access point 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 reboot is to begin and

dd	is days.
hh	is hours.
mm	is minutes.
ss	is seconds.

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 access point 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 access point. If either starttime or nextpoweruptime is counting down, setting this variable stops the timer and halts the countdown process.

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 access point in an undetermined state that may require user intervention.

Syntax:

```
sdvars set terminate
```

sdvars set setactivepointers

Purpose: Sets the setactivepointers command to change inactive segments to active segments the next time the access point 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 access point 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 access point will reboot. When the nextpoweruptime counter reaches 0, the access point checks the value of the setactivepointers variable, takes the appropriate action, and then reboots.

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.

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

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

dd is days.

hh is hours.

mm is minutes.

ss is seconds.

Example: To reboot the access point 2 hours from now, enter:

```
sdvars set nextpoweruptime 00:02:00:00
```

Creating Script Files

You can create a script file that will execute a series of commands. For example, when you upgrade the access point, 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.

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.

Follow these rules when creating script files:

- The total file size including the header must be less than 4096 bytes, which is the size of the RAM file segment.
- Each line in the script file must have fewer than 80 characters
- Each line in the script file must be terminated by a line feed or carriage return.
- You can only have one command per line.
- You can include comments on a line by using the pound (#) sign; all characters after a pound sign are ignored.

To test a script file, log onto an access point and type each of the script file commands.

```
#Sample script file for upgrading an access point
#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 and Default Settings

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.

Specifications

WA22

Height	4.6 cm (1.8 in)
Length	25.0 cm (9.8 in)
Width	15.9 cm (6.3 in)
Weight	526 g (1.16 lb)
Power over Ethernet electrical rating	⎓ 48V, 315 mA
Operating temperature	-20°C to +55°C (-4°F to +131°F)
Storage temperature	-40°C to +70°C (-40°F to +158°F)
Humidity (non-condensing)	10 to 90%
Architecture	Transparent bridge
Ethernet interfaces	10BaseT/100BaseTx (twisted-pair)
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Ethernet data rate	10 Mbps/100 Mbps (Ethernet) 100 Mbps (Fiber optic)
Fiber optic interface (optional)	MT-RJ
Radios supported	IEEE 802.11b, IEEE 802.11a
Media Access protocol	CSMA/CD
Filters (protocol)	IP, IPX, NetBEUI, DECNET, AppleTalk
Filters (others)	IP, ARP, Novell RIP, SAP, LSP
Serial port maximum data rate	115,200 bps
Management interfaces	Web browser-based manager, text-based menu system, serial port, Telnet, SNMP
Software upgrades	Downloadable over the network or serial port
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x, Enterprise MobileLAN access

2101

Height	3.8 cm (1.5 in)
Length	25.0 cm (9.8 in)
Width	15.9 cm (6.3 in)
Weight	526 g (1.16 lb)
AC electrical rating	~100 to 240V, 1.0A, 50 to 60 Hz
Power over Ethernet electrical rating	⎓ 48V, 315 mA
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%
Architecture	Transparent bridge
Ethernet interfaces	10BaseT/100BaseTx (twisted-pair)
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Ethernet data rate	10 Mbps/100 Mbps (Ethernet) 100 Mbps (Fiber optic)
Fiber optic interface (optional)	MT-RJ
Radios supported	IEEE 802.11b, WLI-Forum OpenAir
Media Access protocol	CSMA/CD
Filters (protocol)	IP, IPX, NetBEUI, DECNET, AppleTalk
Filters (others)	IP, ARP, Novell RIP, SAP, LSP
Serial port maximum data rate	115,200 bps
Management interfaces	Web browser-based manager, text-based menu system, serial port, Telnet, SNMP
Software upgrades	Downloadable over the network or serial port
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x, Enterprise MobileLAN access

WA21

Height	9.5 cm (3.8 in)
Length	35.5 cm (14.0 in)
Width	23.6 cm (9.3 in)
Weight	2.63 kg (5.8 lb)
AC electrical rating Standard Heater (optional)	 ~100 to 240V, 1.0 to 0.5A, 50 to 60 Hz ~100 to 120V, 1.0A, 50 to 60 Hz or ~200 to 240V, 0.5A, 50 to 60 Hz
Power over Ethernet electrical rating	⎓ 48V, 315 mA
Operating temperature	
Standard	-25°C to +70°C (-13°F to +158°F)
Heater (optional), AC only	-30°C to +70°C (-22°F to +158°F)
Heater/insulated bag (optional), AC only	-30°C to 0°C (-22°F to +32°F)
Storage temperature	-40°C to +70°C (-40°F to +158°F)
Humidity (non-condensing)	10 to 90%
Industrial sealing	IP 54 (NEMA 4)
Architecture	Transparent bridge
Ethernet interfaces	10BaseT/100BaseTx (twisted-pair)
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Ethernet data rate	10 Mbps/100 Mbps (Ethernet) 100 Mbps (Fiber optic)
Fiber optic interface (optional)	MT-RJ
Radios supported	IEEE 802.11b, IEEE 802.11a
Media Access protocol	CSMA/CD
Filters (protocol)	IP, IPX, NetBEUI, DECNET, AppleTalk
Filters (others)	IP, ARP, Novell RIP, SAP, LSP
Serial port maximum data rate	115,200 bps
Management interfaces	Web browser-based manager, text-based menu system, serial port, Telnet, SNMP
Software upgrades	Downloadable over the network or serial port
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x, Enterprise MobileLAN access

2100

Height	9.5 cm (3.8 in)
Length	35.5 cm (14.0 in)
Width	23.6 cm (9.3 in)
Weight	2.63 kg (5.8 lb)
AC electrical rating	
Standard	~100 to 240V, 1.0 to 0.5A, 50 to 60 Hz
Heater (optional)	~100 to 120V, 1.0A, 50 to 60 Hz or ~200 to 240V, 0.5A, 50 to 60 Hz
Power over Ethernet electrical rating	⎓ 48V, 315 mA
Operating temperature	
Standard	-25°C to +70°C (-13°F to +158°F)
Heater (optional), AC only	-30°C to +70°C (-22°F to +158°F)
Heater/insulated bag (optional), AC only	-30°C to 0°C (-22°F to +32°F)
Storage temperature	-40°C to +70°C (-40°F to +158°F)
Humidity (non-condensing)	10 to 90%
Industrial sealing	IP 54 (NEMA 4)
Architecture	Transparent bridge
Ethernet interfaces	10BaseT/100BaseTx (twisted-pair)
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Ethernet data rate	10 Mbps/100 Mbps (Ethernet) 100 Mbps (Fiber optic)
Fiber optic interface (optional)	MT-RJ
Radios supported	IEEE 802.11b, WLI-Forum OpenAir, 902 MHz, S-UHF
Media Access protocol	CSMA/CD
Filters (protocol)	IP, IPX, NetBEUI, DECNET, AppleTalk
Filters (others)	IP, ARP, Novell RIP, SAP, LSP
Serial port maximum data rate	115,200 bps
Management interfaces	Web browser-based manager, text-based menu system, serial port, Telnet, SNMP
Software upgrades	Downloadable over the network or serial port
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x, Enterprise MobileLAN access

2102

Height	9.3 cm (3.7 in)
Length	14.7 cm (5.8 in)
Width	3.5 cm (1.4 in)
Weight	232 g (0.5 lb)
Electrical	~100 to 240V, 1.0A, 50 to 60 Hz
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%
Architecture	Transparent bridge
Ethernet interfaces	10BaseT (twisted-pair)
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Ethernet data rate	10 Mbps (Ethernet)
Radios supported	IEEE 802.11b, WLI-Forum OpenAir
Media Access protocol	CSMA/CD
Filters (protocol)	IP, IPX, NetBEUI, DECNET, AppleTalk
Filters (others)	IP, ARP, Novell RIP, SAP, LSP
Serial port maximum data rate	115,200 bps
Management interfaces	Web browser-based manager, text-based menu system, serial port, Telnet, SNMP
Software upgrades	Downloadable over the network or serial port
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x, Enterprise MobileLAN access

2106

Height	9.3 cm (3.7 in)
Length	14.7 cm (5.8 in)
Width	3.5 cm (1.4 in)
Weight	232 g (0.5 lb)
Electrical	~100 to 240V, 1.0A, 50 to 60 Hz
Operating temperature	0°C to +45°C (32°F to +113°F)
Storage temperature	-20°C to +70°C (-4°F to +158°F)
Humidity (non-condensing)	10 to 90%
Architecture	Transparent bridge
Ethernet interfaces	10BaseT/100BaseTx (twisted-pair)
Ethernet data rate	100 Mbps
Radios supported	IEEE 802.11a
Media Access protocol	CSMA/CD
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Filters (protocol)	IP, IPX, NetBEUI, DECNET, AppleTalk
Filters (others)	IP, ARP, Novell RIP, SAP, LSP
Management interfaces	Web browser-based manager, text-based menu system, Telnet, SNMP
Software upgrades	Downloadable over the network
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x, Enterprise MobileLAN access

Radio Specifications

IEEE 802.11b

Frequency band	2.4 to 2.5 GHz worldwide
Type	Direct sequence, spread spectrum
Modulation	Direct sequence, spread spectrum (CCK, DQPSK, DBPSK)
Power output	32 mW (15 dBm)
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), 14 (Japan). 1 (Israel)
Range (11 Mbps)	160 m (525 ft) open environment 50 m (165 ft) semi-open environment 24 m (80 ft) in closed environment Unlimited range with roaming
Receiver sensitivity (11 Mbps)	-82 dBm
Security	IEEE 802.11 Wired Equivalent Privacy (WEP) standard, WEP 64, WEP 128

IEEE 802.11a

Frequency band	Full range Mid range	5.15 to 5.35 GHz (Indoor only) 5.25 to 5.35 GHz (Indoor and outdoor)
Type	Direct sequence, spread spectrum	
Power output	40mW	
Data rate	802.11 compliant mode: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps, 6 Mbps with automatic fallback for increased range Turbo mode: 72 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps with automatic fallback for increased range	
Channels	802.11 compliant mode (Full range): 8 (North America) 802.11 compliant mode (Mid range): 4 (North America) Turbo mode: 3 (North America)	
Range (depending on environment)	248 m (813.7 ft) 240 m (787.4 ft) 175 m (574.2 ft) 132 m (433.1 ft) 56 m (183.7 ft) 37 m (121.4 ft) 19 m (62.3 ft)	6 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps
Receiver sensitivity (54 Mbps)	-68 dBm	

WLI Forum OpenAir

Frequency band	2.4 GHz, actual frequencies vary by country
Type	Frequency hopping, spread spectrum
Power output	
2100	500 mW (27 dBm) 100 mW (20 dBm) (Europe)
2101	100 mW (20 dBm)
2102	100 mW (20 dBm)
Data rate	1.6 Mbps
Channels	15
Range	Up to 300 m (1,000 ft) outdoors Up to 150 m (500 ft) indoors
Receiver sensitivity	-77 dBm @ 1.6 Mbps -85 dBm @ 800 Kbps

902 MHz

Frequency band	902 to 928 MHz (not available in Europe)	
Type	Direct sequence, spread spectrum	
Power output	Minimum Typical Maximum	24dBm (250 mW) 25.5dBm (350 mW) 27dBm (500 mW)
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)	

S-UHF

Frequency band	
Low band High band	430-450 MHz 450-470 MHz
Type	Synthesized UHF (four-level frequency shift keying)
Power output	0.5 W (27 dBm) low and high bands 10 mW (10 dBm) (must meet local regulatory requirements)
Data rate	19.2 Kbps (14.4 Kbps with forward error correction)
Channels spacing	20 KHz or 25 KHz
Range	Up to 1,067 m (3,500 ft) line of sight
Coverage	
0.5 W 10 mW	74,320 sq m (800,000 sq ft) indoors 9,290 sq m (100,000 sq ft) indoors
Receiver sensitivity	-105 dBm

Antennas and Antenna Accessories

This table identifies many of the Intermec antennas and antenna accessories for the radios. Contact your local Intermec representative for detailed information.

Description	Part Number	Description
MobileLAN access antennas	067261	Antenna, 2.4 GHz, 3 dBi Mini Omni
	067262	Antenna, 2.4 GHz, 5 dBi Dual Flat
	063363	Antenna, 2.4 GHz, 5 dBi Omni
	065349	Antenna, 2.4 GHz, 9 dBi Omni
	067263	Antenna, 2.4 GHz, 9 dBi Flat Panel
	063365	Antenna, 2.4 GHz, 15 dBi Yagi
	071122	Antenna, Corner Reflector
	071121	Antenna, Diversity
MobileLAN access 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)
	071178	Cable, TNC/N male, 3.7 m (12 ft)
	071179	Cable, Coaxial, 9.1 m (30 ft)
	064432	LMR400 cable, 30.5 m (100 ft)
	589377	LMR400 cable prep tool
	061868	Lightning suppressor and bracket
	586610	Lightning suppressor capsule
WA21/WA22 antennas	072730	Antenna, 5 GHz, swivel, TNC
	072759	Antenna, 5 GHz, 6 dbi, omni
	072760	Antenna, 5 GHz, 9 dbi, omni
	072761	Antenna, 5 GHz, 3 dbi, omni, ceiling mount
	072762	Antenna, 5 GHz, corner reflect
WA21/2100 antennas	066147	Antenna, 2.4 GHz, Omni
	063366	Antenna, 2.4 GHz, 14 dBi Flat Panel (hardware mast provided)

Antennas and Antenna Accessories (continued)

Description	Part Number	Description
2100 antennas	065285	Antenna, 900 MHz, 7 dBi Omni
	067264	Antenna, 900 MHz, 9 dBi Flat Panel
	805-472-002	Antenna, 900 MHz, Whip
	203-449-002	Antenna, S-UHF, 1.5 m (5 ft)
	203-449-003	Antenna, S-UHF, 5.5 m (18 ft)
	805-430-001	Antenna, S-UHF, 5 dB Mag Mount (includes 3.67 m (12 ft) cable, no extensions)
	805-431-000	Antenna, S-UHF, 1/4 Wave Ground Plane
	805-511-001	Antenna, 400 MHz UHF, Whip
WA21/2100 accessories	067265	Adapter cable (to cable)
	067266	Adapter cable (to antenna)
	069304	Splitter, 900 MHz
	216-565-003	Cable extension, 5.5 m (18 ft)
	216-565-001	Cable extension, 11 m (36 ft)
	216-565-004	Cable extension, 15.2 m (50 ft)
	216-565-006	Cable extension, 30.5 m (100 ft)
WA22/2101/ 2102 antennas	070140	Antenna, 2.4 GHz, 3 dBi Mini Flat (OpenAir)
	070141	Antenna, 2.4 GHz, 3 dBi Mini Flat (802.11b)
	071488	Antenna, Diversity, OpenAir/MobileLAN card 11
	071489	Antenna, Diversity, 802.11b
	069886	Adapter cable, OpenAir/MobileLAN card 11 (to cable)
	069887	Adapter cable, 802.11b (to cable)
	069910	Adapter cable, OpenAir/MobileLAN card 11 (to cable adapter 067265/ 067266)
	069911	Adapter cable, 802.11b (to cable adapter 067265/ 067266)
	070402	Adapter cable, OpenAir/MobileLAN card 11 (to antenna)
	070403	Adapter cable, 802.11b (to antenna)
WA22/2101 antennas	069753	Antenna, 2.4 GHz Omni (2101 spare)
	069903	Antenna, 2.4 GHz Omni, 802.11b (2101 spare)

Antennas and Antenna Accessories (continued)

Description	Part Number	Description
2102 accessories		Mounting kit for printers.

Default Settings

The factory default settings for the access points 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	Your Site?
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	
DHCP Mode	Always use DHCP, Use DHCP if IP Address is Zero, Disable DHCP, This AP is a DHCP Server	Use DHCP if IP Address is Zero	
DHCP Server Name	0 to 31 characters	(blank)	
Auto ARP Minutes	0 to 120	5	

Spanning Tree Settings Menu Defaults

Parameter Name	Range	Default	Your Site?
AP Name	0 to 16 characters	(access point serial number)	
LAN ID (Domain)	0 to 254	0	
Root Priority	0 to 7	1	
Enable Ethernet Bridging	Check/Clear	Check	
Secondary LAN Bridge Priority	0 to 7	0	
Secondary LAN Flooding	Enabled, Multicast, Unicast, Disabled	Disabled	

Global Flooding Menu Defaults

Parameter Name	Range	Default	Your Site?
Multicast Flood Mode	Universal, Hierarchical, Disabled	Hierarchical	
Allow Multicast Outbound to Terminals	Check/Clear	Check	
Multicast Outbound to Secondary LANs	Enabled globally/Set locally	Set locally	
Unicast Inbound Flood Mode	Universal, Hierarchical, Disabled	Disabled	
Enable ARP Flooding	Check/Clear	Check	

Global RF Parameters Menu Defaults

Parameter Name	Range	Default	Your Site?
Perform RFC1042/DIX Conversion	Check/Clear	Check	
S-UHF Rfp Threshold			
Set Globally	Enabled/Disabled	Disabled	
Value	0 to 250 bytes	70 bytes	
S-UHF Frag Size			
Set Globally	Enabled/Disabled	Disabled	
Value	50 to 250 bytes	250 bytes	
902 MHz Frag Size			
Set Globally	Enabled/Disabled	Disabled	
Value	50 to 250 bytes	250 bytes	
S-UHF/902 MHz Awake Time			
Set Globally	Enabled/Disabled	Disabled	
Value	0 to 250 tenths of a second	10 (902 MHz) 20 (S-UHF)	
RFC1042 Types to Pass Through			
1	Two sets of hexadecimal pairs 00 through FF.	80 F3	
2	Two sets of hexadecimal pairs 00 through FF.	81 37	
3 through 20	Two sets of hexadecimal pairs 00 through FF.	00 00	

Ethernet Configuration Menu Defaults

Parameter Name	Range	Default	Your Site?
Port Type	10/100 Mb Twisted-Pair/100 Mb Fiber Optic	10/100 Mb Twisted-Pair	
Link Speed	Auto Select, 100 Mbps Full-Duplex, 100 Mbps Half-Duplex, 10 Mbps Full-Duplex, 10 Mbps Half-Duplex	Auto Select	
Enable Link Status Check	Check/Clear	Clear	
Address Table			
1 through 20	Six sets of hexadecimal pairs 00 through FF.	00 00 00 00 00 00	
Frame Type Filters			
Allow/Pass	Check/Clear	Check	
Scope	Unlisted/All	Unlisted	
Predefined Subtype Filters			
Allow/Pass	Check/Clear	Check	
Customizable Subtype Filters			
Allow/Pass	Check/Clear	Check	
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, 802.2-SAP	DIX-IP-TCP-Port	
Value	Two sets of hexadecimal pairs 00 through FF.	00 00	

Ethernet Advanced Filters Menu Defaults

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

IP Tunnels Menu Defaults

Parameter Name	Range	Default	Your Site?
Mode	Listen, Originate If Root, Disabled	Listen	
Enable IGMP	Check/Clear	Clear	

Tunnel Filters Menu Defaults

Parameter Name	Range	Default	Your Site?
Frame Type Filters			
Allow/Pass	Check/Clear	Clear	
Scope	Unlisted/All	Unlisted	
Predefined Subtype Filters			
Allow/Pass	Check/Clear	Clear (except Check for NNL)	

Tunnel Filters Menu Defaults (continued)

Parameter Name	Range	Default	Your Site?
Customizable Subtype Filters			
Allow/Pass	Check/Clear	Clear	
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, 802.2-SAP	DIX-IP-TCP-Port	
Value	Two sets of hexadecimal pairs 00 through FF.	00 00	

Network Management Menu Defaults

Parameter Name	Range	Default	Your Site?
SNMP Read Community	1 to 15 characters	public	
SNMP Write Community	1 to 15 characters	CR52401	
SNMP Secret Community	1 to 15 characters	Secret	

Security Menu Defaults

Parameter Name	Range	Default	Your Site?
Browser Access	Secure-Only (Port 443), Enabled (Port 80/443), Disabled	Enabled (Port 80/443)	
Allow Telnet Access (Port 23)	Check/Clear	Check	
Allow SNMP Access (Port 161)	Check/Clear	Check	
Allow ICMP Configuration	Check/Clear	Check	

Passwords Menu Defaults

Parameter Name	Range	Default	Your Site?
Use RADIUS for Login Authorization	Check/Clear	Clear	
User Name	1 to 32 characters	Intermec	
Password	1 to 32 characters	Intermec	
Read Only Password	1 to 32 characters	(blank)	
Allow Service Password	Check/Clear	Check	

ACL Menu Defaults

Parameter Name	Range	Default	Your Site?
ACL Client Authorization	Disabled, IEEE 802.11a Radio, IEEE 802.11b Radio, OpenAir Radio, 902 MHz Radio, S-UHF Radio, All Radios	Disabled	

802.1x Menu Defaults

Parameter Name	Range	Default	Your Site?
802.1x Authentication	Disabled, IEEE 802.11a Radio, IEEE 802.11b Radio, All 802.11 Radios, IAPP only	Disabled	

IEEE 802.11 (b or a) WEP Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable WEP Encryption	Check/Clear	Clear	

Internal RADIUS Server Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable Server	Check/Clear	Clear	

IEEE 802.11b Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Node Type	Master, Station, Disabled	Master	
SSID (Network Name)	0 to 32 characters	INTERMEC	
Frequency	Channel 1 to 14, 2400 to 2500 MHz	Channel 03, 2422 MHz	
Advanced Configuration			
Data Rate	11, 5.5, 2, or 1 Mbps	11 MBits (High)	
Allow Data Rate Fallback	Check/Clear	Check	
Basic Rate	11, 5.5, 2, or 1 Mbps	2 MBits (Standard)	
Enable Medium Reservation	Check/Clear	Clear	
Distance Between APs	Large, Medium, or Small	Large	
Enable Microwave Oven Robustness	Check/Clear	Clear	
Enable Load Balancing	Check/Clear	Clear	
Enable Medium Density Distribution	Check/Clear	Clear	
Data/Voice Settings	Data Traffic Only, Data and SpectraLink Traffic, SpectraLink Traffic Only	Data Traffic only	
Disallow Network Name of ‘ANY’	Check/Clear	Clear	
DTIM Period	1 to 65535	1	
Inbound Filters			
Allow IAPP	Check/Clear	Check	
Allow Wireless Transport Protocol (WTP)	Check/Clear	Check	
Allow SpectraLink Voice Protocol (SVP)	Check/Clear	Check	
Allow UDP Plus (UDP/IP Port 5555)	Check/Clear	Check	
Allow DHCP	Check/Clear	Check	
Allow All Other Protocols	Check/Clear	Check	

IEEE 802.11a Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Node Type	Master, Station, Disabled	Master	
SSID (Network Name)	0 to 32 characters	INTERMEC	
Frequency	36, 40, 42, 44, 48, 50, 52, 56, 58, 60, 64	(full-range) Channel 36, 5180 MHz IEEE (mid-range) Channel 52, 5260 MHz IEEE	
Advanced Configuration			
Data Rate	54, 48, 36, 24, 12, or 6 Mbps	54 MBits (High)	
Allow Data Rate Fallback	Check/Clear	Check	
Basic Rate	24, 12, 6 Mbps	6 MBits (Low)	
Reservation Threshold	1 to 65535	2347 (Disabled)	
Fragmentation Threshold	256 to 2346	2346	
Beacon Period	20 to 1000 TU	100	
DTIM Period	1 to 5	1	
Inbound Filters			
Allow IAPP	Check/Clear	Check	
Allow Wireless Transport Protocol (WTP)	Check/Clear	Check	
Allow SpectraLink Voice Protocol (SVP)	Check/Clear	Check	
Allow UDP Plus (UDP/IP Port 5555)	Check/Clear	Check	
Allow DHCP	Check/Clear	Check	
Allow All Other Protocols	Check/Clear	Check	

OpenAir Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Node Type	Master, Station, Disabled	Master	
Security ID	1 to 20 characters	(blank)	
Channel	1 to 15	1	
Subchannel	1 to 15	1	
MAC Configuration	Default, Interference, Throughput, or Manual	Default	
Inbound Filters			
Allow IAPP	Check/Clear	Check	
Allow Wireless Transport Protocol (WTP)	Check/Clear	Check	
Allow SpectraLink Voice Protocol (SVP)	Check/Clear	Check	
Allow UDP Plus (UDP/IP Port 5555)	Check/Clear	Check	
Allow DHCP	Check/Clear	Check	
Allow All Other Protocols	Check/Clear	Check	
Manual MAC Parameters			
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	
Normal Ack Retry	1 to 255	255	
Fragment Ack Retry	1 to 255	255	
Normal QFSK Retry	1 to 255	255	
Fragment QFSK Retry	1 to 255	255	

902 MHz Radio Configuration Menu Defaults

Parameter Name	Range	Default	Your Site?
Port Control	Check/Clear	Check	
Mode-Channel	Depends on country	DS 225K-Channel 25	
Multicast Filter	Check/Clear	Clear	
File Name	FALCON_D.BIN	FALCON_D.BIN	
Hello Period	1, 2, or 3 seconds	1 second	

S-UHF Radio Configuration Menu Defaults

Parameter Name	Range	Default	Your Site?
Port Control	Check/Clear	Check	
Frequency	(programmed at factory based on regulatory requirements)	(first frequency in list)	
Call Sign	0 to 12 characters	(blank)	
Master Mode	Check/Clear	Clear	
Attach Priority	Low, Medium, or High	High	
Multicast Filter	Check/Clear	Clear	
File Name	SYNUHF_D.BIN	SYNUHF_D.BIN	
Hello Period	1, 2, or 3 seconds	2 seconds	

G Glossary

ARP (Address Resolution Protocol) cache

A table that stores IP addresses and their corresponding MAC addresses. The access point maintains an ARP cache and can act as an ARP server.

BFSK (Binary Frequency Shift Key)

A broadcasting method that lengthens the range but halves the throughput as compared to the QFSK method. In access points using an OpenAir radio, the radio can be configured so that it automatically switches to this method when the RF protocol determines that throughput is degrading due to range. The transmit mode parameter determines if BFSK will be used. The default setting for transmit mode is AUTO, which allows this automatic switching to occur.

broadcast

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

data link tunneling

An access point feature that encapsulates the data into an OWL data frame. This frame is then forwarded via the Ethernet port to the next access point on the path and so on until the frame reaches the root access point or designated bridge. The root access point or designated bridge unencapsulates the frame and forwards it to the host. When the root access point or designated bridge receives data on the Ethernet network for an end device, it reverses this process.

You should only use data link tunneling if you have Ethernet switches that do not support the IEEE 802.1d requirements for backward learning or if you are using IP tunnels to provide mobility of other routable protocols.

To enable data link tunneling, disable Ethernet bridging.

designated bridge

Also called a secondary LAN bridge. An access point that is assigned the role of bridging frames destined for or received from a secondary LAN. A designated bridge connects a secondary LAN with the primary LAN. In the access point, the secondary LAN bridge priority parameter determines if the access point 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.

directional antenna

An antenna (often called a yagi) that transmits and receives RF signals more in one direction than others. This radiation pattern is similar to the light that a flashlight produces. These antennas have a narrower beam width, which limits coverage on the sides of the antennas. Directional antennas have much higher gains than omni antennas and work best for covering large narrow areas or on point-to-point bridges.

distribution LAN

Any Ethernet LAN attached to access points that are bridging between the Ethernet LAN and the radio network. At any given time, only one access point 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.

EAP (Extensible Authentication Protocol)

Used in 802.1x-enabled networks. A standard mechanism for support of different authentication methods. EAP authentication types provide devices with secure connections to the network as well as protect credentials and data privacy. See also “TLS” and “TTLS.”

Ethernet bridging

When an access point receives wireless traffic and the destination address is known, it forwards frames to the port with the shortest path to the destination address. When the access point has not learned the direction of the shortest path for the destination address, it forwards frames based on flooding settings to try to locate the destination address.

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.

hello period

A time increment (usually 1, 2, or 3 seconds) that determines how often the access point sends out a type of multicast frame so that it can dynamically discover and test connections to other devices in the network. Once this information is learned, the access point and routers can exchange routing information.

home IP subnet

Also called the root IP subnet and primary LAN. The IP subnet that contains the root access point. If wireless end devices need to roam between IP subnets, each end device needs to have an IP address from the home IP subnet.

IAPP (Inter Access Point Protocol)

Access points use this Intermec protocol to communicate with each other. For example, when a wireless end device roams to a new access point, the new access point informs the old access points via the root access point that any traffic for the end device needs to be routed to the new access point.

This protocol also allows 802.1x-ready devices to roam seamlessly through the network without having to reauthenticate after each roam. IAPP distributes security credentials throughout the network. When an end device roams from one access point to another, its credentials are also transferred.

Secure IAPP prevents unauthorized MobileLAN access products from joining the spanning tree and it encrypts IAPP frames. If you enable secure IAPP, access points will use SWAP to create secure wireless hops when communicating with each other.

IGMP (Internet Group Management Protocol)

A standard protocol that lets you originate multiple IP tunnels using one IP multicast address. IGMP allows IP multicast frames to be routed to remote IP subnets that have hosts participating in the multicast group. By enabling IGMP, access points can act as IP hosts and participate in an IP multicast group.

inbound frames

Frames moving toward the primary LAN.

IP 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.

IP subnet

A single member of the collection of hardware networks that comprise 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.

IP tunneling

IP tunneling is used on networks with routers. IP tunneling allows wireless end devices to roam across IP subnet boundaries without losing connection. IP tunneling encapsulates standard IP frames with Generic Routing Encapsulation (GRE) and forwards the frames from the root access point on a home IP subnet to another access point on a remote IP subnet. IP tunneling is done through the access points' logical IP ports.

MAC address

There are two 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 access point.

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.

NAT (Network Address Translation)

A mechanism for reducing the need for different IP addresses. NAT allows an organization with IP addresses that are not unique to connect to the network by translating those addresses into routable address space. The access point can act as a DHCP/NAT server.

non-bridging secondary LAN

A secondary LAN that does not have a designated bridge. A non-bridging secondary LAN is used to interconnect access points without using wireless hops.

omni antenna

An antenna that transmits and receives RF signals in all directions equally on a horizontal plane. This radiation pattern is similar to a doughnut with the antenna being in the center of the doughnut hole. These antennas provide the widest coverage and are most commonly used inside buildings.

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-multipoint bridge

See also wireless bridge. A bridge that connects two wired networks with similar architectures. Two access points can be used to provide a point-to-multipoint bridge between two buildings so that wired and wireless devices in each building can communicate with devices in the other building. A point-to-multipoint bridge has two radios, which allows wireless end devices to communicate with it.

point-to-point bridge

See also wireless bridge. A bridge that connects two wired networks with similar architectures. Two access points 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.

power bridge

The MobileLAN power bridge combines power and data onto an Ethernet cable that is connected to the MobileLAN splitter or the access point with the power over Ethernet option.

primary bridging

Ethernet bridging on a root port. An access point 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

Also called the home IP subnet and root IP subnet. The IP subnet that contains the root access point. The primary LAN is typically the LAN on which the servers are located.

QFSK (Quad Frequency Shift Key)

A broadcasting method that shortens the range but doubles the throughput as compared to the BFSK method. In access points 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 IP subnet

An IP subnet that is separated from the primary IP subnet (primary LAN) by a router. Remote IP subnets communicate with the primary LAN through IP tunnels. A remote IP subnet is a type of secondary LAN.

root access point

The access point 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 access point 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 access point port that provides the inbound connection to the spanning tree. The root port provides a link to a parent access point. Note that a root access point does not have a root port.

root IP subnet

Also called the home IP subnet and primary LAN. The IP subnet that contains the root access point. If wireless end devices need to roam between IP subnets, each end device needs to have an IP address from the root IP subnet.

secondary bridging

Ethernet bridging on a non-root port. An access point 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 port.

secondary LAN

Any LAN that is reached by routing traffic through an access point. Wireless end devices that are communicating through a WAP comprise a secondary LAN. A remote IP subnet is a type of secondary LAN.

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, such as MobileLAN manager, 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 access points automatically configure into a self-organized network that provides efficient, loop-free forwarding of frames through the network.

splitter

The MobileLAN splitter converts 48V input power to 5V or 3.3V output power. If you want to use power over Ethernet, you plug the access point into the splitter and then you plug the splitter into a MobileLAN power bridge.

The WA22, WA21, and 2100 do not use a splitter.

SWAP (Secure Wireless Authentication Protocol)

This protocol creates secure wireless hops if you enable secure IAPP. It forces access points to authenticate each other using an EAP-MD5 challenge.

TLS (Transport Layer Security)

An EAP authentication type that not only requires a certificate on the authentication server, but also one on the end device. There is both server and client side authentication before the end device can communicate with the network.

TTLS (Tunneled Transport Layer Security)

An EAP authentication type that only requires a certificate on the authentication server. End devices have a user name and password that proves that they are authorized to communicate with the 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.

unicast address

A unique Ethernet address assigned to a single device on the network.

WAP (Wireless Access Point)

Also called a repeater. This access point does not have any connections on its Ethernet port. It forwards data between the access point and the secondary LAN.

WEP (Wired Equivalent Privacy) encryption

A feature that can be enabled in the IEEE 802.11b or 802.11a radio that allows data encryption for wireless communications.

wireless bridge

Also called a point-to-point bridge. A wireless link that connects two wired Ethernet segments. Two access points can be used to provide a wireless bridge between two buildings, so that wired and wireless devices in each building can communicate with devices in the other building.

wireless hop

A wireless link that occurs when data from a wireless end device moves from one access point to another access point through the radio ports. Using MobileLAN access products, Intermec recommends that your data does not travel through more than three wireless hops.

Secure wireless hops are created when secure IAPP is enabled. Access points use SWAP to authenticate each other.

I Index

Intermec

Corporate Headquarters
6001 36th Avenue West
Everett, Washington 98203
U.S.A.

tel 425.348.2600

fax 425.355.9551

www.intermec.com

MobileLAN access System Manual