Intermec

System Manual

MobileLAN™ access WA2XG

Intermec Technologies Corporation

Corporate Headquarters
6001 36th Ave. W.
Everett, WA 98203
U.S.A.

www.intermec.com

The information contained herein is proprietary and is provided solely for the purpose of allowing customers to operate and 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 contained in this document are subject to change without prior notice and do not represent a commitment on the part of Intermec Technologies Corporation.

The word Intermec, the Intermec logo, Norand, ArciTech, CrossBar, Data Collection Browser, dcBrowser, Duratherm, EasyCoder, EasyLAN, Enterprise Wireless LAN, EZBuilder, Fingerprint, i-gistics, INCA (under license), InterDriver, Intermec Printer Network Manager, IRL, JANUS, LabelShop, Mobile Framework, MobileLAN, Nor*Ware, Pen*Key, Precision Print, PrintSet, RoutePower, TE 2000, Trakker Antares, UAP, Universal Access Point, and Virtual Wedge are either trademarks or registered trademarks of Intermec Technologies Corporation.

Wi-Fi is a registered certification mark of the Wi-Fi Alliance.

Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries.

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.

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

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

Document Change Record

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

Version	Date	Description of Change
002	07/2005	Added information about the new features of software release 3.01, including support for dual 802.11g radios, wireless bridging, wireless hops, and antenna diversity.

Contents

Before You Begin

This section provides you with safety information, technical support information, and sources for additional product information.

Safety Summary

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

Safety Icons

This section explains how to identify and understand warnings, cautions, and notes that are in this document.

⚠ 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.

⚠ 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.

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

Global Services and Support

Warranty Information

To understand the warranty for your Intermec product, visit the Intermec web site at www.intermec.com and click **Service & Support**. The Intermec Global Sales & Service page appears. From the **Service & Support** menu, move your pointer over **Support,** and then click **Warranty**.

Disclaimer of warranties: The sample code included in this document is presented for reference only. The code does not necessarily represent complete, tested programs. The code is provided "as is with all faults." All warranties are expressly disclaimed, including the implied warranties of merchantability and fitness for a particular purpose.

Web Support

Visit the Intermec web site at www.intermec.com to download our current manuals in PDF format. To order printed versions of the Intermec manuals, contact your local Intermec representative or distributor.

Visit the Intermec technical knowledge base (Knowledge Central) at intermec.custhelp.com to review technical information or to request technical support for your Intermec product.

Telephone Support

You can find information on Intermec telephone support services on the Intermec web site at www.intermec.com/AIT. To find the correct telephone support number for your country, click **Contact**.

Who Should Read This Document?

This manual is for the people who are responsible for installing, operating, configuring, maintaining, and troubleshooting the MobileLAN access WA21G and WA22G products. It also provides information about the features of the WA21G and WA22G, the specifications and the default configuration.

Before you install and configure an access point, you should be familiar with your network and general networking terms, such as IP address.

Related Documents

The Intermec web site at www.intermec.com contains many of our documents that you can download in PDF format.

To order printed versions of the Intermec manuals, contact your local Intermec representative or distributor.

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.

1 Getting Started

This chapter introduces the MobileLAN™access WA2XG 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 products
- How the access point fits in your network
- Configuring the access point for the first time
- Saving configuration changes

Overview of the MobileLAN access Products

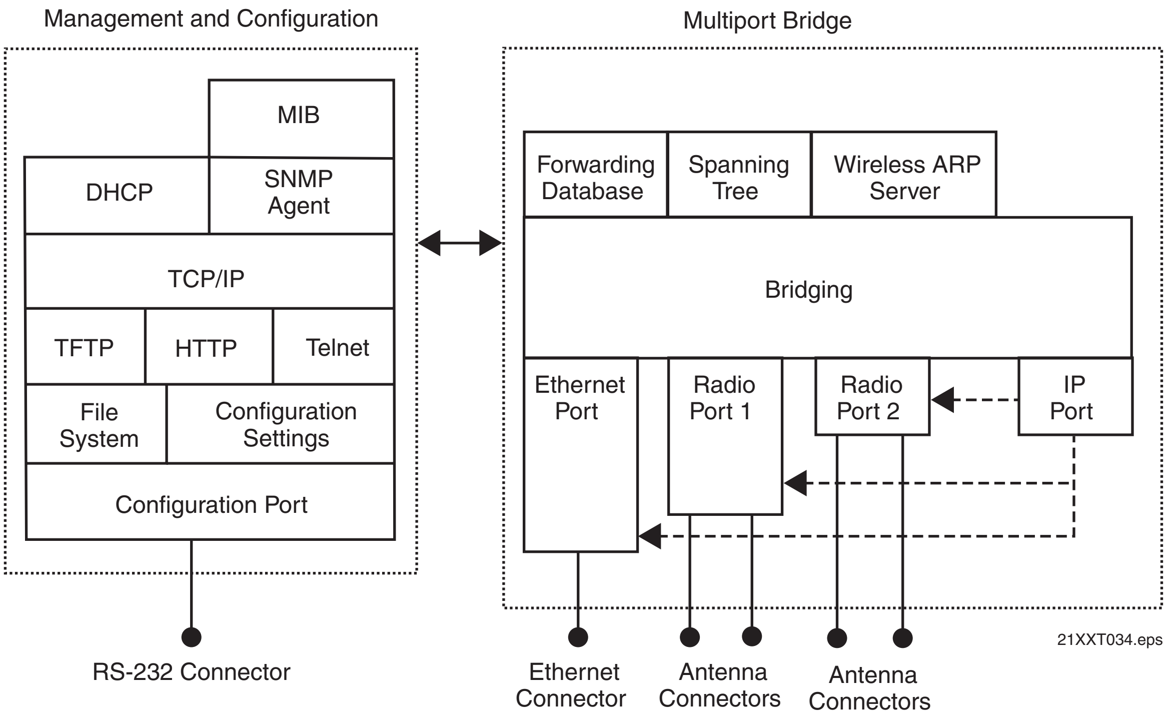
Intermec’s MobileLAN™access WA2XG family of access points delivers reliable and seamless wireless performance to almost any operational environment. They are designed for standards-based connectivity and they support industry standard IEEE 802.11g and 802.11b wireless technologies.

The WA21G and WA22G with an IEEE 802.11g radio installed are Wi-Fi certified for interoperability with other 802.11g and 802.11b wireless LAN devices.

The access point can be configured as an access point, a wireless access point (WAP), a point-to-point bridge, or a 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 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.

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 not only connects two wired LANs, but also communicates with wireless end devices.



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

This table lists the features of the MobileLAN access WA2XG products.

MobileLAN access Feature Comparison

Feature	WA21G	WA22G
Access Point	Yes	Yes
Point-to-Point Bridge (Wireless Bridge)	Yes	Yes
Wireless Access Point (WAP) or Repeater	Yes	Yes
Secure Wireless Hops (SWAP)	Yes	Yes
Secure Wireless Hops (TLS or TTLS)	Yes	Yes
Radios	802.11g*	802.11g*
Dual Radio Support	Yes	Yes
Wi-Fi Compliant	Yes	Yes
Wi-Fi Protected Access (WPA) for 802.1x mode or PSK mode.	Yes	Yes
802.1x Authenticator	Yes	Yes
802.1x Authentication Server	Yes	Yes
Access Control List (ACL) Server	Yes	Yes
Password Server	Yes	Yes
Secure Web Browser Interface (HTTPS)	Yes	Yes
10BaseT/100BaseTx	Yes	Yes
Fiber Optics	Yes	Yes
Serial Port	Yes	Yes
Data Link Tunneling	Yes	Yes
IP Tunneling	Yes**	Yes**
Antenna Diversity	Yes	Yes
Non-incentive Antenna System	Yes	Yes
NEMA 4/IP 54 Protection	Yes	No
Power Supply	AC	No
Power Over Ethernet	Yes	Yes
Heater Option	Yes	No

*The 802.11g radio is sometimes referred to as the 802.11b/g radio because it can be configured to communicate with any 802.11b and 802.11g radios that have the same SSID and security settings.

**If you are using IPv6 addressing, IP tunneling is not supported.

Other features of all access points include:

- the ability to be managed by the Wavelink Avalanche client management system, 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.
- basic WEP security for 802.11g radios.

What's New for Software Releases 3.01?

Antenna diversity: The 802.11g radio now supports antenna diversity.

Support for dual 802.11g radios: The WA2XG now supports two 802.11g radios. An access point requires two radios before it can do point-to-multipoint bridging and wireless hops.

Wireless bridging and wireless hops: The WA2XG with two radios now supports wireless bridging and wireless hops.

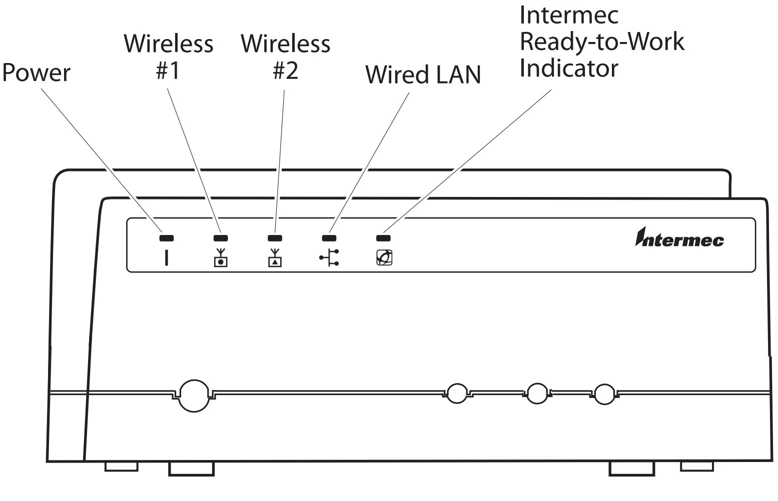
Important Note: With this software release, a WA2XG can bridge a primary LAN to a secondary LAN. If the designated bridge on the secondary LAN has two radios, it can also communicate with wireless end devices. However, even if the designated bridge has two radios, it cannot bridge to another LAN. If you need the secondary LAN to bridge to another secondary LAN, you must use another access point. For more information, see Chapter 5, "Configuring the Spanning Tree."

Understanding the LEDs

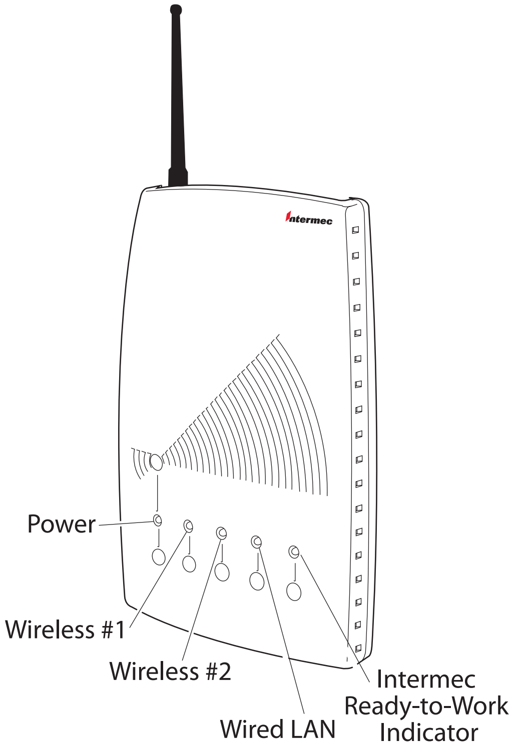
The WA21G and WA22G have five LEDs. To understand the LEDs during normal use, see the next table. To use the LEDs to help troubleshoot the radios, see “Troubleshooting the Radios” on page 191.

LED Descriptions

Icon	LED	Description
|	Power	Remains on when power is applied.
●	Wireless #1	Blinks when a frame is transmitted or received on the radio port for the radio installed in radio slot 1.
▲	Wireless #2	Blinks 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	Blinks when a frame is transmitted or received on the Ethernet port.
⊘	Intermec Ready-to-Work™ Indicator	Indicates the operational status of the access point. This blue LED can be off, blinking, or on: **Off** indicates that the access point is not operational or that it has not been booted. **Blinking** indicates that the access point is searching for the root access point in the system. **On** indicates that the access point either has found a root access point or it has become the root access point. The access point is now ready for use in your Intermec network. **Note:** In the **Spanning Tree Settings** screen, you can configure this LED to behave as if it were a Root/error LED.



WA21G LEDs: *This illustration shows the LEDs that are on the WA21G. For help understanding these LEDs, see the LED Descriptions table on this page.*



***WA22G LEDs:** This illustration shows the LEDs that are on the WA22G. For help understanding these LEDs, see the LED Descriptions table on the previous page.*

Understanding the Ports

The access point may have up to four ports.

Port Descriptions

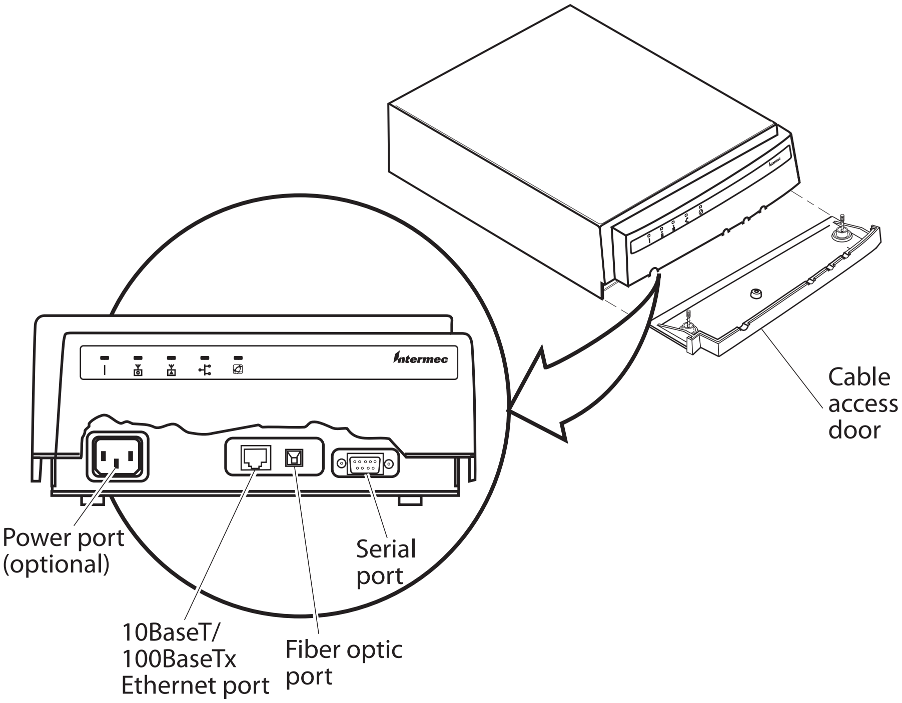
Port	Description
Power (Not WA22G)	Used with an appropriate power cable, this port connects the access point to an AC power source.
Serial	Used with an RS-232 null-modem cable, this port connects the access point to a terminal or PC to perform configuration.
Ethernet	10BaseT/100BaseTx port. Used with 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.
Fiber optic	100BaseFX port. You must use a patch cable with a female MT-RJ connector to connect the access point to your MT-RJ, SC, or ST fiber optic network.

To access the ports on the WA21G, you must remove the cable access door.

To remove the WA21G cable access door

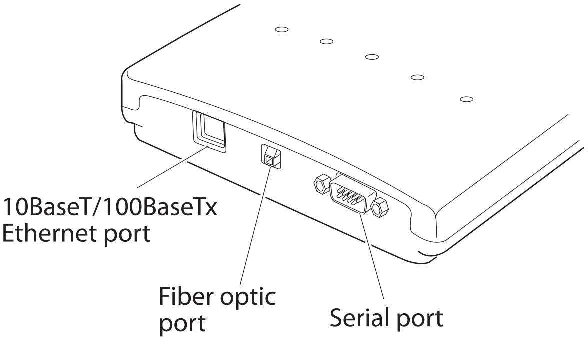
1 Unscrew the two thumbscrews on the cable access door.

2 Remove the door.



WA21G ports: *This illustration shows the ports that are on the WA21G. For help understanding these ports, see the Port Descriptions table on the previous page.*

The WA22G ports are located on the bottom of the access point.



WA22G ports: *This illustration shows the ports that are on the WA22G. For help understanding these ports, see the Port Descriptions table on the previous page.*

For more information on connecting the ports, see Chapter 2, “Installing the Access Points.”

How the Access Point Fits in Your Network

In general, the access point forwards data from wireless end devices to the wired Ethernet network. Since both the WA21G and the WA22G have two radios, you can also use them as point-to-multipoint bridges or as WAPs.

Use the access point in the following locations and environments.

Which Access Point to Use for Your Environment

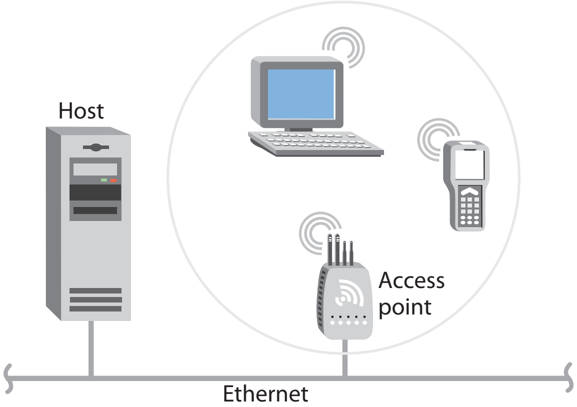
Access Point	Environment
WA21G	Use in locations where an access point is exposed to extreme environments.
WA22G	Use in most indoor environments.

The access point supports a variety of network configurations. These configurations are explained in the next sections:

- Using One Access Point in a Simple Wireless Network (on page 9)
- Using Multiple Access Points and Roaming Wireless End Devices (on page 11)
- Using an Access Point as a WAP (on page 13)
- Using Access Points to Create a Point-to-Point Bridge (on page 16)
- Using Dual Radio Access Points for Redundancy (on page 20)

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 provide a wireless extension of the wired LAN.



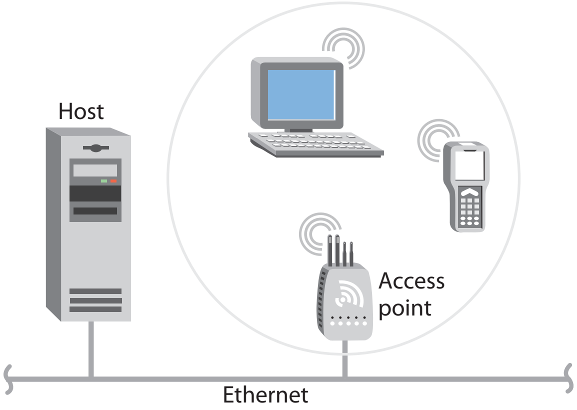
This illustration shows a simple wireless network with one access point and some wireless end devices.

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" on page 21.
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 802.11g Access Point



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

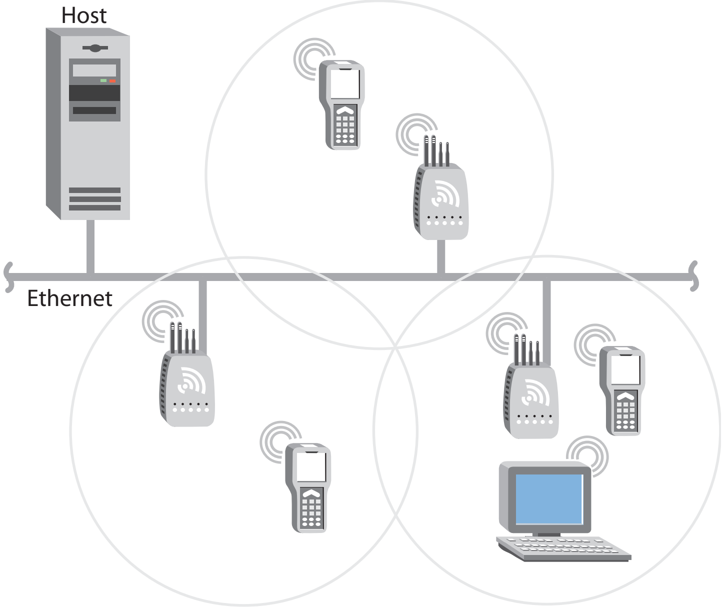
Configuring 802.11g Access Point Parameters

Screen	Parameter	Access Point
802.11g Radio	Node Type	Master
	SSID (Network Name)	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" on page 20.

To install multiple access points with roaming end devices

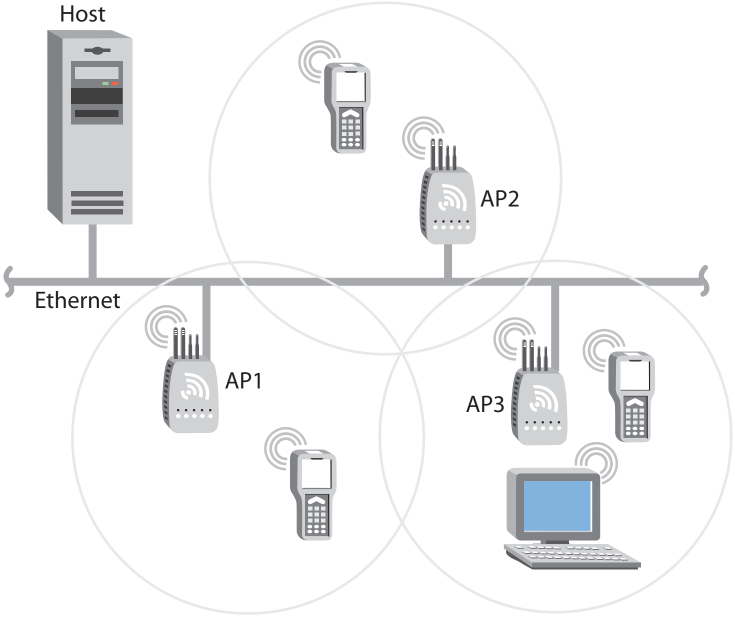
1 Follow the instructions for installing a simple wireless network on page 9.

2 Configure the LAN ID. For help, see "Configuring the Spanning Tree Parameters" on page 91.

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" on page 87.

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 Ethernet Bridging/Data Link Tunneling” on page 89.

Example - Configuring an 802.11g Access Point with Roaming End Devices



In this example, there is one 802.11g radio in each access point. Wireless end devices can roam between the access points to communicate with the host and other end devices.

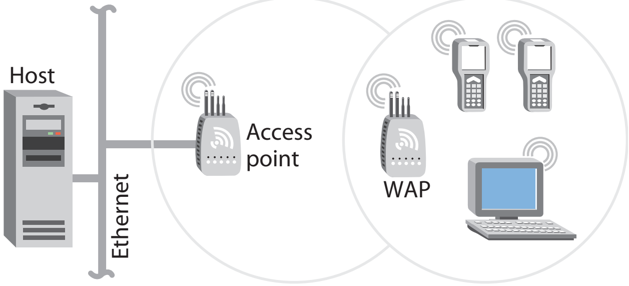
Configuring 802.11g Access Points Parameters

Screen	Parameter	AP1 802.11g Radio (Root)	AP2 802.11g Radio	AP3 802.11g Radio
802.11g Radio	Node Type	Master	Master	Master
	SSID	Op3rat!ons	Op3rat!ons	Op3rat!ons
Spanning Tree Settings	LAN ID	0	0	0
	Root Priority	5	4	3
	Ethernet Bridging Enabled	Checked	Checked	Checked
	Secondary LAN Bridge Priority	0	0	0

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 SSID set to Op3rat!ons.

Using an Access Point as a WAP

You can extend the range of your wireless network by configuring an access point with two 802.11g radios 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 WAP. Wireless end devices use the WAP to forward data to the access point, which forwards data to the host. If you do not want end devices to be able to roam to the access point, use a different SSID for the access point master radio and the WAP station radio.

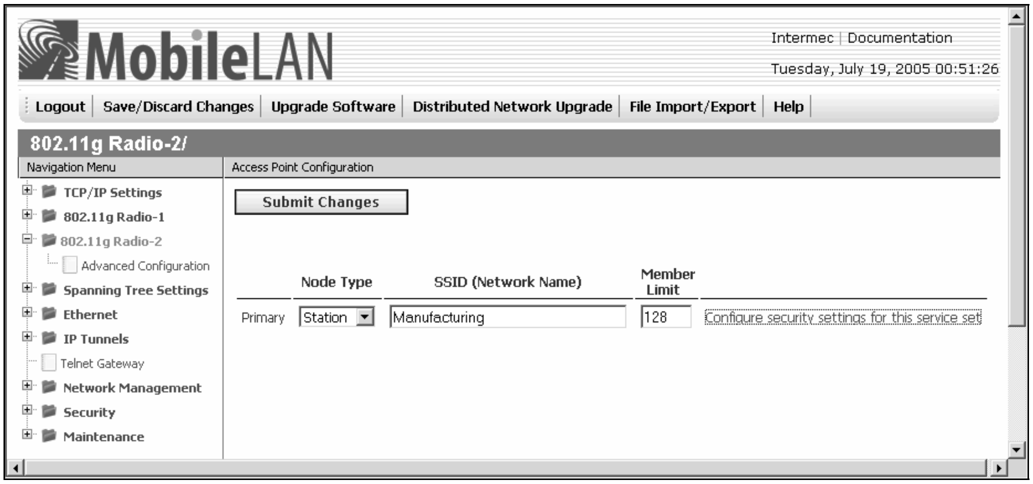
WAPs send data from end devices to the access points via wireless hops. Wireless hops are formed when data from end devices move from one access point to another access point through the radio ports. The master radio in the access point transmits hello messages, which allow the WAPs to attach to the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

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 on page 9.
2. Configure the LAN ID. For help, see “Configuring the Spanning Tree Parameters” on page 91.
3. Configure the station radio in the WAP to communicate with one of the master radio service sets in the access point:
   - **a** In the Navigation Menu, click the link corresponding to the station radio. The radio screen appears.



802.11g Radio-2/

	Node Type	SSID (Network Name)	Member Limit
Primary	Station	Manufacturing	128

b In the Primary service set **Node Type** field, choose **Station**.

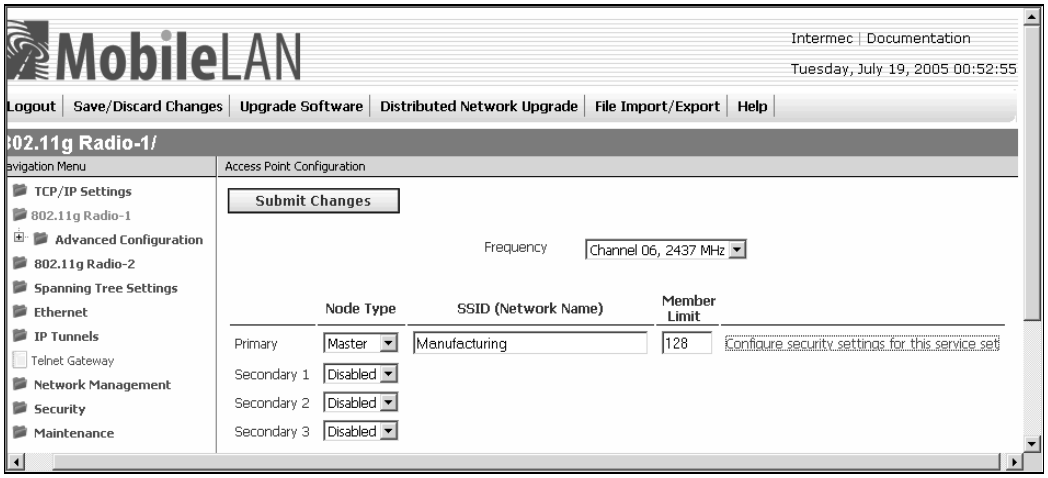
c In the Primary service set **SSID (Network Name)** field, type the SSID that matches the SSID of the access point radio service set (Step 1). In this example, the SSID is Manufacturing.

d Click **Submit Changes** to save your changes. The screen updates.

4 Configure a WAP master radio service set to communicate with the end device radios.

Note: If you do not want the end devices to be able to roam to the access point, you must configure the WAP master radio service set and the end device radios with a unique SSID.

a In the Navigation Menu, click the link corresponding to the WAP master radio. The radio screen appears.



:02.11g Radio-1/

Frequency: Channel 06, 2437 MHz

	Node Type	SSID (Network Name)	Member Limit
Primary	Master	Manufacturing	128
Secondary 1	Disabled		
Secondary 2	Disabled		
Secondary 3	Disabled		

b In the **Frequency** field, choose the radio frequency of your wireless network.

c In the Primary service set **Node Type** field, choose **Master**.

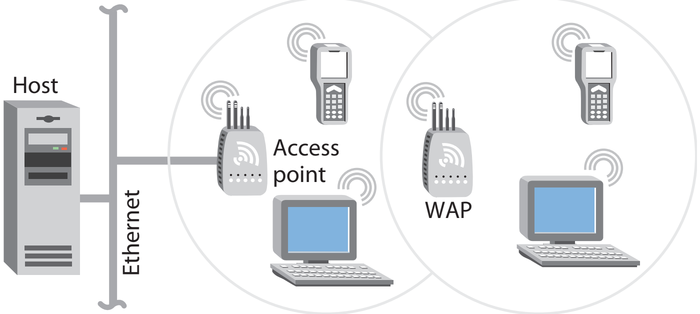
d In the Primary service set **SSID (Network Name)** field, type the SSID that matches the SSID of the end device radios. In this example, the SSID is Manufacturing.

e Click **Submit Changes** to save your changes.

5 Configure the access point to be a root access point. For help, see "About the Primary LAN and the Root Access Point" on page 87.

6 Click **Submit Changes** to save your changes. To activate your changes, in the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 30.

Example - Configuring an 802.11g WAP With Roaming End Devices



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

Configuring the 802.11g Access Point and WAP Parameters

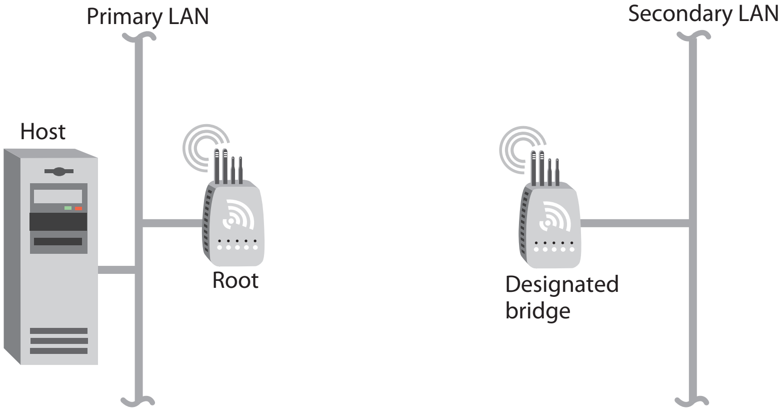
Screen	Parameter	Access Point 802.11g	WAP 802.11g Radio-1	WAP 802.11g Radio-2
802.11g Radio	Node Type	Master	Master	Station
	SSID	Manufacturing	Manufacturing	Manufacturing
Spanning Tree Settings	LAN ID	11	11	11
	Root Priority	5	0	(not applicable)
	Ethernet Bridging Enabled	Checked	Checked	(not applicable)

You need to configure the wireless end devices to have the same SSID (Manufacturing), LAN ID (11), and frequency as the WAP master radio (802.11g Radio-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.

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.

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.

How many radios do you need in each access point?

- If you have an 802.11g network and the access points are simply acting as point-to-point bridges, each access point only needs one radio.
- If you have an 802.11g network and you want the designated bridge to also communicate with wireless end devices (point-to-multipoint), the designated bridge must have two radios. The designated bridge master radio must match the end device radios, and the station radio must match the root master radio.

Important Note: Currently, a designated bridge cannot bridge to another secondary LAN. If it has two radios, it can communicate to a WAP or wireless end devices. If you need to bridge to another secondary LAN, you must use two access points.

Note: 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 root priority to 0 and the secondary LAN bridge priority to a number other than 0.

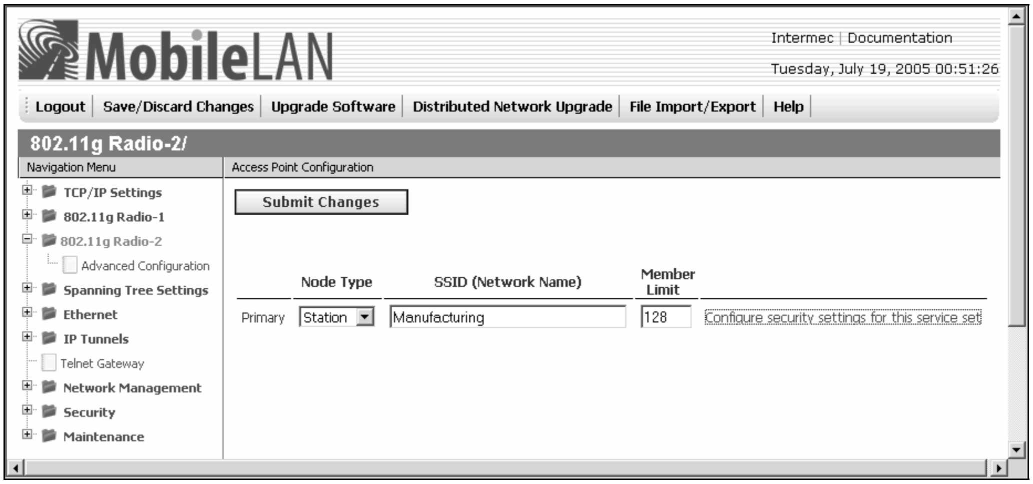
You may also need to adjust the flooding parameters. Here are some recommendations:

- If there are no end devices on the secondary LAN, the bridge on the secondary LAN can use the default flooding settings. The **Secondary LAN Flooding** parameter is disabled.
- If there are end devices on the secondary LAN, the bridge on the secondary LAN should have **Secondary LAN Flooding** parameter set to **Multicast**. If you also want unicast flooding, you can set this parameter to **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 Flooding** parameter set to **Universal**. This setting ensures that all ARP requests and multicast traffic is distributed through a second or third hop.

To install a point-to-multipoint bridge

1. Follow the instructions for installing a simple wireless network on page 9.
2. Configure the LAN ID. For help, see “Configuring the Spanning Tree Parameters” on page 91.
3. Configure one of the master radio service sets in the designated bridge on the secondary LAN to communicate with the end device radios.
4. Configure the station radio in the designated bridge to communicate with one of the master radio service sets in the point-to-point bridge on the primary LAN.

   a In the Navigation Menu, click the link corresponding to the station radio. The radio screen appears.



Tuesday, July 19, 2005 00:51:26

802.11g Radio-2/

Access Point Configuration

	Node Type	SSID (Network Name)	Member Limit
Primary	Station	Manufacturing	128

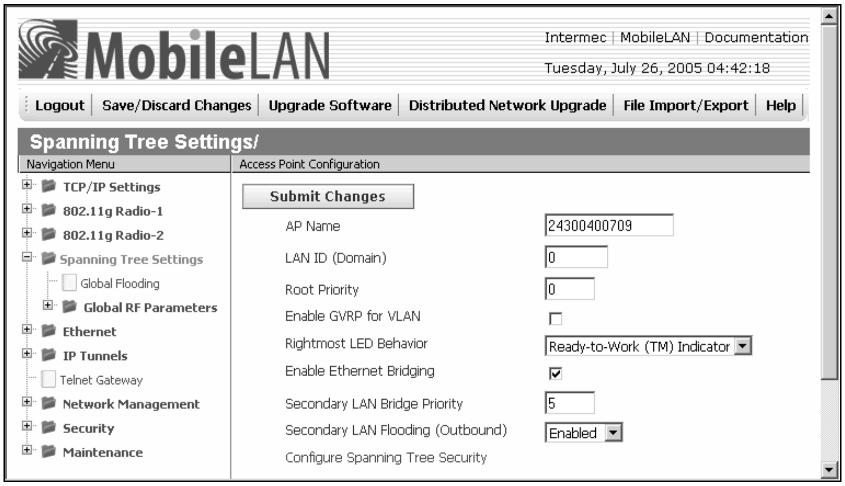
b In the Primary service set **Node Type** field, choose **Station**.

c In the Primary service set **SSID (Network Name) field**, type the SSID that matches the SSID of the root access point radio service set (Step 1). In this example, the SSID is Manufacturing.

d Click **Submit Changes**. The screen updates.

5 Configure the spanning tree settings for the designated bridge:

a In the Navigation Menu, click **Spanning Tree Settings**. The Spanning Tree Settings screen appears.



Tuesday, July 26, 2005 04:42:18

Spanning Tree Settings/

Access Point Configuration

AP Name: 24300400709
LAN ID (Domain): 0
Root Priority: 0
Enable GVRP for VLAN: ☐
Rightmost LED Behavior: Ready-to-Work (TM) Indicator
Enable Ethernet Bridging: ☑
Secondary LAN Bridge Priority: 5
Secondary LAN Flooding (Outbound): Enabled

b In the **Root Priority** field, enter **0**.

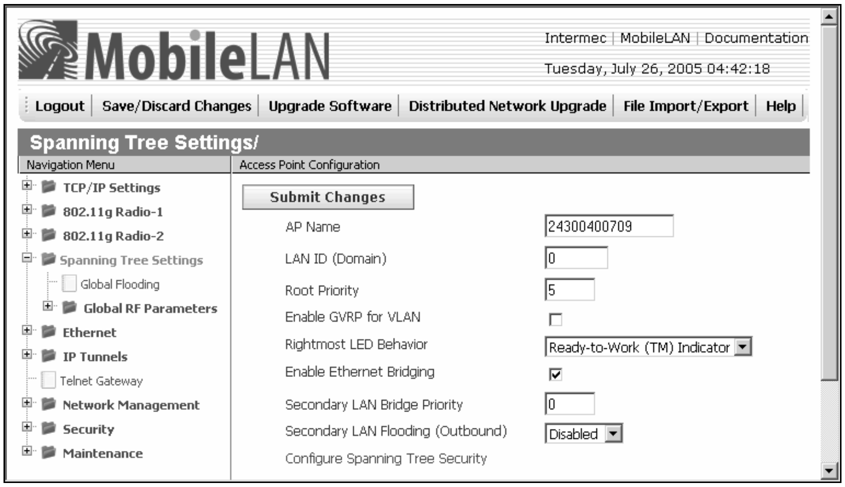
c In the **Secondary LAN Bridge Priority** field, enter a number other than 0.

d In the **Secondary LAN Flooding** field, choose **Enabled**.

6 Click **Submit Changes** to save your changes. To activate your changes, in the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see “Saving Configuration Changes” on page 30.

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

a In the Navigation Menu, click **Spanning Tree Settings**. The Spanning Tree Settings screen appears.



AP Name	24300400709
LAN ID (Domain)	0
Root Priority	5
Enable GVRP for VLAN	☐
Rightmost LED Behavior	Ready-to-Work (TM) Indicator
Enable Ethernet Bridging	☑
Secondary LAN Bridge Priority	0
Secondary LAN Flooding (Outbound)	Disabled
Configure Spanning Tree Security	

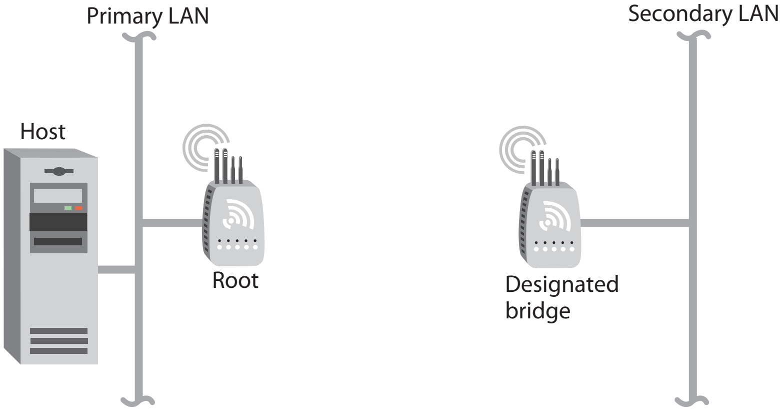
b In the **Root Priority** field, enter a number other than 0.

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

d In the **Secondary LAN Flooding** field, choose **Disabled**.

8 Click **Submit Changes** to save your changes. To activate your changes, in the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 30.

Example - Configuring an 802.11g Bridge



In this example, each access point only has one 802.11g 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 802.11g Point-to-Point Bridges Parameters

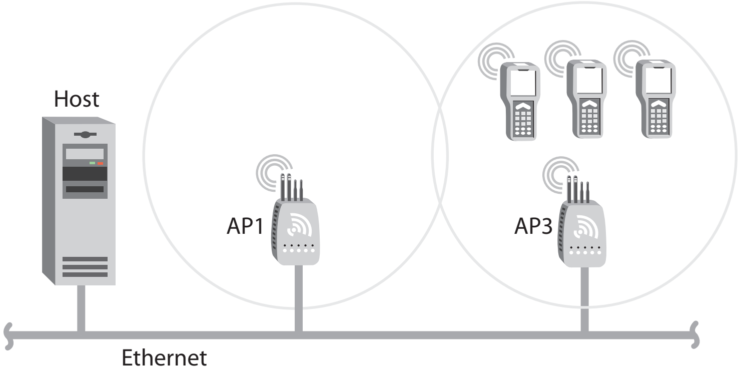
Screen	Parameter	Bridge Primary LAN (Root)	Bridge Secondary LAN (Designated Bridge)
802.11g Radio	Node Type	Master	Station
	SSID	Manufacturing	Manufacturing
Spanning Tree Settings	LAN ID	0	0
	Root Priority	5	0
	Ethernet Bridging Enabled	Checked	Checked
	Secondary LAN Bridge Priority	0	1
	Secondary LAN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

Intermec recommends that you always implement some type of security.

Using Dual Radio Access Points for Redundancy

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.



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 on page 13.

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 can use:

- the MobileLAN access Utility v2.0 (or later), but you need to know the access point MAC address. You can download this utility from the Intermec web site. This utility must be installed on a PC that is on the same Ethernet segment and subnet as (or must be communicating wirelessly with) the access point. For help, see the next section, "Using the MobileLAN access Utility."
- a communications program, such as HyperTerminal, which also configures other parameters. This program must be installed on a PC with an open serial port. For help, see "Using a Communications Program" on page 23.

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

Note: If you are setting an IPv6 address, you must use a communications program. For help, see "Using a Communications Program" on page 23.

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

- set the initial IPv4 address for the access point. This utility eliminates the need to serially connect a PC to the access point to configure an 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" on page 181.
- recover a failed access point. For help, see the online help and "Recovering a Failed Access Point" on page 197.
- upgrade the access point software. For help, see the online help and "Upgrading the Access Points" on page 200.

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 a PC that is running Windows 95-OSR2/98SE/ME or Windows NT4/2000/XP.

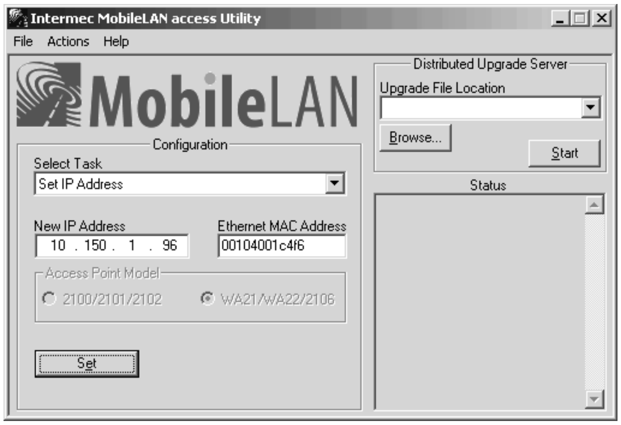
Note: You need to install the MobileLAN access Utility on a PC that is on the same IP subnet as the access point. Or you can install it on a PC that is communicating wirelessly (configured to Intermec's default radio settings) to the access point. Before you use the utility, you must have an active radio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

To use the MobileLAN access Utility

1 Use a web browser to navigate to www.intermec.com. From the Service & Support menu, click Downloads. Choose Wireless: MobileLAN access Utility to download the MobileLAN access Utility.

2 Extract the .zip file, double-click the .exe file, and then follow the instructions that appear on your screen.

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



Select Task: Set IP Address

New IP Address: 10 . 150 . 1 . 96

Ethernet MAC Address: 00104001c4f6

○ 2100/2101/2102 ● WA21/WA22/2106

Upgrade File Location:

4 In the **Select Task** field, 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 IPv4 or an IPv6 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 order this cable, contact your local Intermec representative.

To use a communications program

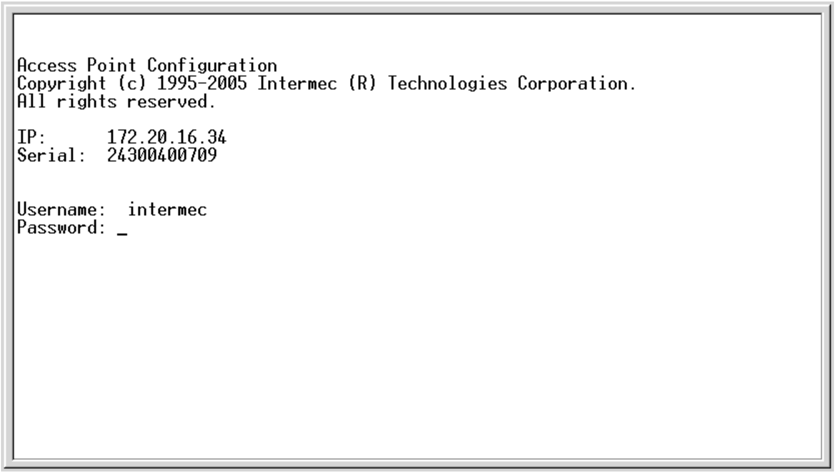
1 Use the RS-232 null-modem cable to connect the serial port on the access point to a serial port on your PC. You may need to remove the serial port plug.

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.



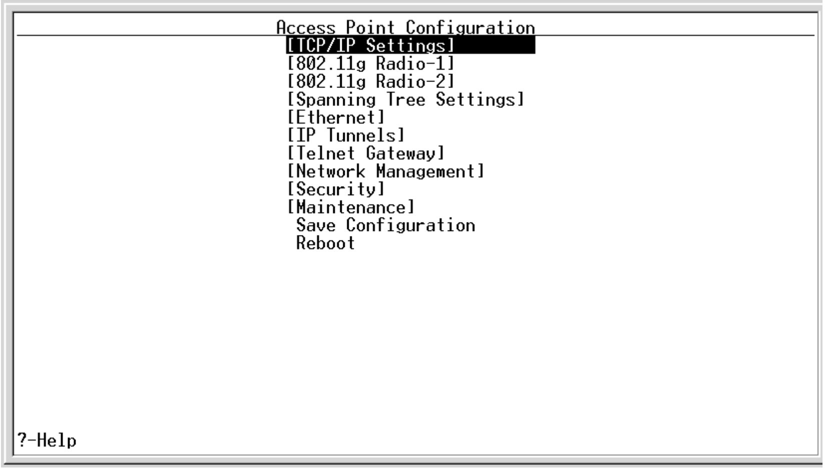
```
Access Point Configuration
Copyright (c) 1995-2005 Intermec (R) Technologies Corporation.
All rights reserved.

IP:       172.20.16.34
Serial:  24300400709


Username:  intermec
Password: _
```

5 In the **Username** field type the default user name Intermec, and then press **Enter**. The user name is case sensitive.

6 In the Password field type the default password Intermec, and then press **Enter**. The password is case sensitive. The Access Point Configuration menu appears.



```
                          Access Point Configuration
                           [TCP/IP Settings]
                           [802.11g Radio-1]
                           [802.11g Radio-2]
                           [Spanning Tree Settings]
                           [Ethernet]
                           [IP Tunnels]
                           [Telnet Gateway]
                           [Network Management]
                           [Security]
                           [Maintenance]
                            Save Configuration
                            Reboot







?-Help
```

7 Press **Enter** to access the **TCP/IP Settings** menu.

8 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 IPv4 or IPv6 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 <Use DHCP 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.

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

10 Choose **Save Configuration**.

11 Choose **Reboot**.

When the access point is done rebooting, you are 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. Remotely accessing the access point using other browsers may provide unpredictable results. 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

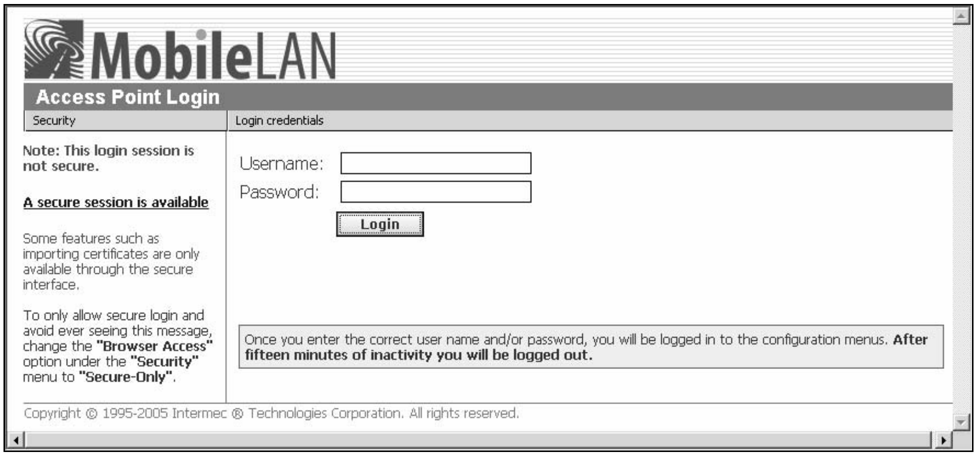
1 Determine the IP address of the access point. If a DHCP server assigned the IP address, you must get the IP address from the DHCP server.

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.



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"**.

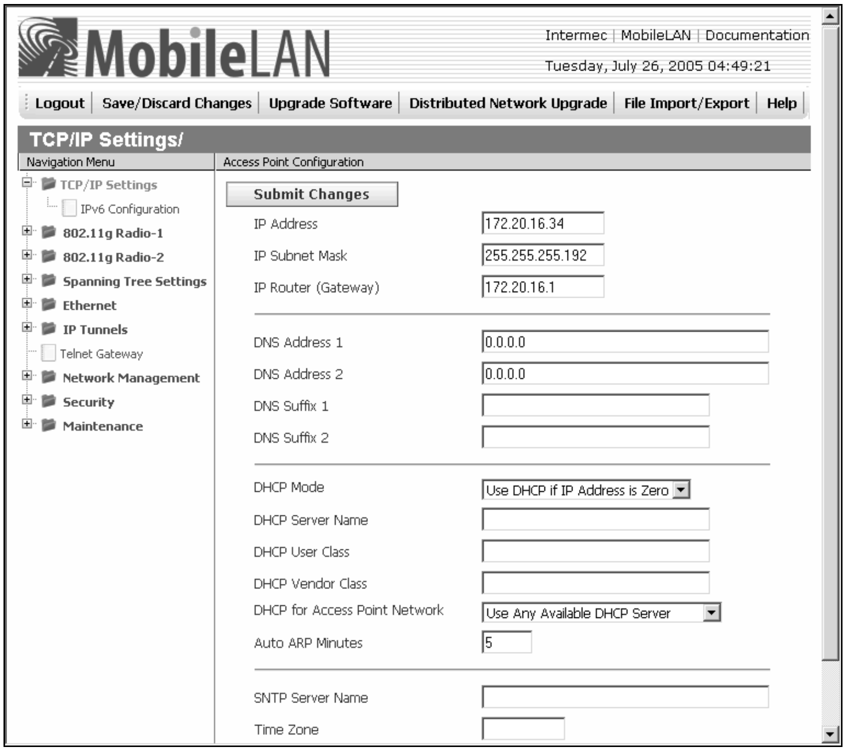
Once you enter the correct user name and/or password, you will be logged in to the configuration menus. **After fifteen minutes of inactivity you will be logged out.**

Copyright © 1995-2005 Intermec ® Technologies Corporation. All rights reserved.

4 If necessary, enter a user name and a password. The default user name is Intermec and the default password is Intermec. You can define a user name and password. For help, see “Setting Up Logins” on page 126.

Or you may want to log in to a secure session.

5 Click **Login**. The TCP/IP Settings screen appears.



Tuesday, July 26, 2005 04:49:21

IP Address	172.20.16.34
IP Subnet Mask	255.255.255.192
IP Router (Gateway)	172.20.16.1
DNS Address 1	0.0.0.0
DNS Address 2	0.0.0.0
DNS Suffix 1	
DNS Suffix 2	
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	
DHCP User Class	
DHCP Vendor Class	
DHCP for Access Point Network	Use Any Available DHCP Server
Auto ARP Minutes	5
SNTP Server Name	
Time Zone	

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 set the initial 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.

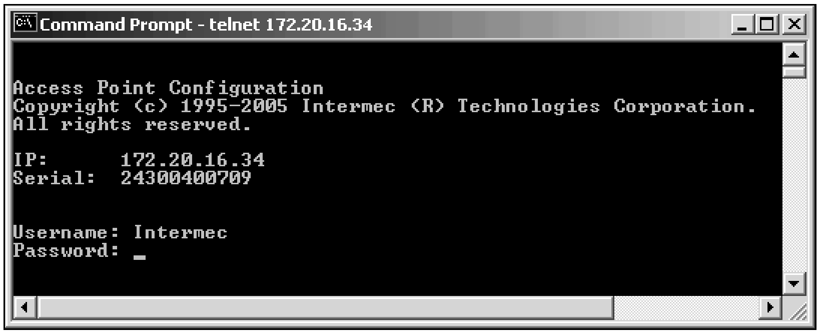
To use a telnet session

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.



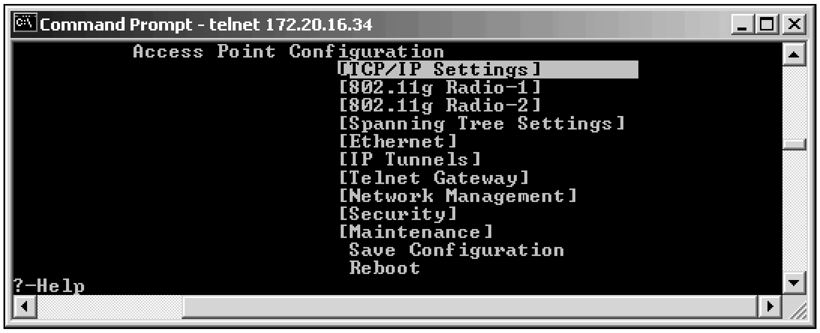
```
Access Point Configuration
Copyright (c) 1995-2005 Intermec (R) Technologies Corporation.
All rights reserved.

IP:       172.20.16.34
Serial:   24300400709


Username: Intermec
Password: _
```

3 Press **Enter**.

4 If necessary, enter the user name and press **Enter**. Then, enter the password and press **Enter**. The default user name is Intermec and the default password is Intermec. You can define a user name and password. For help, see “Setting Up Logins” on page 126. The Access Point Configuration menu appears.



```
          Access Point Configuration
                           [TCP/IP Settings]
                           [802.11g Radio-1]
                           [802.11g Radio-2]
                           [Spanning Tree Settings]
                           [Ethernet]
                           [IP Tunnels]
                           [Telnet Gateway]
                           [Network Management]
                           [Security]
                           [Maintenance]
                            Save Configuration
                            Reboot
?-Help
```

Setting the Clock

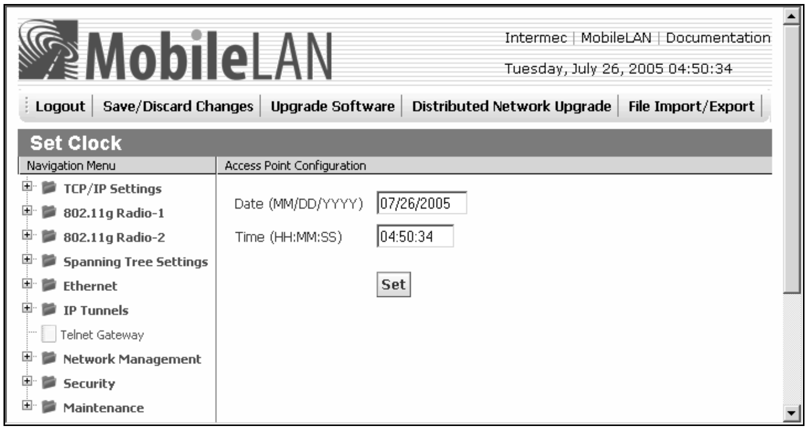
The access point has a date and time clock that you can configure. You may also want to configure the **Time Zone** field so that users know the origination of any time stamps.

You can also configure the root access point to periodically query an NTP (Network Time Protocol) server or a SNTP (Simple Network Time Protocol) server to set its clock. Then, the root access point acts as an SNTP server to all other access points in the spanning tree and periodically updates their clocks. NTP is widely used to synchronize computer clocks in the Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet, and adjust the local clock in each participating subnet peer. SNTP is a simplified access strategy for servers and clients. SNTP is designed to operate in a dedicated server configuration including an integrated radio clock.

Note: You must configure an NTP or an SNTP server if you want the access point to validate certificate dates.

To set the clock

1 In the access point header, click the date and time link. The Set Clock screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Tuesday, July 26, 2005 04:50:34
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export
Set Clock
Navigation Menu
TCP/IP Settings
802.11g Radio-1
802.11g Radio-2
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Set

Date (MM/DD/YYYY) 07/26/2005

Time (HH:MM:SS) 04:50:34

2 In the **Date** field, enter the current date.

3 In the **Time** field, enter the current time.

4 Click **Set**. The clock is immediately set to the correct date and time.

5 (Optional) Configure a time zone stamp.

a In the Navigation Menu, click **TCP/IP Settings**. The TCP/IP Settings screen appears.

b In the **Time Zone** field, type:

xxxn[*yyy*]

where:

xxx is the time zone (for example, PST)

n is the offset from Greenwich Mean Time (GMT)

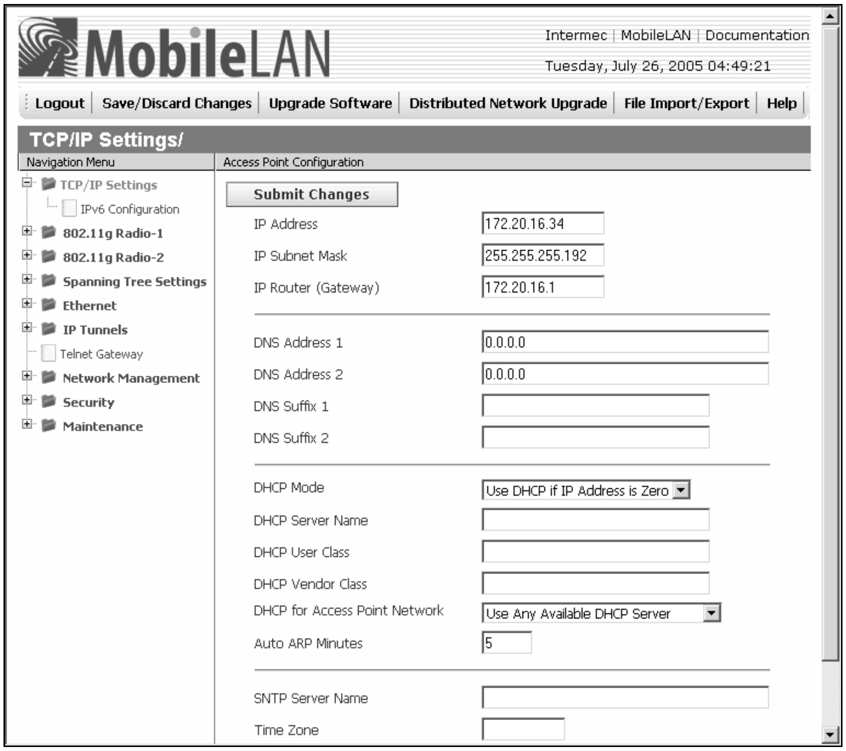
yyy is the optional identifier for daylight savings time (for example PDT)

Note: Even if you use the optional identifier, you must change the offset each time daylight savings time begins and ends.

c 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 the next section.

To configure an NTP or SNTP server

1 In the Navigation Menu, click **TCP/IP Settings**. The TCP/IP Settings screen appears.



Tuesday, July 26, 2005 04:49:21

TCP/IP Settings/

IP Address 172.20.16.34

IP Subnet Mask 255.255.255.192

IP Router (Gateway) 172.20.16.1

DNS Address 1 0.0.0.0

DNS Address 2 0.0.0.0

DNS Suffix 1

DNS Suffix 2

DHCP Mode Use DHCP if IP Address is Zero

DHCP Server Name

DHCP User Class

DHCP Vendor Class

DHCP for Access Point Network Use Any Available DHCP Server

Auto ARP Minutes 5

SNTP Server Name

Time Zone

2 In the **SNTP Server Name** field, enter an IP address or a DNS name of an NTP or SNTP server.

3 In the **Time Zone** field, type:

xxxn[*yyy*]

where:

xxx is the time zone (for example, PST)

n is the offset from Greenwich Mean Time (GMT)

yyy is the optional identifier for daylight savings time (for example PDT)

Note: Even if you use the optional identifier, you must change the offset each time daylight savings time begins and ends.

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 the next section.

Saving Configuration Changes

As you are configuring the access point, you may want to move your changes to the saved or active configuration file. As you hover over fields, a text box shows you the saved value, active value, and default value.

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.

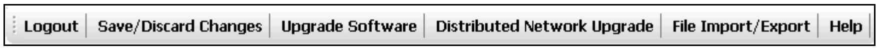
Access Point Configuration Files

Configuration File	Description
Default	This configuration file is the factory default configuration. For help, see “Restoring the Access Point to the Default Configuration” on page 181.
Current	When you click **Submit Changes**, the access point updates the current configuration file. The access point does not change the saved or active configuration file. You can see a list of pending changes when you click **Save/Discard Changes**.
Saved	When you click **Save/Discard Changes** > **Save Changes without Reboot**, the access point copies the current configuration file to the saved configuration file. Having separate files for the saved and active configurations lets you make changes while the access point is running without interrupting communication.
Active	When you click **Save/Discard Changes** > **Save Changes and Reboot**, the access point copies the saved configuration file to the active configuration file. The active configuration file is the file that the access point uses.

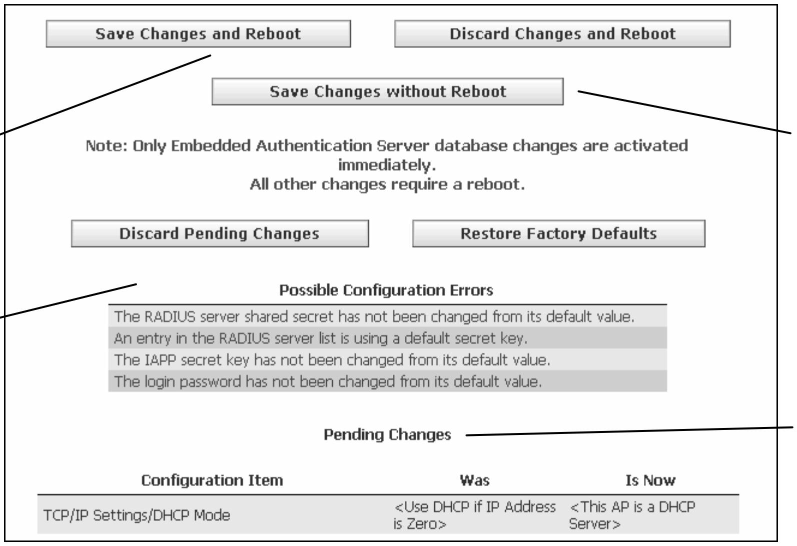
Note: For the 802.11g radio, some of the advanced configuration parameters let you immediately activate the changes without rebooting the access point. For instructions, see “Applying Hot Settings” on page 84.

Using a Web Browser Interface

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



This screen appears.



Note: Only Embedded Authentication Server database changes are activated immediately.
All other changes require a reboot.

Possible Configuration Errors

The RADIUS server shared secret has not been changed from its default value.
An entry in the RADIUS server list is using a default secret key.
The IAPP secret key has not been changed from its default value.
The login password has not been changed from its default value.

Pending Changes

Configuration Item	Was	Is Now
TCP/IP Settings/DHCP Mode	<Use DHCP if IP Address is Zero>	<This AP is a DHCP Server>

Click to use your new configuration now.

Lists possible configuration changes you may still need to make.

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

Lists configuration changes you have made.

2 Resolve any error messages listed under the heading, “Possible Configurations Errors.” For help, see “Using the Configuration Error Messages” on page 183.

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

4 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 configuration and continues to run its active configuration. You need to reboot the access point when you want the saved configuration to become the active configuration.

To discard the changes

- Click **Discard Pending Changes**.

Using a Telnet Session

1 From the Access Point Configuration menu, choose Save Configuration.

2 Choose Reboot to reboot the access point and immediately use your new active configuration.

2 Installing the Access Points

This chapter explains how to install the MobileLAN access WA2XG family of access points 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 WA21G
- Installing the WA22G
- Connecting to your fiber optic network
- Connecting power over Ethernet
- External antenna placement guidelines

Installation Guidelines

Intermec recommends that you have an Intermec-certified RF specialist conduct a site survey to determine the ideal locations for all your Intermec wireless network devices. 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” on page 43.

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.

Microwave Ovens

Microwave ovens operate in the same frequency band as 802.11g 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.

Cordless Telephones

If you have an 802.11g 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 five channels apart, such as channels 1, 6, and 11.

Installing the WA21G

You can place the WA21G horizontally or vertically on a desk or counter. If you want to mount the WA21G 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 IP54 environmental rating, you must mount the WA21G in either the horizontal or vertical position. If you order the WA21G with the heater option, you must use one of the mounting bracket kits to mount the WA21G with the LEDs facing down.

A variety of external antenna options are available for the WA21G. 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” on page 235.

To install the WA21G

1. Attach the antenna or antennas. For more information, see “External Antenna Placement Guidelines” on page 43.
2. Mount the WA21G. For help, see the *MobileLAN access WA21G Quick Start Guide* and the instructions that shipped with the bracket kit.
3. Connect the WA21G to your wired LAN (unless you are using it as a WAP). For help, see “Connecting the WA21G to Your Wired LAN” on page 36.
4. Connect the WA21G to power. For help, see “Connecting the WA21G to Power” on page 36.

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

Connecting the WA21G to Your Wired LAN

Unless you are using the WA21G as a WAP, you need to connect it to your Ethernet or fiber optic network. For help connecting the WA21G to your fiber optic network, see "Connecting to Your Fiber Optic Network" on page 38.

To connect the WA21G to the Ethernet network

- Attach one end of the Ethernet cable to the 10BaseT/100BaseTx port on the WA21G and attach the other end to your Ethernet network.

  Or, if you are using power over Ethernet, attach one end of the Ethernet cable to the 10BaseT/100BaseTx port on the WA21G and attach the other end to a MobileLAN power bridge, a Cisco power bridge or another 802.3af-compliant power bridge.

Connecting the WA21G to Power

The WA21G can be powered using the power over Ethernet (POE) interface. The POE interface is compatible with the MobileLAN power bridge, a Cisco power bridge, or another 802.3af-compliant power bridge. For help, see "Connecting Power Over Ethernet" on page 42 and the documentation that came with your power bridge.

Or, the WA21G with the power port option can be powered from an AC power source. You can use a power cord to connect the WA21G directly from the power port to an AC power outlet.

Note: When both POE and AC are applied, the WA21G is redundantly powered and will continue to operate if one of the power sources fails.

To connect the WA21G power port to an AC power source

- Plug one end of the power cord into the power port on the WA21G and plug the other end into an AC power outlet. The access point boots as soon as you apply power.

Installing the WA22G

You can place the WA22G horizontally on a desk or counter. The WA22G also ships with a mounting bracket that lets you mount it vertically to a wall. Additional mounting options that you can use with the mounting bracket include a cubicle bracket that lets you mount the WA22G 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” on page 235.

To install the WA22G

1. Attach the antenna or antennas. For more information, see “External Antenna Placement Guidelines” on page 43.
2. Mount the WA22G. For help, see the *MobileLAN access WA22G Quick Start Guide* and the instructions that shipped with the bracket kit.
3. Connect the WA22G to your wired LAN (unless you are using it as a WAP). For help, see “Connecting the WA22G to Your Wired LAN and Power” in the next section.
4. Connect the WA22G to power. For help, see “Connecting the WA22G 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 WA22G to Your Wired LAN and Power

Unless you are using the WA22G as a WAP, you must connect it to your Ethernet or fiber optic network. For help connecting to your fiber optic network, see “Connecting to Your Fiber Optic Network” on page 38.

To connect the WA22G to your Ethernet network and to power, you must first connect it to a MobileLAN power bridge, a Cisco power bridge, or another 802.3af-power bridge. For help, see “Connecting Power Over Ethernet” on page 42 and the documentation that shipped with your power bridge.

Connecting to Your Fiber Optic Network

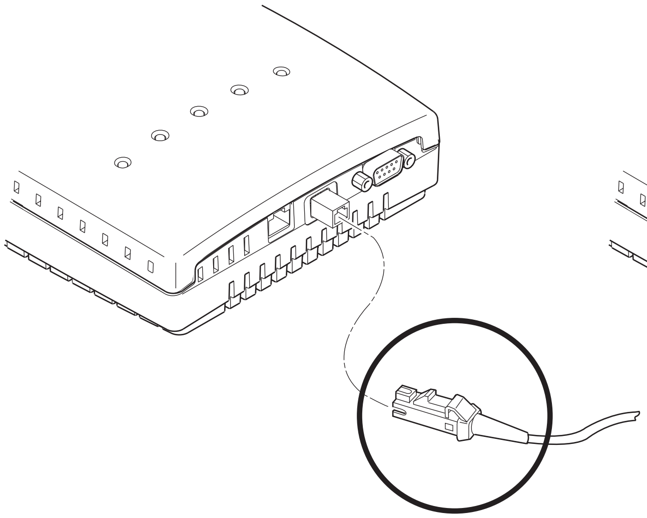
Using appropriate patch cords and an adapter (as described in the next section), you can connect your WA21G and WA22G to:

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

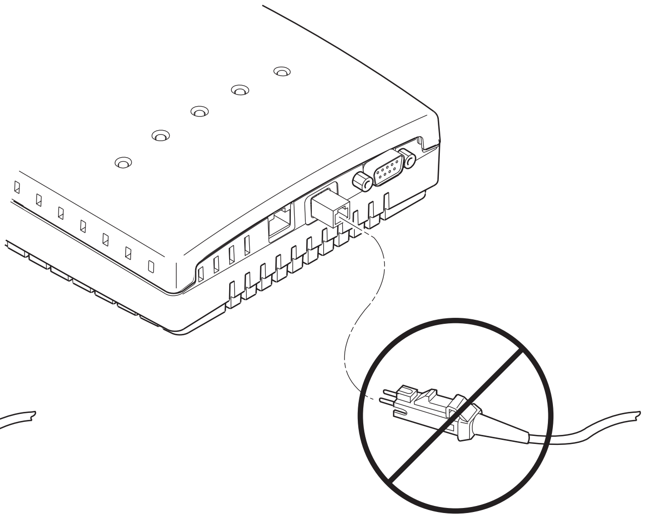
Using and Purchasing the Required Patch Cord and Adapter

To connect the access point to your fiber optic network, you must supply a patch cord and an adapter.

The access point fiber optic port consists of a male MT-RJ connector interface. Therefore, the patch cord must have a female MT-RJ connector that you insert into the access point fiber optic port.



Insert a **female** MT-RJ connector into the fiber optic port



Do not insert a **male** MT-RJ connector into the fiber optic port

Note: Inserting a male MT-RJ connector into the fiber optic port may result in unreliable operation because there is no internal mechanism to ensure the alignment of the fiber when using male-to-male connectors. Such a connection may temporarily provide some level of connectivity, despite a high level of signal loss. However, any movement of the cable or change in cable tension could cause complete loss of signal.

Both the connector at the other end of the patch cord and the adapter you select depend on the type of network to which the access point is connected: MT-RJ, SC, or ST.

Patch cords and adapters are available from many different manufacturers. For help choosing the proper patch cord and adapter, contact your local Intermec representative.

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

Connecting to an MT-RJ Network

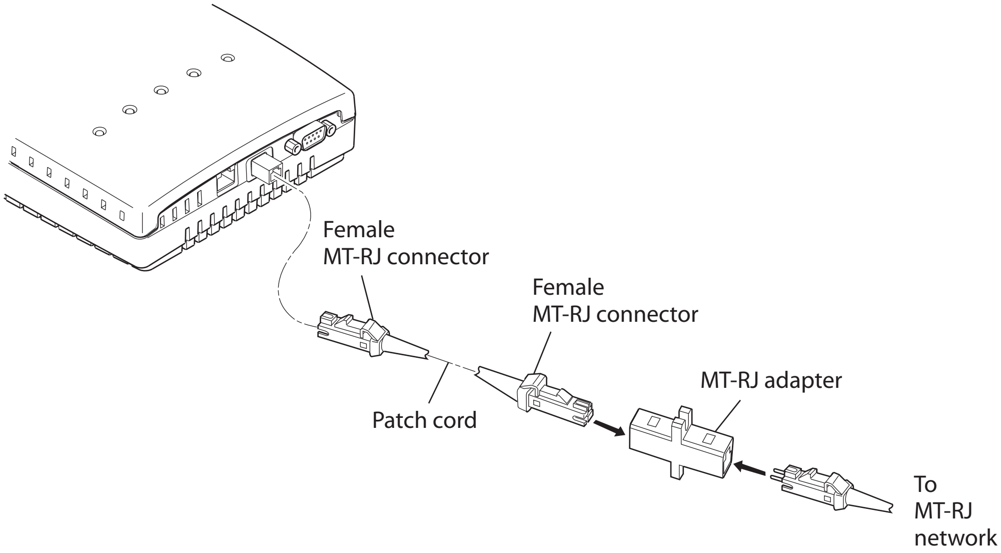
To connect to an MT-RJ network, you need:

- a patch cord with a female MT-RJ connector to insert into the access point's male MT-RJ fiber optic port, and another female MT-RJ connector to insert into the MT-RJ adapter.
- an adapter for connecting the patch cord to the 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 as shown in the next illustration.



Note: The patch cord shown above must connect to the access point with a female MT-RJ connector. For details, see "Using and Purchasing the Required Patch Cord and Adapter" on page 38.

Connecting to an SC Network

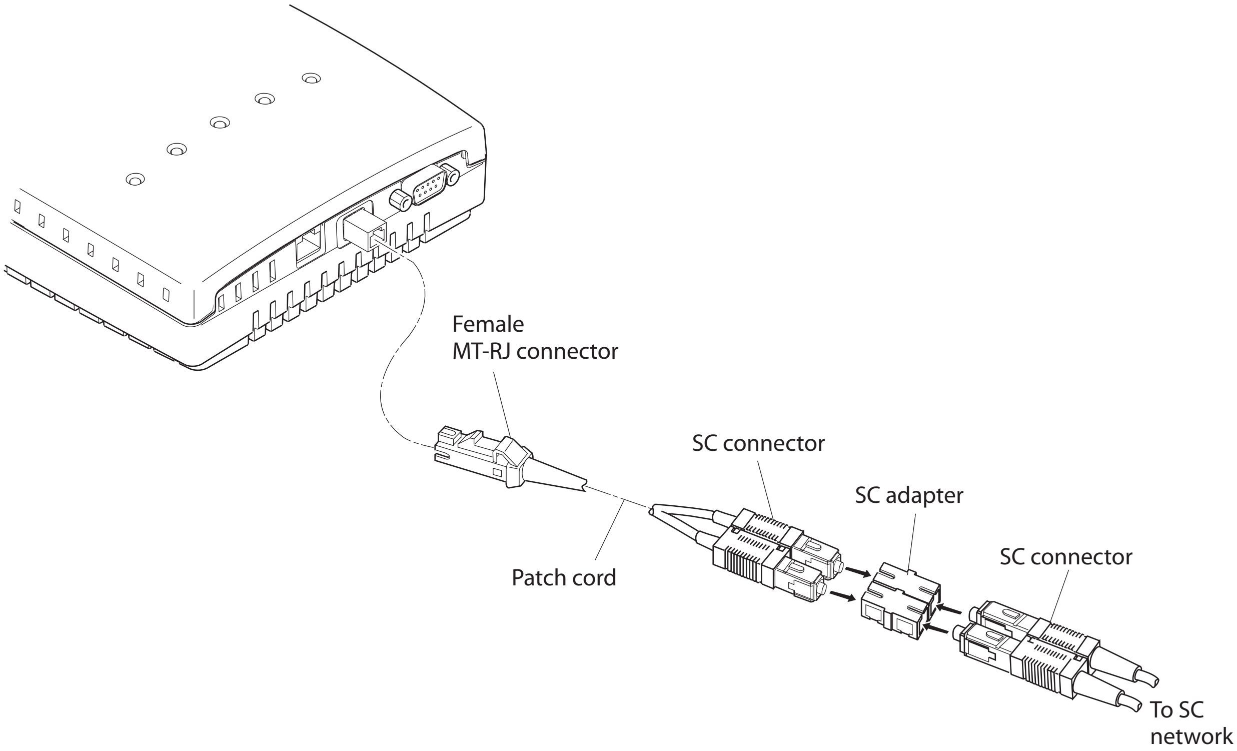
To connect to an SC network, you need:

- a patch cord with a female MT-RJ connector to insert into the access point's male MT-RJ fiber optic port, and an SC connector to insert into the SC adapter.
- an adapter for connecting the patch cord to an SC network.

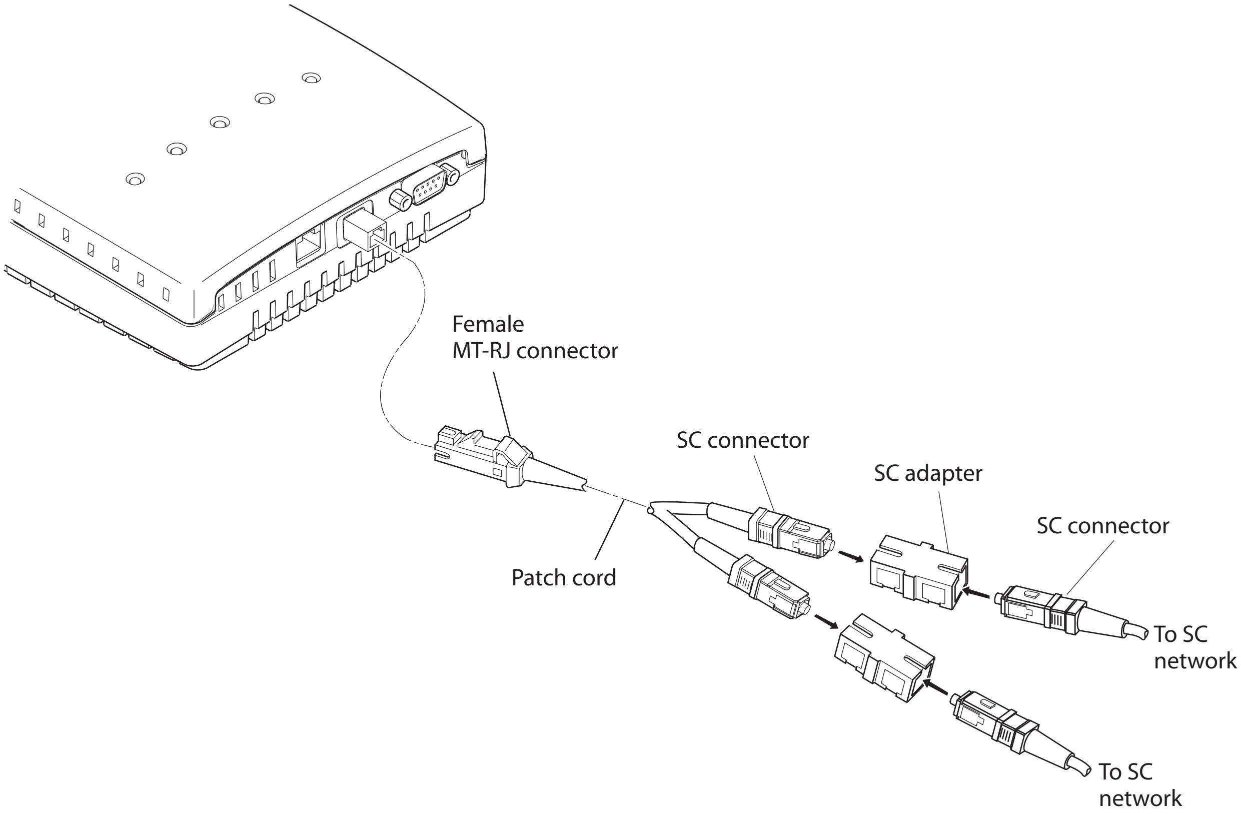
To connect to an SC network

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 two illustrations.



Note: The patch cord shown above must connect to the access point with a female MT-RJ connector. For details, see "Using and Purchasing the Required Patch Cord and Adapter" on page 38.



Note: The patch cord shown above must connect to the access point with a female MT-RJ connector. For details, see “Using and Purchasing the Required Patch Cord and Adapter” on page 38.

Connecting to an ST Network

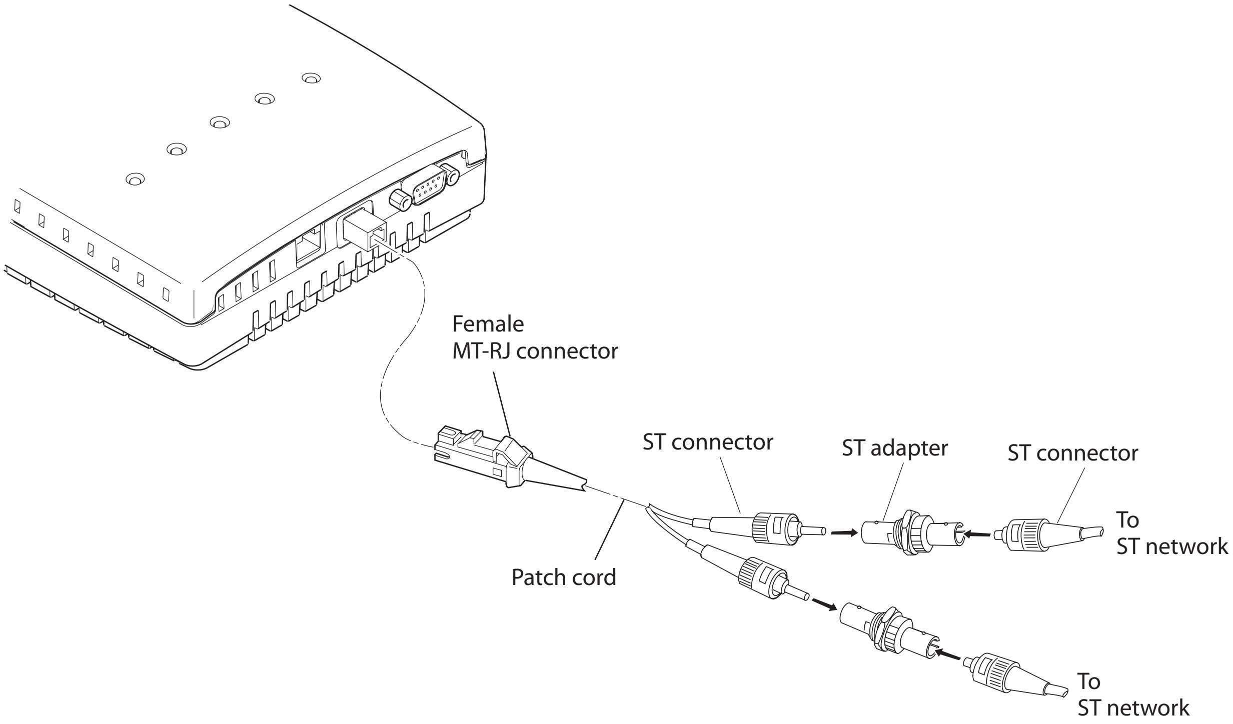
To connect to an ST network, you need:

- a patch cord with a female MT-RJ connector to insert into the access point’s male MT-RJ fiber optic port, and an ST connector to insert into the ST adapter.
- an adapter for connecting the patch cord to the ST network.

To connect to an ST network

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

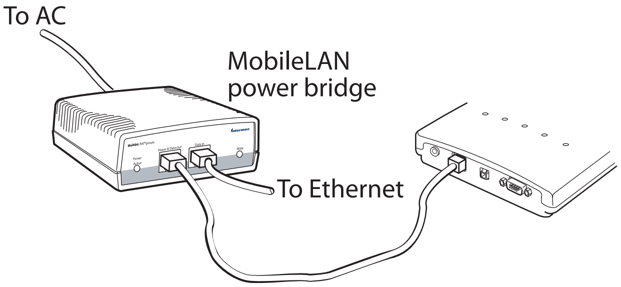
2 Connect the access point to your network as shown in the next illustration.



Note: The patch cord shown above must connect to the access point with a female MT-RJ connector. For details, see “Using and Purchasing the Required Patch Cord and Adapter” on page 38.

Connecting Power Over Ethernet

The WA22G is powered by power over Ethernet. The WA21G can be powered by AC power or by power over Ethernet or both. For all access points, you need a power bridge. For a list of the power bridges that Intermec sells, contact your local Intermec representative.



Connecting WA22G Using Power Over Ethernet: *This illustration shows how you connect the WA22G to the MobileLAN power bridge with a typical Ethernet cable to 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 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 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.
- Keep the line-of-sight between the antennas and wireless end devices clear of metal surfaces (like beams or girders) and large quantities of paper products.
- 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 802.11g Radios

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

Use antenna connectors 1 and 2 or 3 and 4 to attach antennas to the send/receive ports.

Recommended Antenna Separation for Antenna Diversity

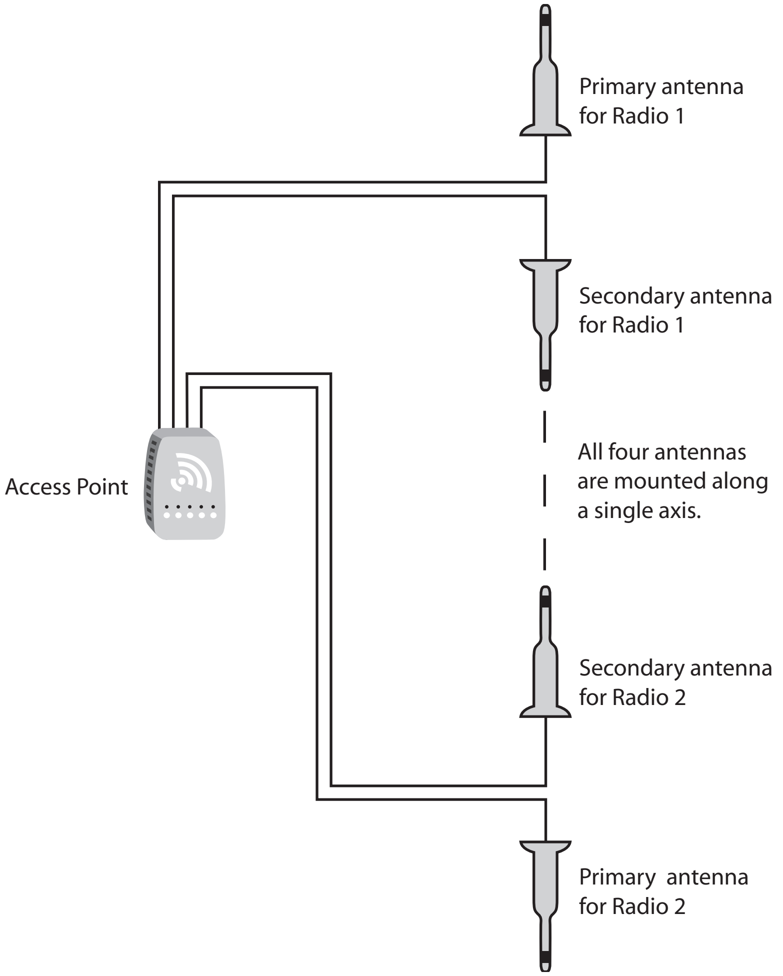
Location	Recommended Antenna Separation
Highly reflective warehouse environment	0.33 m (13 in) or 0.64 m (25 in)
Moderately reflective warehouse environment	0.64 m (25 in), 1.22 m (4 ft), or 1.83 m (6 ft)
Open/Office environment	1.22 m (4 ft) to 3.05 m (10 ft)

Positioning Antennas for Dual Radio Access Points

The recommendations in the previous table apply to omni antennas; if you are using directional antennas, you should increase the recommended separation between the antennas:

- If your access point has two 802.11g 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 802.11g radio (the other radio may be any radio), cable the antennas for the radio at least 3.05 m (10 ft) from the access point.

Positioning Stacked Antennas for Dual Radio Access Points



Using Stacked Antenna Positioning: *As an alternative to the physical separation of omni antennas, you can mount them along a single axis to minimize the antenna-to-antenna coupling.*

About Antenna Diversity for 802.11g Radios

Antenna diversity lets you attach two antennas to one radio to increase the odds of receiving a better signal on either of the antennas. 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 802.11g 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.

3 Configuring the Ethernet Network

This chapter explains how to configure the MobileLAN access WA2XG family of access points so that they communicate with your Ethernet network. This chapter explains:

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

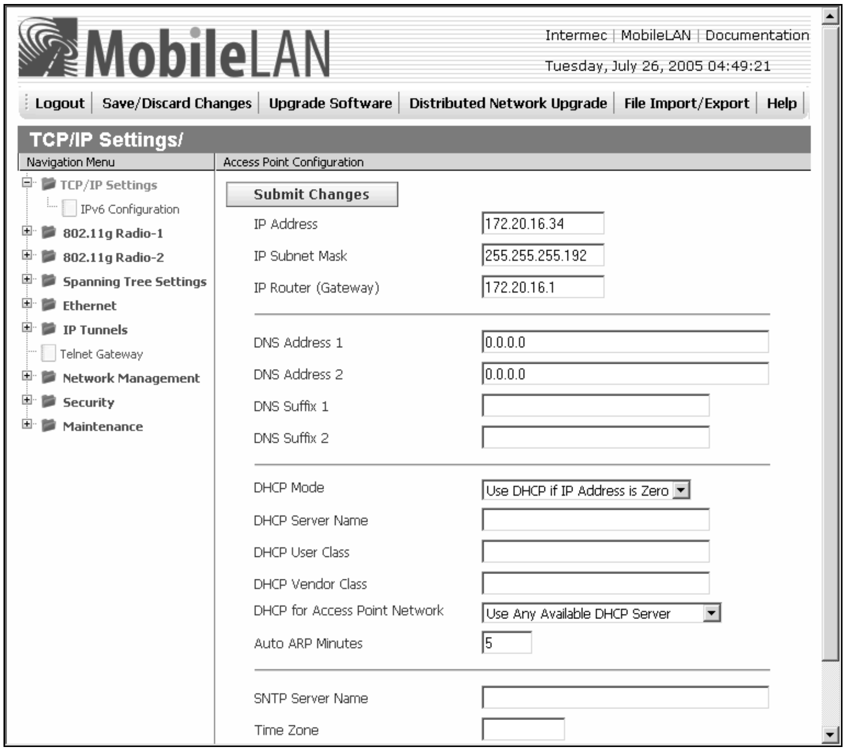
Configuring the TCP/IP Settings

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" on page 51. 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)" on page 21.

To configure the TCP/IP settings

1 In the Navigation Menu, click **TCP/IP Settings**. The TCP/IP Settings screen appears.



IP Address 172.20.16.34

IP Subnet Mask 255.255.255.192

IP Router (Gateway) 172.20.16.1

DNS Address 1 0.0.0.0

DNS Address 2 0.0.0.0

DNS Suffix 1

DNS Suffix 2

DHCP Mode Use DHCP if IP Address is Zero

DHCP Server Name

DHCP User Class

DHCP Vendor Class

DHCP for Access Point Network Use Any Available DHCP Server

Auto ARP Minutes 5

SNTP Server Name

Time Zone

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

3 If you are using IPv6 addresses, see "Using IPv6 Addresses" in the next section.

4 If you want to configure the access point as a DHCP server, see "Configuring the Access Point as a DHCP Server" on page 53.

5 If you want to configure the access point as a NAT server, see "About Network Address Translation (NAT)" on page 57.

6 If you want to configure the access point to send ARP requests, see “Configuring the Access Point to Send ARP Requests” on page 58.

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” on page 30.

TCP/IP Settings Descriptions

Parameter	Explanation
IP Address	Enter the IP address of the access point. In an IPv4 network, the IP address has the form *x.x.x.x*, where *x* is a number from 0 to 255. For help setting up IPv6 addresses, see “Using IPv6 Addresses” in the next section.
IP Subnet Mask	Enter the subnet mask that matches the other devices in your network. In an IPv4 network, the subnet mask has the form *x.x.x.x*, where *x* is a number from 0 to 255. For help setting up IPv6 addresses, see “Using IPv6 Addresses” in the next section. If you use DHCP to obtain an IP address for this access point, the subnet mask that is obtained from DHCP will supercede this one.
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. In an IPv4 network, the IP address has the form *x.x.x.x*, where *x* is a number from 0 to 255. For help setting up IPv6 addresses, see “Using IPv6 Addresses” in the next section.
DNS Address 1	Enter the IP address of a domain name server that the access point uses to resolve DNS names. If this access point is a DHCP server, this DNS address 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 the access point uses to resolve DNS names if the DNS server at DNS Address 1 is not responding. If this access point is a DHCP server, this DNS address will be distributed to DHCP clients.
DNS Suffix 1	Enter a domain name suffix that will be appended to DNS names that cannot be resolved. If the access point is a DHCP server, this is the only DNS suffix that is delivered to DHCP clients. For example, enter a suffix of UVW.COM. When you try to resolve ABC, the DNS will look for ABC.UVW.COM.
DNS Suffix 2	Enter a domain name suffix that will be appended to DNS names that cannot be resolved either by themselves or using DNS suffix 1. For example, enter a suffix of XYZ.COM. When you try to resolve ABC, the DNS will first look for ABC.UVW.COM and then it will look for ABC.XYZ.COM.

Using IPv6 Addresses

The access point supports IPv6 addresses. If your network supports using IPv6 addresses, you can configure the access point with an IPv6 address, forward packets from wireless end devices that have IPv6 addresses, and participate in VLANs using IPv6 addresses.

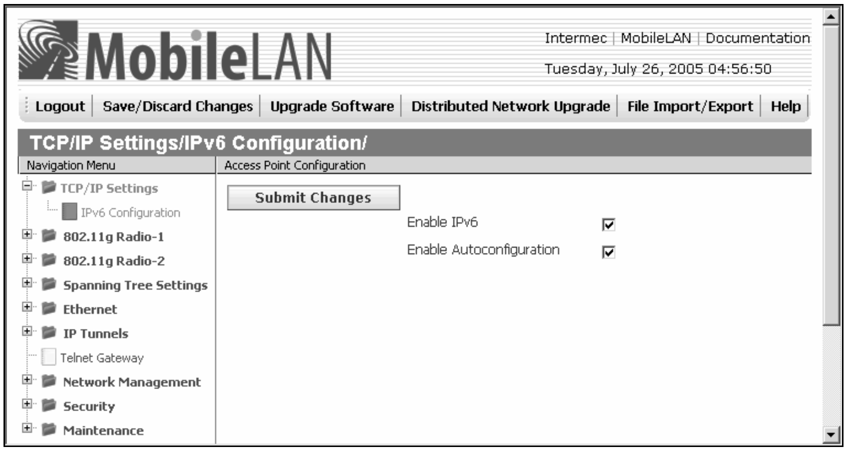
Note: You cannot use IPv6 addressing with the MobileLAN access Utility, IP tunnels, and SNMP.

The access point also supports networks that use both IPv4 and IPv6 addresses. In this case, you may find it helpful to check the **Enable Autoconfiguration** check box and the access point will generate its own TCP/IP settings or use whatever settings the router gives it. If you clear this check box, you need to enter an IP address, subnet mask and router using the IPv6 format.

To use IPv6 addresses

1 In the Navigation Menu, click **TCP/IP Settings** > **IPv6 Configuration**. The IPv6 Configuration screen appears.

2 Check the **Enable IPv6** check box and then click **Submit Changes**.


MobileLAN
Intermec | MobileLAN | Documentation
Tuesday, July 26, 2005 04:56:50
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
TCP/IP Settings/IPv6 Configuration/
Navigation Menu
Access Point Configuration
TCP/IP Settings
IPv6 Configuration
802.11g Radio-1
802.11g Radio-2
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

Enable IPv6 ☑

Enable Autoconfiguration ☑

3 Check the **Enable Autoconfiguration** check box to allow the access point to generate its own TCP/IP settings or use whatever settings the router gives it.

Or, to enter IPv6 parameters, clear the **Enable Autoconfiguration** check box and then click **Submit Changes**. You can now enter values for the **IPv6 IP Address** field, the **IPv6 Subnet Mask** field, and the **IPv6 Router** field.

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” on page 30.

Configuring the Access Point as a DHCP Client

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

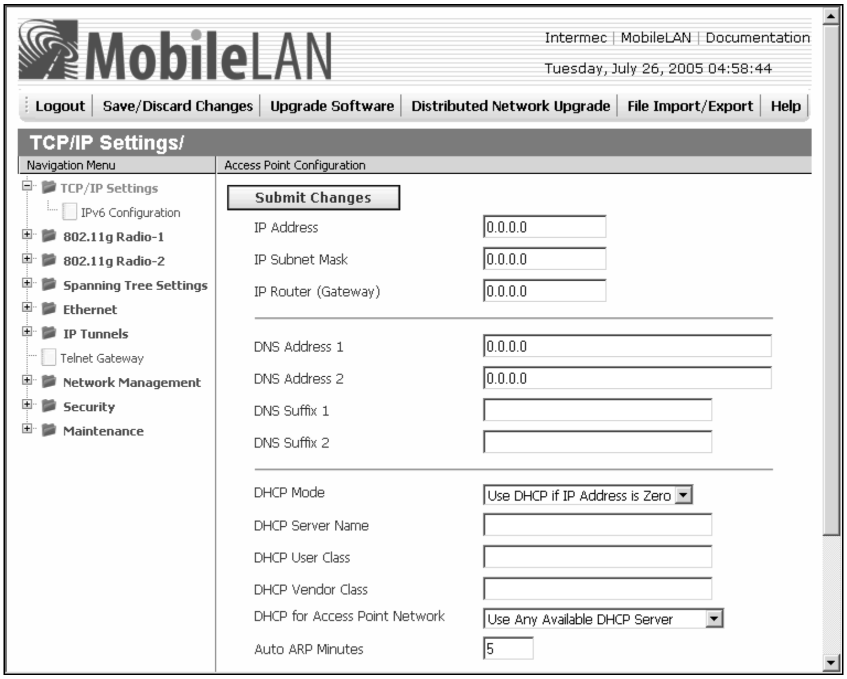
A DHCP client accepts offers from DHCP or BOOTP servers. Preference is given to DHCP servers. If a BOOTP reply is received before a DHCP offer, the access point waits 4 seconds. If a DHCP offer is received within the 4 seconds, the DHCP offer is used and the BOOTP reply is ignored. (BOOTP offers are treated like infinite DHCP leases.)

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 In the Navigation Menu, click **TCP/IP Settings**. The TCP/IP Settings screen appears.



IP Address 0.0.0.0
IP Subnet Mask 0.0.0.0
IP Router (Gateway) 0.0.0.0

DNS Address 1 0.0.0.0
DNS Address 2 0.0.0.0
DNS Suffix 1
DNS Suffix 2

DHCP Mode Use DHCP if IP Address is Zero
DHCP Server Name
DHCP User Class
DHCP Vendor Class
DHCP for Access Point Network Use Any Available DHCP Server
Auto ARP Minutes 5

2 Configure the DHCP parameters to make this access point a DHCP client. For help, see the next table.

Note: If you set **DHCP Mode** to **Disable DHCP** and the IP address for this access point is all zeroes, all IP communications are disabled for this access point.

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” on page 30.

DHCP Client Parameter Descriptions

Parameter	Explanation
DHCP Mode	To configure the access point as a DHCP client, you must choose one of these options: **Always Use DHCP:** The access point uses DHCP after every reboot whether or not an infinite lease was granted in a previous session. If this option is not selected, infinite leases are stored in non-volatile memory and reused after each reboot. (BOOTP is treated like an infinite lease.) **Use DHCP if IP Address is Zero:** (Default.) The access point uses DHCP only if the IP Address is set to all zeros. If you choose this option, make sure that the IP address is all zeroes.
DHCP Server Name	Leave this field blank if you want the access point to respond to offers from any server. Or enter the name of the DHCP server that this access point accesses for information. This access point will not respond to any other DHCP server.
DHCP User Class	Leave the field blank if you do not want the DHCP client to include a user class identifier in its requests. Or enter the DHCP user class identifier as defined in RFC 3004. When this access point acts as a DHCP client, the string entered in this field is sent in DHCP option 77 in DHCP request messages.
DHCP Vendor Class	Leave the field blank if you do not want the DHCP client to include the vendor class identifier in its requests. Or enter the DHCP vendor class identifier as defined in RFC 2132. When this access point acts as a DHCP client, the string entered in this field is sent in DHCP option 60 in DHCP request messages.
DHCP for Access Point Network	Determines which DHCP servers may be used by access points and wireless devices: **Use Any Available DHCP Server:** Access points and wireless devices may receive DHCP responses and addresses from any available DHCP server.

DHCP Client Parameter Descriptions (continued)

Parameter	Explanation
DHCP for Access Point Network (*continued*)	**Only Use Access Point DHCP Server:** Access points and any associated wireless devices may receive DHCP responses and addresses only from an access point DHCP server. Currently, the DHCP server must be located in the root access point. If this option is selected and the root access point does not have a DHCP server enabled, access points and wireless devices will not be able to receive a DHCP address. You can use this option, in combination with a DHCP user class, to segment a network that has an existing DHCP server and an access point DHCP server.

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 and other TCP/IP settings 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.

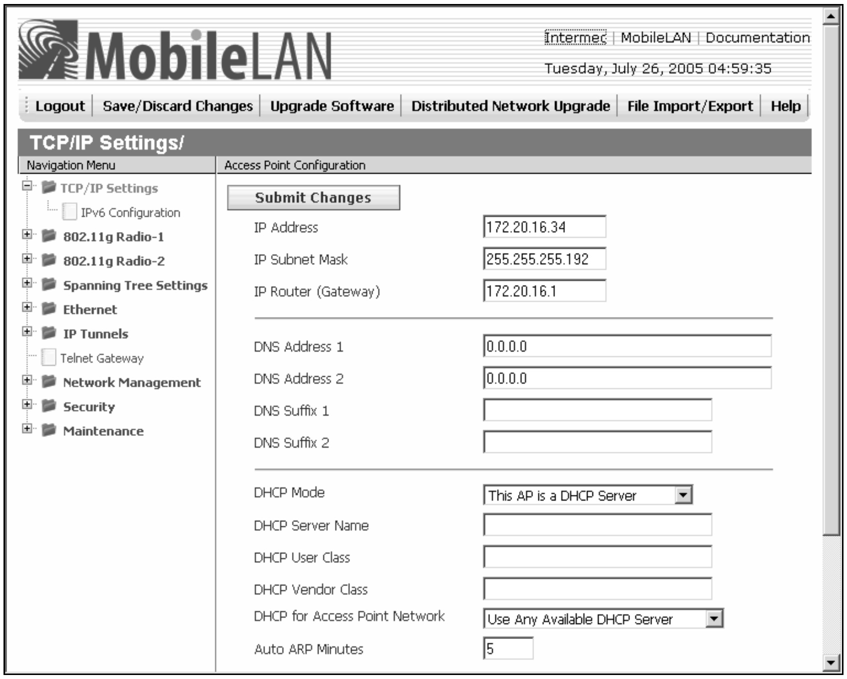
Note: If you configure the access point as a DHCP server, it is not intended to replace a general purpose, configurable DHCP server, and it makes no provisions for synchronizing DHCP policy between itself and other DHCP servers. Customers with complex DHCP policy requirements should use other DHCP server 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 In the Navigation Menu, click **TCP/IP Settings**. The TCP/IP Settings screen appears.



IP Address	172.20.16.34
IP Subnet Mask	255.255.255.192
IP Router (Gateway)	172.20.16.1
DNS Address 1	0.0.0.0
DNS Address 2	0.0.0.0
DNS Suffix 1	
DNS Suffix 2	
DHCP Mode	This AP is a DHCP Server
DHCP Server Name	
DHCP User Class	
DHCP Vendor Class	
DHCP for Access Point Network	Use Any Available DHCP Server
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” on page 48.

3 Configure the DHCP parameters to make this access point a DHCP server. For help, see the next table.

DHCP Server Parameter Descriptions

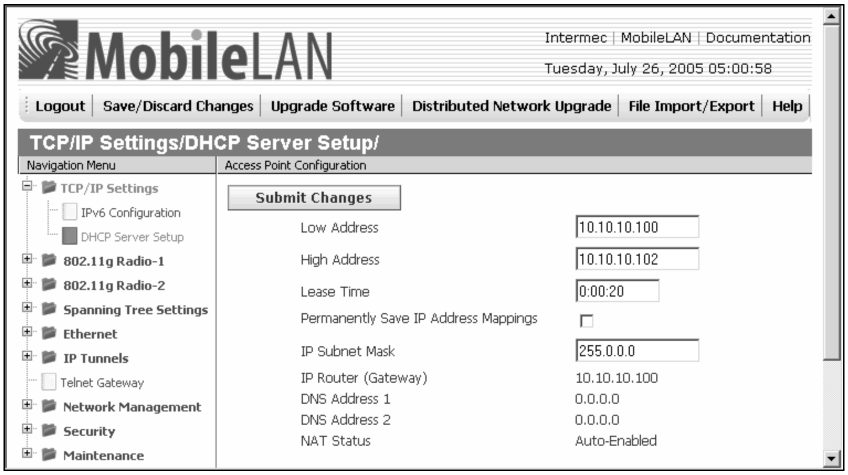
Parameter	Explanation
DHCP Mode	Choose **This AP is a DHCP Server**. The access point must have a valid IP address and subnet mask.
DHCP Server Name	Enter the name for this access point as a DHCP server.
DHCP User Class	Leave the field blank if you want this access point to respond to requests from any client. Or enter the DHCP user class identifier as defined in RFC 3004. When this access point acts as a DHCP server, the access point offers addresses to client requests only when the client requests contain a matching user class identifier.
DHCP Vendor Class	Leave the field blank if you want this access point to respond to requests from any client. Or enter the DHCP vendor class identifier as defined in RFC 2132. When this access point acts as a DHCP server, the access point offers addresses to client requests only when the client requests contains a matching vendor class identifier.

DHCP Server Parameter Descriptions (continued)

Parameter	Explanation
DHCP for Access Point Network	Determines which DHCP servers may be used by access points and wireless devices: **Use Any Available DHCP Server:** Access points and wireless devices may receive DHCP responses and addresses from any available DHCP server. **Only Use Access Point DHCP Server:** Access points and any associated wireless devices may receive DHCP responses and addresses only from an access point DHCP server. Currently, the DHCP server must be located in the root access point. If this option is selected and the root access point does not have a DHCP server enabled, access points and wireless devices will not be able to receive a DHCP address. You can use this option, in combination with a DHCP user class, to segment a network that has an existing DHCP server and an access point DHCP server.

4 Click **Submit Changes** to save your changes. **DHCP Server Setup** appears in the menu.

5 In the Navigation Menu, click **DHCP Server Setup**. The DHCP Server Setup screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Tuesday, July 26, 2005 05:00:58
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
TCP/IP Settings/DHCP Server Setup/
Navigation Menu
Access Point Configuration
TCP/IP Settings
IPv6 Configuration
DHCP Server Setup
802.11g Radio-1
802.11g Radio-2
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

Low Address	10.10.10.100
High Address	10.10.10.102
Lease Time	0:00:20
Permanently Save IP Address Mappings	□
IP Subnet Mask	255.0.0.0
IP Router (Gateway)	10.10.10.100
DNS Address 1	0.0.0.0
DNS Address 2	0.0.0.0
NAT Status	Auto-Enabled

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

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” on page 30.

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.
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.
Permanently Save IP Address Mappings	If you check this check box, the DHCP server stores permanent mappings of IP addresses to DHCP client identifiers. A DHCP client is guaranteed to receive the same IP address each time it requests an address even if the DHCP server reboots. If you clear this check box, the DHCP server tries to grant clients the same address each time, but that result is not guaranteed.
Display-only parameters	
IP Subnet Mask	Displays the subnet mask entered at the TCP/IP Settings screen.
IP Router (Gateway)	Displays the address of the IP Router.
DNS Address 1	Displays the IP address of the Domain Name Server. This address will be used for name solution and will be distributed to DHCP clients when this access point is a DHCP server.
DNS Address 2	Displays the IP address of the Domain Name Server. This address will be used for name solution and will be distributed to DHCP clients when this access point is a DHCP server.
NAT Status	This informative entry lets you know if DHCP has been properly configured, and if the range of addresses has automatically enabled Network Address Translation (NAT).

Supported DHCP Server Options

When the access point is acting as a DHCP server, it issues IP address leases to configure the IP address, along with the DNS addresses, DNS suffixes, 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. In the Navigation 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” on page 48.
3. In the **DHCP Mode** field, 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” on page 30.

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 minutes parameter controls the time interval between ARP requests.

If the address of the IP router is set to all zeroes, 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 In the Navigation Menu, click **TCP/IP Settings**. The TCP/IP Settings screen appears.

2 In the **Auto ARP Minutes** field, enter a time period from 1 to 120 minutes. To disable this parameter, enter 0.

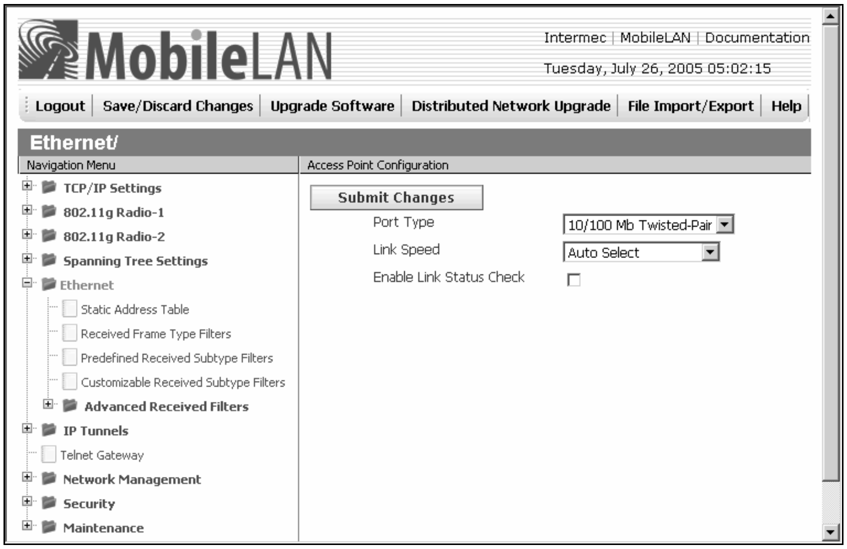
3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see “Saving Configuration Changes” on page 30.

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” on page 48. In the Ethernet screen, you can set the port type, set the link speed, and enable or disable the link status check.

To configure the Ethernet or fiber optic settings

1 In the Navigation Menu, click **Ethernet**. The Ethernet screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Tuesday, July 26, 2005 05:02:15
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Ethernet/
Navigation Menu
TCP/IP Settings
802.11g Radio-1
802.11g Radio-2
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

Port Type: 10/100 Mb Twisted-Pair

Link Speed: Auto Select

Enable Link Status Check ☐

2 Configure the 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” on page 30.

Ethernet Parameter Descriptions

Parameter	Explanation
Port Type	This field specifies the port that the access point uses to communicate with the Ethernet network: **10/100 Mb Twisted-Pair**: The access point communicates with the Ethernet network through the Ethernet port. **100 Mb Fiber Optic**: The access point communicates with the Ethernet network through the fiber optic port.
Link Speed	If **Port Type** is 100 Mb Fiber Optic, this field is automatically set to 100 Mbps Fiber Optic (full duplex). Choose the speed and duplex mode you want this port to use to communicate with the Ethernet. If you want the access point to auto-negotiate this field, choose Auto Select. Auto Select should work for most networks.
Enable 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.

Configuring the Ethernet Static Address Table

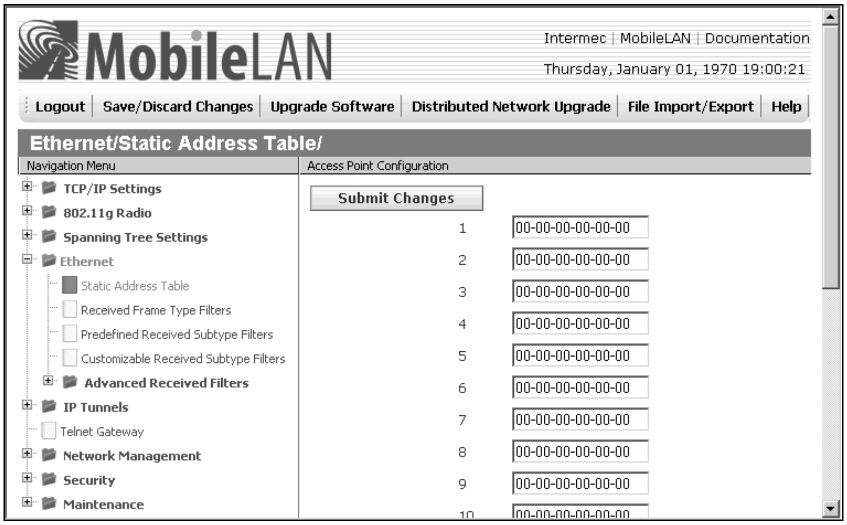
If you have a secondary LAN, you should configure the Ethernet static address table in the designated bridge or WAP on the secondary LAN. This table contains all the MAC addresses on the secondary LAN that are communicating with the primary LAN. You must enter the MAC addresses of all devices on the 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 static address table

1 In the Navigation Menu, click **Ethernet** > **Static Address Table**. The Static Address Table screen appears.



MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 19:00:21
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Ethernet/Static Address Table/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

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

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

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” on page 30.

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" on page 104.

Using Ethernet Received 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 cannot 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 cannot 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.

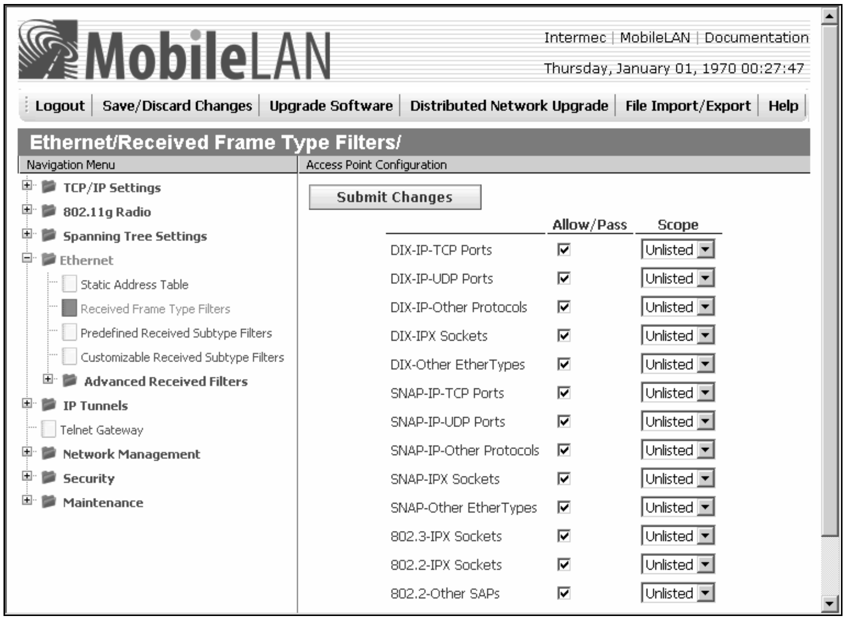
Here is the action and scope you can set for each parameter:

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 received frame type filters

1 In the Navigation Menu, click Ethernet > Received Frame Type Filters. The Received Frame Type Filters screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:27:47
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Ethernet/Received Frame Type Filters/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

	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 **Allow/Pass** check box to configure if the frame types are allowed to pass or are dropped. If you check the check box, the frame type is allowed to pass. For help, see the next table.

3 For each frame type field, set the **Scope** field 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” on page 30.

5 If you set the **Scope** field to Unlisted for a frame type, you must also configure predefined subtype filters or customizable subtype filters. For help, see the next section, “Using Predefined Received Subtype Filters,” or “Customizing Received Subtype Filters” on page 64.

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.

Frame Type Filter Descriptions (continued)

Frame Type	Explanation
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.

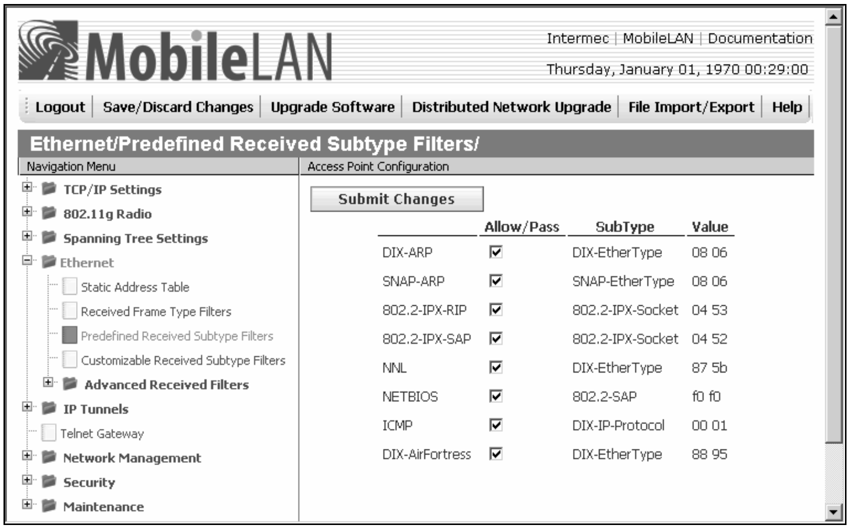
Note: You should not filter HTTP, Telnet, SNMP, and ICMP frames if you are using WAPs because these frame types are used for configuring, troubleshooting, and upgrading WAPs.

Using Predefined Received Subtype Filters

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

To configure predefined received subtype filters

1 In the Navigation Menu, click **Ethernet** > **Predefined Received Subtype Filters**. The Predefined Received Subtype Filters screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:29:00
Logout
Save/Discard Changes
Upgrade Software
Distributed Network Upgrade
File Import/Export
Help
Ethernet/Predefined Received Subtype Filters/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

	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
DIX-AirFortress	☑	DIX-EtherType	88 95

2 For each frame subtype field, check or clear the **Allow/Pass** check box to configure if the frame subtypes are allowed to pass 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” on page 30.

Customizing Received Subtype Filters

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

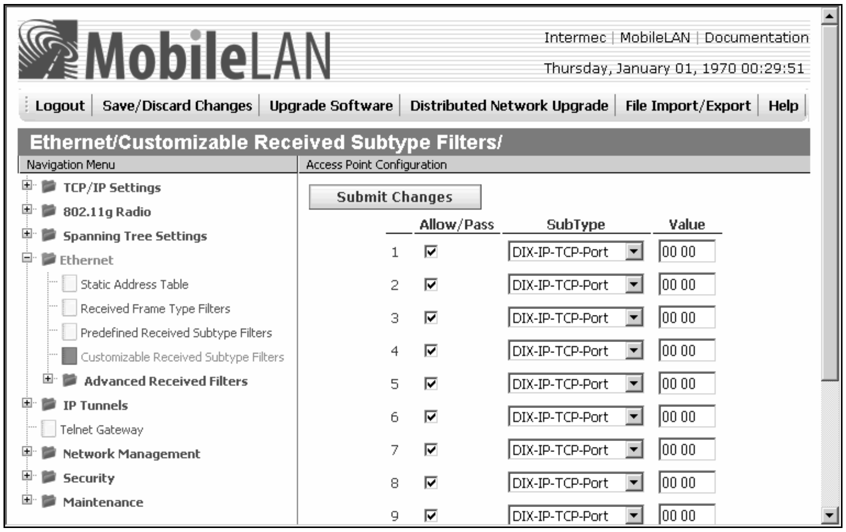
Allow/Pass: Check or clear this check box. Check this check box to pass all frames of the subtype and value. Clear this check box to drop all frames of the subtype and value.

SubType: Selects the frame subtype you wish to configure. For help setting the subtype and value, see the Subtype Filter Descriptions table on page 65.

Value: 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 In the Navigation Menu, click **Ethernet** > **Customizable Received Subtype Filters**. The Customizable Received Subtype Filters screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:29:51
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Ethernet/Customizable Received Subtype Filters/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

	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 **Allow/Pass** check box to configure if the subtypes are allowed to pass or are dropped. If you check the check box, the subtype is allowed to pass.

3 In the **SubType** field, choose the customizable frame subtype. For help, see the next table.

4 In the **Value** field, 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” on page 30.

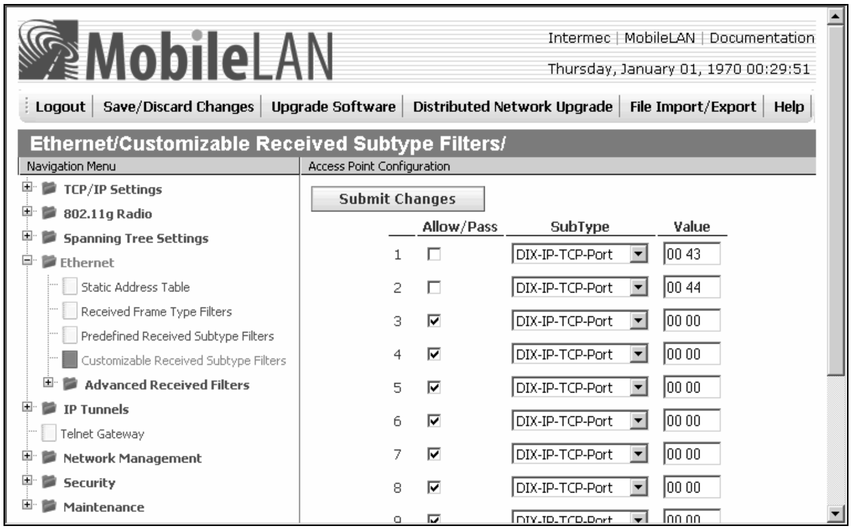
Subtype Filter Descriptions

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 allow only the wireless end devices (DHCP clients) 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.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:29:51
Logout
Save/Discard Changes
Upgrade Software
Distributed Network Upgrade
File Import/Export
Help
Ethernet/Customizable Received Subtype Filters/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

	Allow/Pass	SubType	Value
1	□	DIX-IP-TCP-Port	00 43
2	□	DIX-IP-TCP-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 Received 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.
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 Received Filters

You can configure advanced received filters if you need more flexibility in your filtering. Settings for advanced received filters execute after those for other filters; that is, advanced received filters are only applied if the frame has passed the other filters.

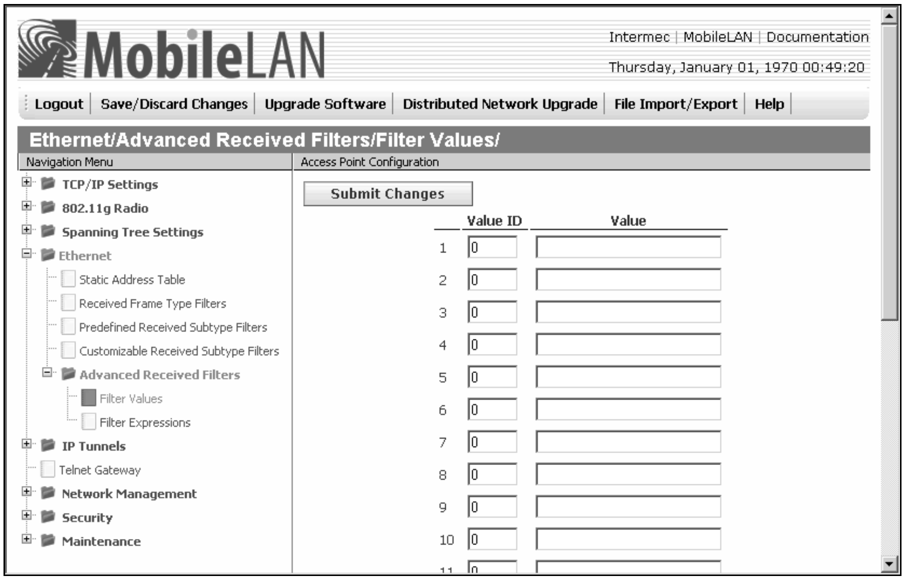
You can use filter values and filter expressions to minimize network traffic over the wireless links; however, Intermec recommends that you use advanced Ethernet filters only if you have an extensive understanding of network frames and their contents. Use other existing filters whenever possible.

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 In the Navigation Menu, click **Ethernet** > **Advanced Received Filters**. The Filter Values screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:49:20
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Ethernet/Advanced Received Filters/Filter Values/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
Filter Values
Filter Expressions
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

	Value ID	Value
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	0	
11	0	

2 Enter up to 22 value IDs and values.

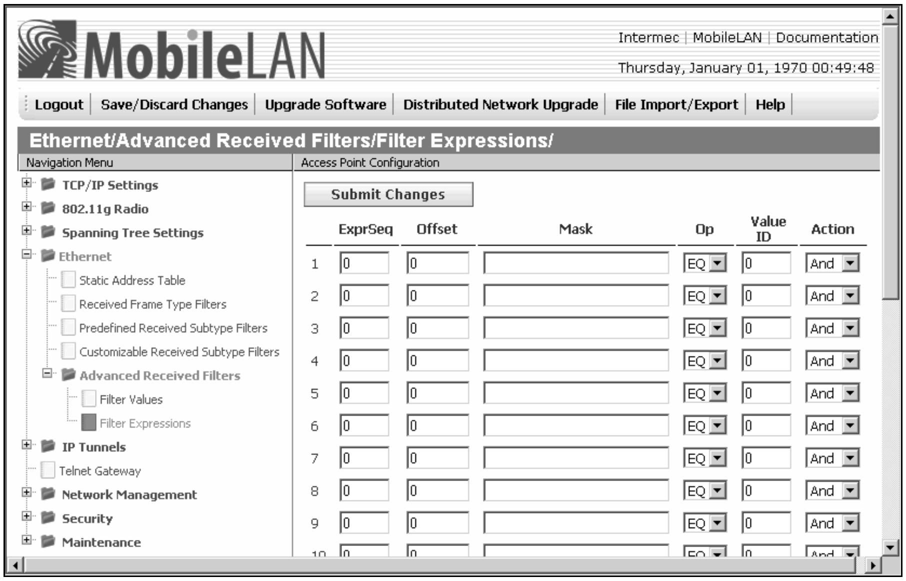
3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see “Saving Configuration Changes” on page 30.

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 In the Navigation Menu, click **Ethernet** > **Advanced Received Filters** > **Filter Expressions**. The Filter Expressions screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:49:48
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Ethernet/Advanced Received Filters/Filter Expressions/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
Filter Values
Filter Expressions
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

	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

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

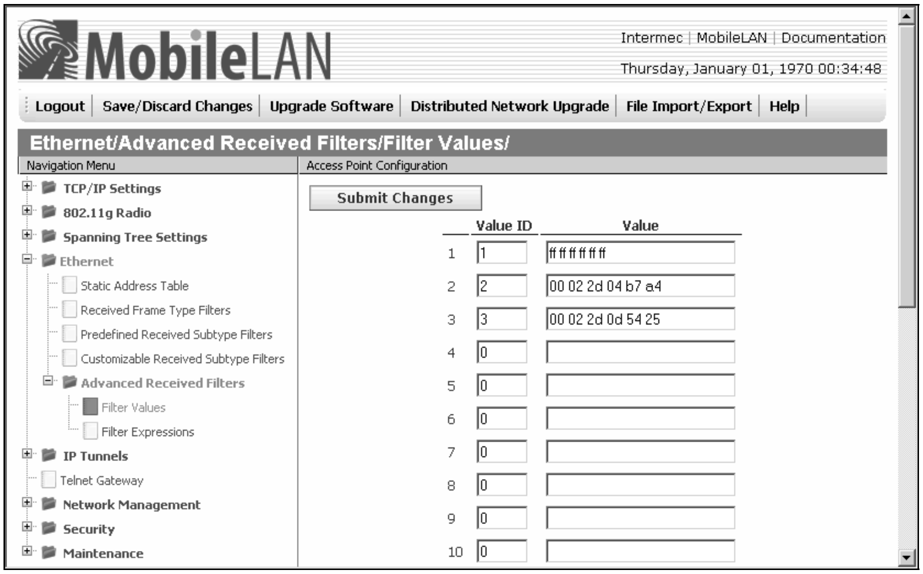
3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see “Saving Configuration Changes” on page 30.

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 0 to 8 hexadecimal 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)
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.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:34:48
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
Filter Values
Filter Expressions
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

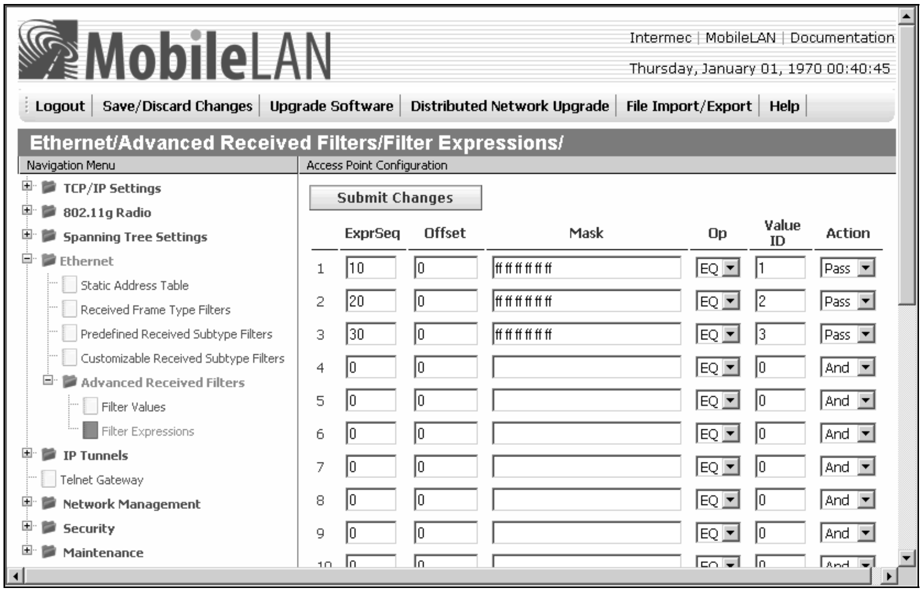
Ethernet/Advanced Received Filters/Filter Values/

	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.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:40:45
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
Filter Values
Filter Expressions
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

Ethernet/Advanced Received Filters/Filter Expressions/

	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

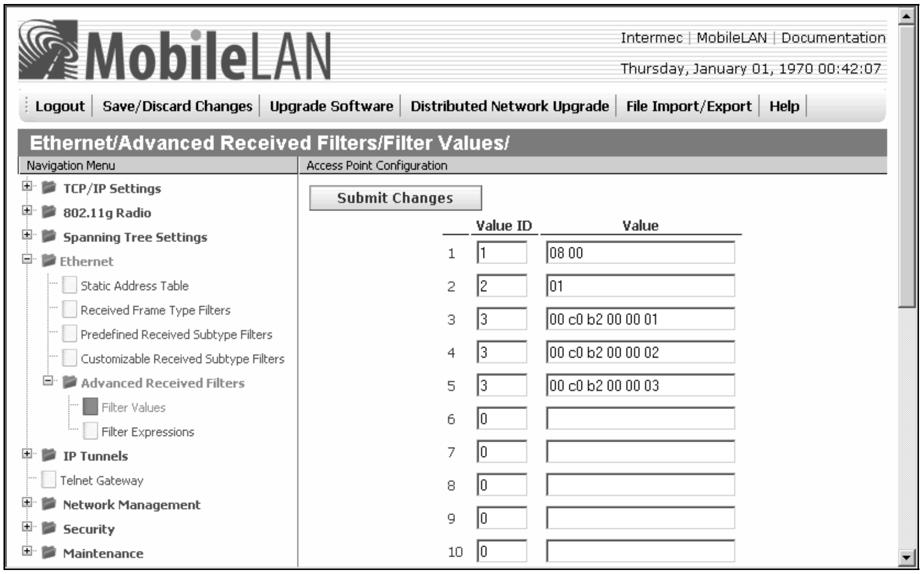
Example 1 – Filter Expressions

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.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:42:07
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Ethernet/Advanced Received Filters/Filter Values/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
Filter Values
Filter Expressions
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

	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	

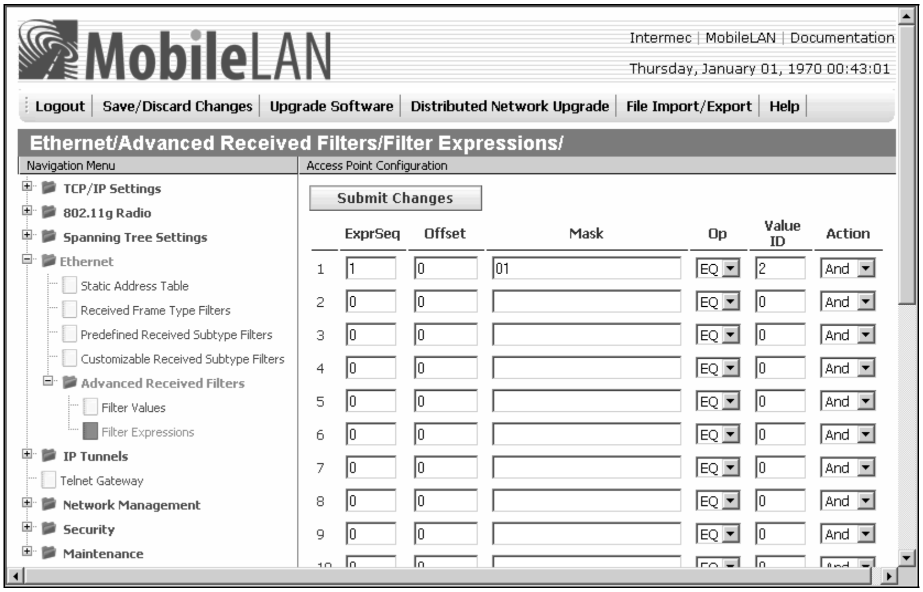
Example 2 - Filter Values

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.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:43:01
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
Filter Values
Filter Expressions
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

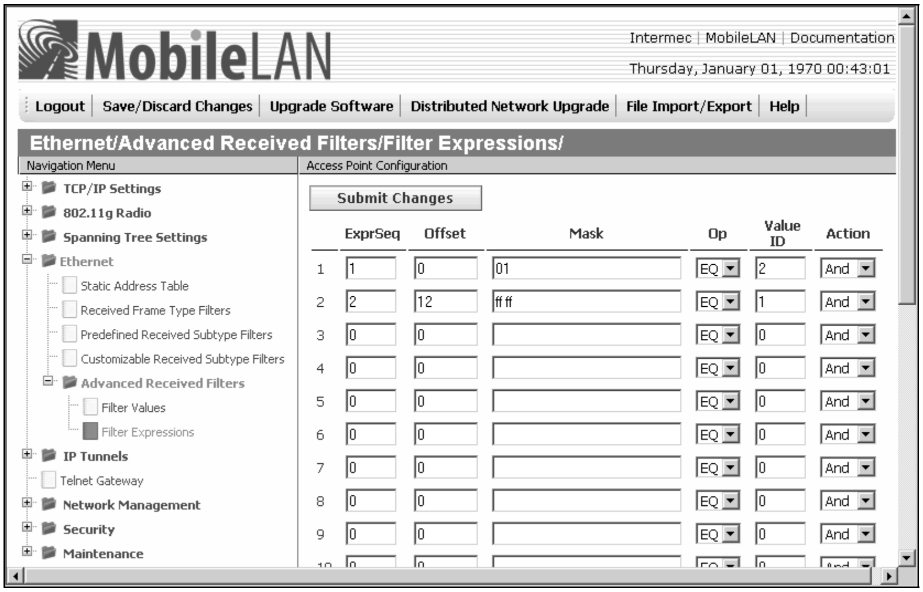
Ethernet/Advanced Received Filters/Filter Expressions/

	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

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.

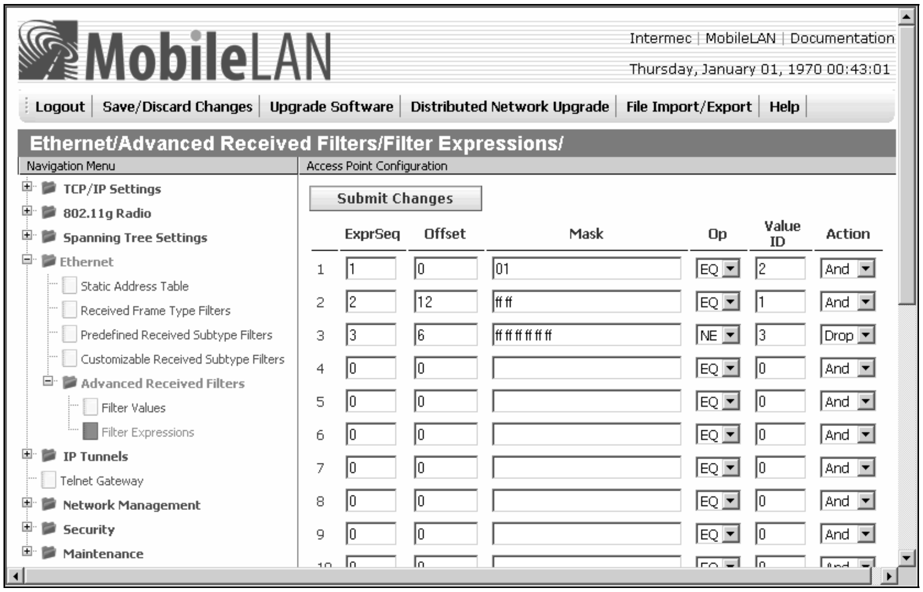

MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:43:01
Logout
Save/Discard Changes
Upgrade Software
Distributed Network Upgrade
File Import/Export
Help
Ethernet/Advanced Received Filters/Filter Expressions/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
Filter Values
Filter Expressions
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

	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

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.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 00:43:01
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Ethernet/Advanced Received Filters/Filter Expressions/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
Static Address Table
Received Frame Type Filters
Predefined Received Subtype Filters
Customizable Received Subtype Filters
Advanced Received Filters
Filter Values
Filter Expressions
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

	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

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 802.11g radios in the MobileLAN access WA2XG family of access points so that they communicate with your wireless end devices. This chapter covers these topics:

- About the 802.11g radio
- Configuring the 802.11g radio

Configuring the 802.11g Radio

You can configure the 802.11g radios to communicate with other 802.11g and 802.11b radios that have the same:

- SSID (Network Name)
- Security

For each radio, you can assign up to four service sets, creating one primary service set and up to three secondary service sets. The service sets share the same Advanced Configuration and Inbound Filters settings, but you can configure each service set for a different security environment. Multiple service sets are used primarily to allow one physical radio to support multiple virtual LANs (VLANs). For details about VLANs, see “Configuring VLANs” on page 134.

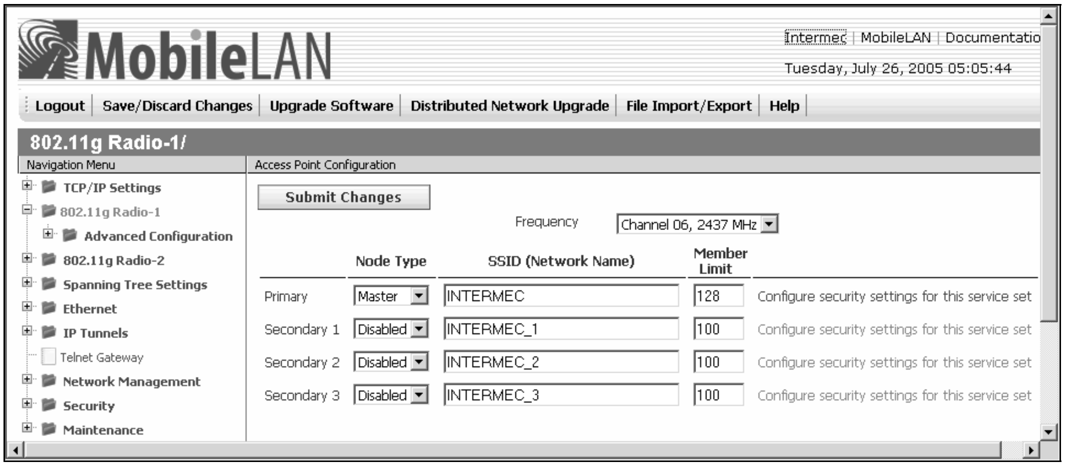
Before you enable a mixed security environment, verify that your wireless end devices perform active scanning. In active scanning, an end device sends a probe request to the SSID that it wants to associate with. Intermec’s newer end devices with newer 802.11g radios (such as the CK30, CK31, and CV60) work in a mixed security environment.

End devices that perform passive scanning do not support a mixed security environment. In passive scanning, an end device listens for beacons (sent by the access point radio’s primary service set), picks one it likes, and then associates with it. The beacons contain a security bit that advertises the type of security the primary service set is using. If the end device’s security setting does not match the beacon’s security bit, the end device cannot associate.

For details, see “When You Configure Different SSIDs With Different Security Settings” on page 122.

To configure the 802.11g radio

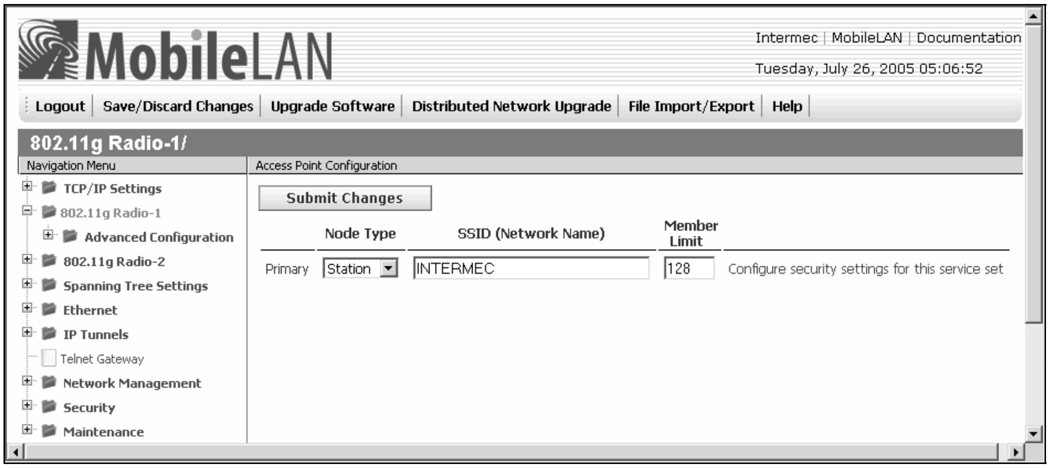
1 In the Navigation Menu, click **802.11g Radio**. The 802.11g Radio screen appears.



Frequency: Channel 06, 2437 MHz

	Node Type	SSID (Network Name)	Member Limit	
Primary	Master	INTERMEC	128	Configure security settings for this service set
Secondary 1	Disabled	INTERMEC_1	100	Configure security settings for this service set
Secondary 2	Disabled	INTERMEC_2	100	Configure security settings for this service set
Secondary 3	Disabled	INTERMEC_3	100	Configure security settings for this service set

If your screen does not look like the previous one, your primary service set may be configured as station (instead of master), so that the secondary service sets are not available, as shown next.



	Node Type	SSID (Network Name)	Member Limit	
Primary	Station	INTERMEC	128	Configure security settings for this service set

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 Advanced Parameters” on page 80.

4 (Master only) Configure inbound filters. For help, see “Configuring Inbound Filters” on page 82.

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" on page 30.

6 (Optional) Configure security by clicking **Configure security settings for this service set**. For help, see Chapter 6, "Configuring Security."

802.11g Radio Parameter Descriptions

Parameter	Explanation
Frequency (Master radio only)	Choose the frequency 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 802.11g Radios" table on page 79. 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.
Node Type	Configure the 802.11g radio to master, station, or disabled: **Master:** The radio always operates in Master mode. The radio becomes active to accept connections for wireless devices when the access point joins the spanning tree. All service sets to be configured for a VLAN must be set to Master. **Station:** The radio always operates in Station mode. The radio searches for an access point with an active Master mode radio to connect to. If a connection is established, this link becomes a possible connection to the root. **Disabled:** The radio is disabled. You can create up to four service sets for this radio by setting the Node Type as follows: • If the primary service set is Master, up to three secondary SSIDs may be set to Master. • If the primary SSID is Station, all secondary service sets are disabled and do not appear on screen. • If the primary service set is Disabled, all secondary service sets (and the physical radio) are disabled.
SSID (Network Name)	Enter a unique SSID for each enabled service set. You can configure up to four service sets for this radio. The SSID is case sensitive and cannot be blank or more than 32 alphanumeric characters. 802.11g radios can be configured to communicate with other 802.11g and/or 802.11b radios with the same SSIDs. You need to assign the same SSID to the wireless end devices that will connect to the radio.
Member Limit	Controls the maximum number of devices that can be associated with this radio (including the primary and secondary service sets).

Worldwide Frequencies for 802.11g Radios

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 802.11g 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:

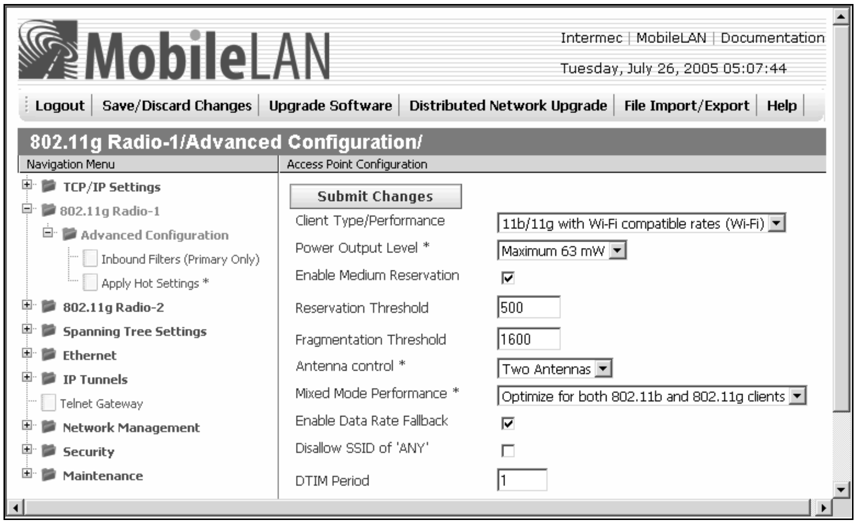
- FCC countries include the United States, Canada, China, Taiwan, India, Thailand, Indonesia, Malaysia, Hong Kong, and most South American countries.
- ETSI countries include all European Union countries except France. It also includes Switzerland, Iceland, Norway, Czech Republic, Slovenia, Slovakia, Turkey, Russia, and the United Arab Emirates.
- France, Mexico, and Singapore use the same channels.

Configuring Advanced Parameters

You can configure advanced parameters for the 802.11g radio primary service set. These settings are shared by any secondary service sets defined for the radio.

To configure advanced parameters

1 In the Navigation Menu, click **802.11g Radio** > **Advanced Configuration**. The Advanced Configuration screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Tuesday, July 26, 2005 05:07:44
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
802.11g Radio-1/Advanced Configuration/
Navigation Menu
TCP/IP Settings
802.11g Radio-1
Advanced Configuration
Inbound Filters (Primary Only)
Apply Hot Settings *
802.11g Radio-2
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

Client Type/Performance	11b/11g with Wi-Fi compatible rates (Wi-Fi)
Power Output Level *	Maximum 63 mW
Enable Medium Reservation	☑
Reservation Threshold	500
Fragmentation Threshold	1600
Antenna control *	Two Antennas
Mixed Mode Performance *	Optimize for both 802.11b and 802.11g clients
Enable Data Rate Fallback	☑
Disallow SSID of 'ANY'	□
DTIM Period	1

2 Configure the advanced 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” on page 30.

Note: If the field name is marked with an asterisk (*), you can immediately activate the changes without rebooting. For help, see “Applying Hot Settings” on page 84.

Advanced Parameter Descriptions

Parameter	Description
Client Type/Performance	Specifies if this radio will communicate with 802.11b and/or 802.11g radios: **11b/11g with range reliability (Not Wi-Fi):** Allows clients with 802.11b or 802.11g radios. Parameters are adjusted for longer range. Basic rates are 1 or 2 Mbps. Extended rates are 6, 12, or 24 Mbps. Data rates are 1, 2, 5.5, or 11 Mbps and extended data rates are 6, 9, 12, 18, 24, 36, 48, or 54 Mbps. **11b/11g with Wi-Fi compatible rates:** Allows clients with 802.11b or 802.11g radios. Basic rates are 1, 2, 5.5, or 11 Mbps. Data rates are 1, 2, 5.5, or 11 Mbps. Extended data rates are 6, 9, 12, 18, 24, 36, 48, or 54 Mbps. **11g only for better throughput (Wi-Fi):** Allows clients with 802.11g radios only. Basic rates are 1, 2, 5.5, or 11 Mbps. Extended data rates are 6, 9, 12, 18, 24, 36, 48, or 54 Mbps. Clients without extended rates capabilities are rejected. **11b/11g using 11b supported rates (Wi-Fi):** Allows clients with 802.11b or 802.11g radios. Clients that have mandatory extended data rate requirements will not associate. Basic rates are 1 or 2 Mbps. Data rates are 1, 2, 5.5, or 11 Mbps.
Power Output Level*	Set the transmitted power level: **Maximum:** Sets the output power to the highest level supported by the radio. **Medium:** Sets the output power to 3 dB lower than the highest level supported by the radio. **Low:** Sets the output power to a level higher than the lowest level supported by the radio. **Minimum:** Sets the output power to the lowest level supported by the radio. Lowering the power output level reduces the radio coverage for this area and reduces the range for this radio.
Enable Medium Reservation	Determines if you want to set a reservation threshold. Check this check box to set a threshold value. Click **Submit Changes**, and the **Reservation Threshold** parameter appears. 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	Appears only if the **Enable Medium Reservation** parameter is checked. 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.
Fragmentation Threshold	Specifies the largest data frame that can be transmitted without fragmentation. Range is 256 to 1600. 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.

Advanced Parameter Descriptions (continued)

Parameter	Description
Antenna control*	Specifies whether the radio uses one or both antennas: **Two Antennas:** The radio selects the antenna with the best reception for transmission and reception. **One Antenna:** The radio uses only one antenna for transmission and reception.
Mixed Mode Performance*	Gives more time to higher rate frames to maximize throughput in the presence of low rate clients. Range is 0 to 2000. **Optimized for 802.11g clients:** 802.11g transmissions are maximized. **Optimized for 802.11g clients:** 802.11b transmissions are maximized. **Optimize Mixed (802.11b and 802.11g):** Allows an optimal mix of 802.11g and 802.11b transmissions.
Enable Data Rate Fallback	Determines if you want the radio to drop to a slower data rate when it has trouble communicating with another radio. Intermec recommends that you leave this check box checked or you may affect radio network performance. Clearing this check box is only used when performing site surveys.
Disallow SSID (Network Name) of 'ANY' (Master radio only)	Determines if end devices that have their SSID set to ANY or are left blank (empty) can associate with this radio. Clear this check box to allow these end devices to associate with this radio. Although this setting is 802.11 compliant, it is not very secure. Check this check box to prevent end devices with an SSID of ANY or are left blank from associating with this radio.
DTIM Period (Master radio only)	Specifies the number of beacon periods to skip before including a DTIM (delivery traffic indication message) in a beacon frame. Range is 1 to 65535. Setting a higher DTIM period may conserve battery life in an end device, but it may increase response time.

Configuring Inbound Filters

You can configure inbound filters for the 802.11g radio primary service set. These settings are shared by any secondary service sets defined for the 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 need to check the **Allow IAPP** check box if you want the access point to be able to communicate with other access points and participate in the spanning tree.

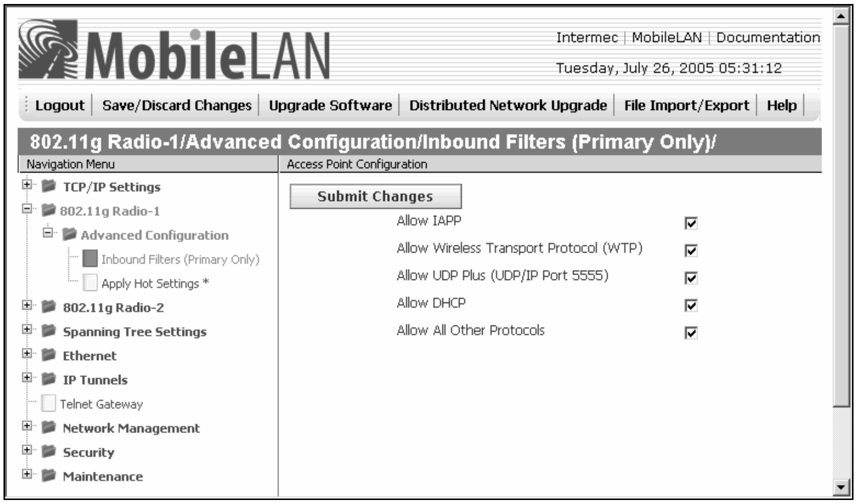
You can use this feature to form a secure wireless hop. Clear all check boxes, except for the **Allow IAPP** check box.

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 inbound filters

1. In the Navigation Menu, click **802.11g Radio** > **Advanced Configuration** > **Inbound Filters (Primary Only)**. The Inbound Filters screen appears.



Allow IAPP ☑

Allow Wireless Transport Protocol (WTP) ☑

Allow UDP Plus (UDP/IP Port 5555) ☑

Allow DHCP ☑

Allow All Other Protocols ☑

2. For each frame type, check or clear each check box. 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” on page 30.

802.11g Radio Inbound Filter Descriptions

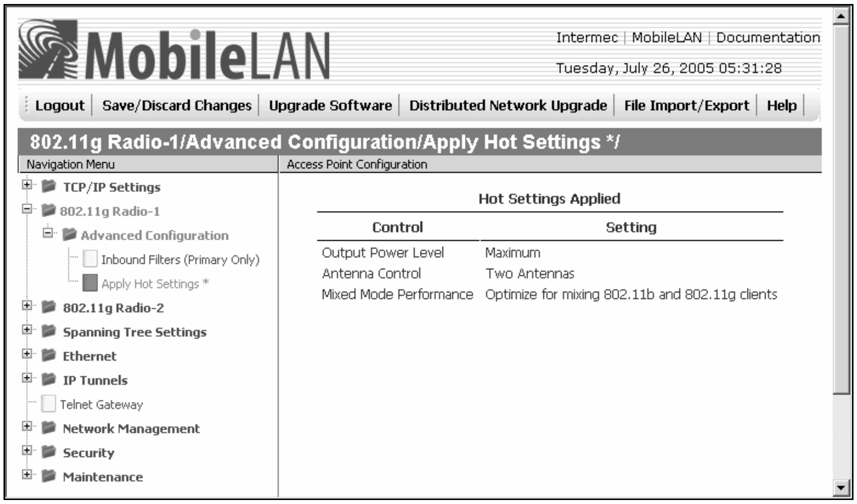
Parameter	Description
Allow IAPP	Determines if this radio accepts IAPP (Inter Access Point Protocol) frames from other access point station radios. The IAPP frames must match Ethernet protocol 875c.
Allow Wireless Transport Protocol (WTP)	Determines if this radio accepts WTP frames from end devices. The WTP frames must match Ethernet protocol 875b.
Allow 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, Intermec Gateway, 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.

Applying Hot Settings

You can “hot set” the Power Output Level and Mixed Mode Performance parameters for the 802.11g radio, which means that the new settings can be immediately activated without rebooting the access point.

To apply hot settings

1. In the Navigation Menu, click **802.11g Radio** > **Advanced Configuration** and change the parameters as needed.
2. Click **Submit Changes** to save your changes to the “current” configuration file (as defined on page 30).
3. In the Navigation Menu, click **Apply Hot Settings** to save your changes to the “active” configuration file (as defined on page 30). The Apply Hot Settings screen appears. This screen is read-only.


MobileLAN
Intermec | MobileLAN | Documentation
Tuesday, July 26, 2005 05:31:28
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
802.11g Radio-1/Advanced Configuration/Apply Hot Settings */
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio-1
Advanced Configuration
Inbound Filters (Primary Only)
Apply Hot Settings *
802.11g Radio-2
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance

Hot Settings Applied

Control	Setting
Output Power Level	Maximum
Antenna Control	Two Antennas
Mixed Mode Performance	Optimize for mixing 802.11b and 802.11g clients

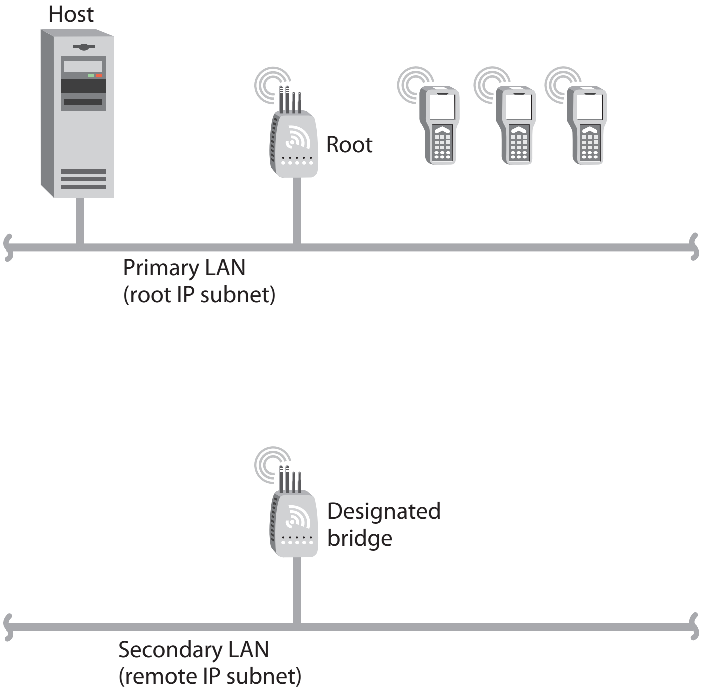
5 Configuring the Spanning Tree

This chapter explains how to configure the MobileLAN access WA2XG family of access points so that they create a spanning tree topology. This chapter covers these topics:

- About the access point spanning tree
- Configuring the spanning tree parameters
- About IP tunnels
- Configuring IP tunnels
- Filter examples
- Comparing IP tunnels to mobile IP
- Configuring global parameters

About the Access Point Spanning Tree

MobileLAN access WA2XG family of access points 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.



This spanning tree contains a root access point on the primary LAN and a designated bridge on the secondary LAN.

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 802.11g 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 also be on another subnet.

The root access point coordinates the network and distributes common system parameters to other access points and end devices. Consider these selection criteria when choosing which access point to be the root:

- The root must be installed on the primary LAN.
- The root should be an access point that does not handle a large volume of wireless traffic.
- The root should have the latest software release available because the root distributes parameters to the child access points. In a mixed network of WA2Xs and 210Xs, choose a WA21 or WA22 as the root.
- If your mixed network contains MobileLAN access products and 6710s, configure a MobileLAN access product as the root.

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 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. (Use the selection criteria listed earlier in this section to determine which access points should be root candidates.) 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. Using the selection criteria listed earlier in this section, determine which access point to configure as the root.
2. On that access point, from the Navigation Menu click **Spanning Tree Settings**. The Spanning Tree Settings screen appears.

3. In the **LAN ID (Domain)** field, enter a LAN ID. All access points that want to participate in the spanning tree must have the same LAN ID.
4. Set the **Root Priority** parameter to be the highest number of all access points on the primary LAN. Verify that the **Enable Ethernet Bridging** check box is checked.
5. Verify that the **Secondary LAN Bridge Priority** is zero.
6. Verify that the **Secondary LAN Flooding** parameter is **Disabled**.
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” on page 30.

About Secondary LANs and Designated Bridges

Important Note: Currently, a designated bridge cannot bridge to another secondary LAN. If it has two radios, it can communicate to a WAP or wireless end devices. If you need to bridge to another secondary LAN, you must use two access points.

There are two types of secondary LANs:

- A wireless secondary LAN, which is an Ethernet segment containing access points that join the primary LAN network through a wireless connection.
- A remote IP subnet, which is connected via an IP tunnel.

Comparison of Wireless Secondary LANS and Remote IP Subnets

Wireless Secondary LANs	Remote IP Subnets
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. Consider these selection criteria when choosing which access point to be the designated bridge:

- The designated bridge must be installed on the secondary LAN and within radio coverage of an access point on the primary LAN.
- The designated bridge should have the latest software release available. In a mixed network of WA2Xs and 210Xs, choose a WA21 or WA22 as the designated bridge.

- The designated bridge must be configured so that the **Secondary LAN Bridge Priority** value is a non-zero number.
- The designated bridge must have at least one radio set to Station mode, or the designated bridge must be the endpoint of an IP tunnel (as defined on page 94).

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. Using the selection criteria listed earlier in this section, determine which access point to configure as the designated bridge.
2. On that access point, from the Navigation Menu click **Spanning Tree Settings**. The Spanning Tree Settings screen appears.
3. In the **LAN ID (Domain)** field, enter a LAN ID. All access points that want to participate in the spanning tree must have the same LAN ID.
4. Set the **Root Priority** parameter to zero. All access points on the secondary LAN should have a root priority of zero.
5. Verify that the **Enable Ethernet Bridging** check box is checked.
6. Set the **Secondary LAN Bridge Priority** to be the highest number of all access points on the secondary LAN.
7. Set the **Secondary LAN Flooding** parameter to **Enabled**.
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” on page 30.

About Ethernet Bridging/Data Link Tunneling

Ethernet bridging is simply forwarding a frame received on the radio port to the Ethernet port, and vice versa. Using this default mode, the access point acts as a bridge between the wireless and wired networks.

Note: Intermec recommends that you enable Ethernet bridging on all access points. However, if you meet the criteria listed later in this section, you can disable Ethernet bridging and use data link tunneling instead. Be aware that data link tunneling increases network traffic.

Turning off Ethernet bridging enables data link tunneling. The data link tunneling mode causes the child access point to encapsulate inbound wireless data into an Intermec-assigned 875C frame. This data 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 encapsulates 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.

When should you use data link tunneling?

- 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 are sent to the wrong port. If the switch does not support 802.1d, it may become confused and communications with the end device are 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.

- 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. In this situation, using data link tunneling does not increase 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 **Enable Ethernet Bridging** check box is checked.
3. On all other access points on the primary LAN, clear the **Enable Ethernet Bridging** 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 **Enable Ethernet Bridging** check box is checked.

3. On all other access points on the secondary LAN, clear the **Enable Ethernet Bridging** 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" on page 94.

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

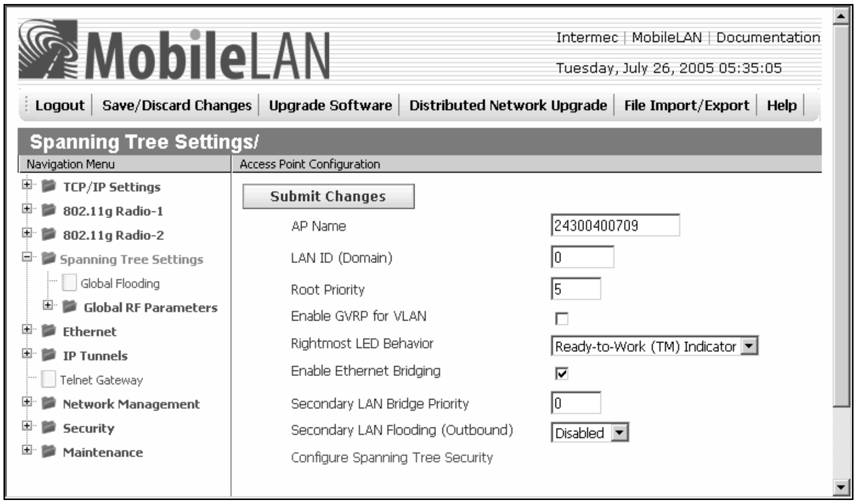
When you configure the spanning tree parameters, you identify the access point as part of the spanning tree. That is, you specify if this access point is a root, or a candidate to become a root, or a designated bridge, or a candidate to become a designated bridge.

You also specify if the access point uses Ethernet bridging to forward frames between the wired and wireless networks. Intermec recommends that you use Ethernet bridging on all access points unless you meet the criteria listed on page 90.

Note: On the designated bridge, 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 Navigation Menu, click **Spanning Tree Settings**. The Spanning Tree Settings screen appears.



Tuesday, July 26, 2005 05:35:05

Spanning Tree Settings/

AP Name	24300400709
LAN ID (Domain)	0
Root Priority	5
Enable GVRP for VLAN	□
Rightmost LED Behavior	Ready-to-Work (TM) Indicator
Enable Ethernet Bridging	☑
Secondary LAN Bridge Priority	0
Secondary LAN Flooding (Outbound)	Disabled
Configure Spanning Tree Security	

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” on page 30.

4 (Optional) Configure security by clicking **Configure Spanning Tree Security**. For help, see “Creating a Secure Spanning Tree” on page 130.

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.
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.
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. All access points on the secondary LAN should have a root priority of 0. For help deciding if this access point should be a candidate to become root, see the selection criteria listed on page 87.

Spanning Tree Parameter Descriptions (continued)

Parameter	Explanation
Enable GVRP for VLAN	The access point uses GARP VLAN Registration Protocol (GVRP) to request a VLAN-capable Ethernet switch to forward traffic for specific VLANs. Enabling this parameter lets the switch exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast, prune unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports. A switch may also be configured statically to always forward specific VLANs to specific ports. You should clear this check box for a static configuration.
Rightmost LED Behavior	Determines if this LED to behaves as if it were an Intermec Ready-to-Work indicator or a legacy Root/error indicator. Choosing **Spanning Tree Root Indicator** causes the LED to blink if the access point is configured as the root and remain on if an error is detected.
Enable Ethernet Bridging	Determines how frames from end devices are moved between the wired and wireless networks. For more details, see "About Ethernet Bridging/Data Link Tunneling" on page 89. 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. Clear this check box if you meet the selection criteria listed on page 90 and you want to use data link tunneling. **Note:** If you enable this parameter on the root or designated bridge, but you disable it on all other access points on the same IP subnet, then Ethernet bridging is disabled on the IP subnet. This means that data link tunneling is enabled on the IP subnet.
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 help deciding if this access point should become the designated bridge, see the selection criteria listed on page 88.

Spanning Tree Parameter Descriptions (continued)

Parameter	Explanation
Secondary LAN Flooding (Outbound)	Appears for Designated Bridge only. Specifies the types of frames it forwards from the primary LAN to the secondary LAN: **Disabled:** No flooding occurs unless the root access point (in the Global Flooding screen) enables the Multicast or Unicast Outbound to Secondary LANs parameter. **Enabled:** Multicast and unicast flooding occurs unless the root access point (in the Global Flooding screen) disables multicast or unicast flooding. **Multicast:** Multicast flooding occurs unless the root access point (in the Global Flooding screen) disables multicast flooding. **Unicast:** Unicast flooding occurs unless the root access point (in the Global Flooding screen) disables unicast flooding.

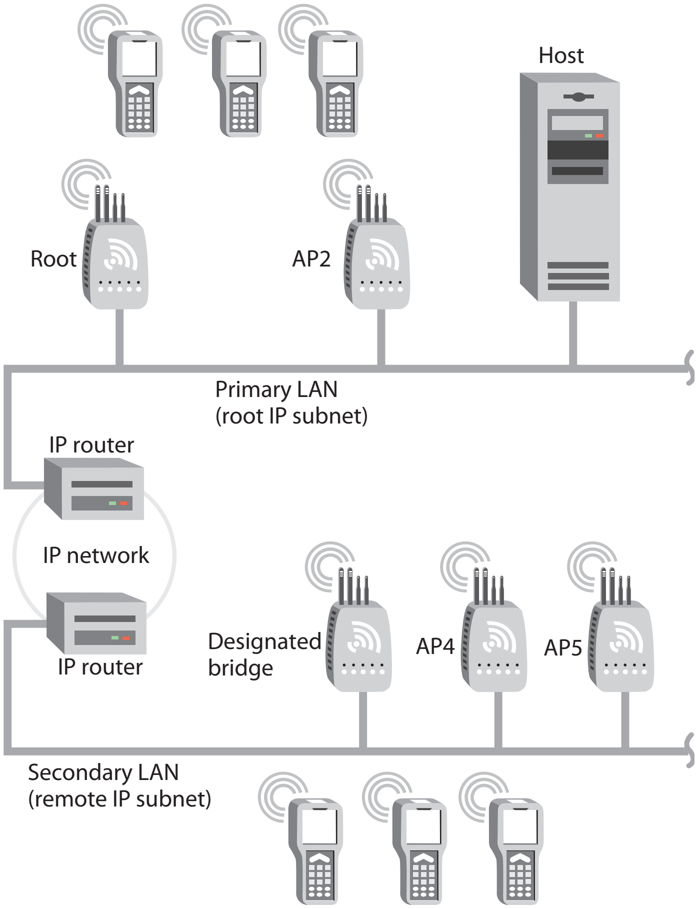
About IP Tunnels

Note: You cannot use IPv6 addressing with IP tunnels. The IP tunnel endpoints must have IPv4 addresses.

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 (VLAN) segment through IP routers. The VLAN 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” on page 98.

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" on page 87.
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** > **IP Addresses**. Enter the IP address or DNS name 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 **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 **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" on page 30.

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 IAPP. You must enter this address in the IP address list in the root access point (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" on page 87.
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** > **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" on page 30.

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.

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.

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:

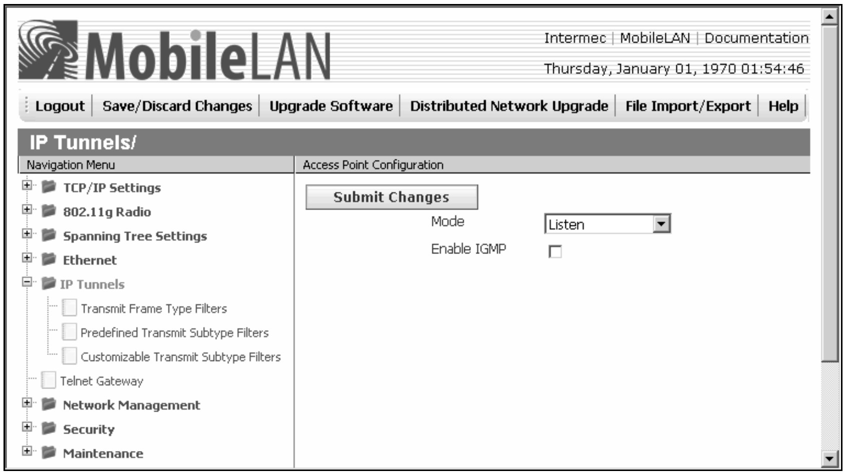
- 802.1d bridge frames
- Proprietary VLAN switch frames
- IP frames with a broadcast or multicast Ethernet address
- IP frames with the following router protocol types and decimal values:
  - DGP (86) (Dissimilar Gateway Protocol)
  - EGP (8) (Exterior Gateway Protocol)
  - IDPR (35) (Inter-Domain Policy 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” on page 94.

To configure the IP Tunnels screen

1 From the Navigation Menu, click **IP Tunnels**. The IP Tunnels screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 01:54:46
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
IP Tunnels/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Transmit Frame Type Filters
Predefined Transmit Subtype Filters
Customizable Transmit Subtype Filters
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

Mode: Listen

Enable IGMP: □

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” on page 30.

IP Tunnel Parameter Descriptions

Parameter	Explanation
Mode	Choose the mode: **Originate if Root:** Lets the root access point and root candidates originate the IP tunnel if they are functioning as the root access point for the network. **Listen:** Configures access points that are designated bridges or designated bridge candidates for their remote IP subnets to serve as the endpoint of an IP tunnel. **Disabled:** Disables the IP tunnel port.
Allow IP Multicast	Appears only if **Mode** parameter is **Originate if Root**. Determines if the root access point should forward IP multicast frames through its IP tunnels. Check this check box if you have a DHCP server issuing TCP/IP information to end devices.
Enable IGMP	Appears only if **Mode** parameter is **Listen**. Determines if IGMP is enabled or disabled.

IP Tunnel Parameter Descriptions (continued)

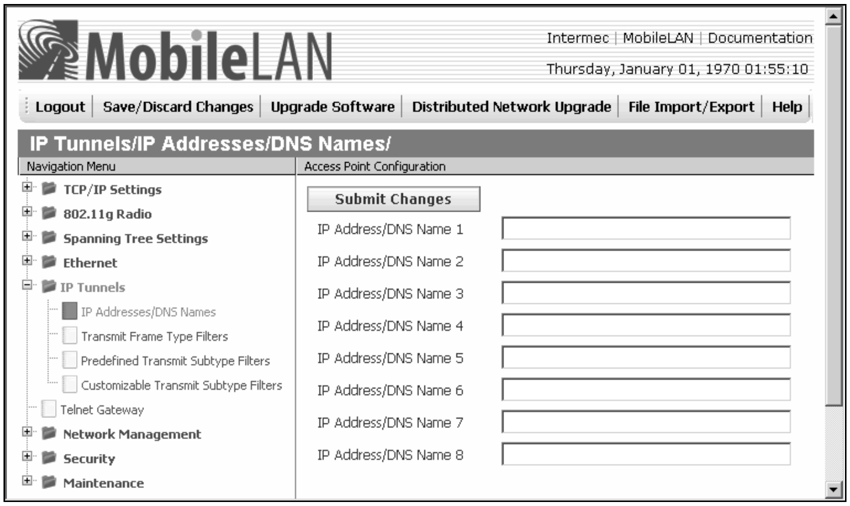
Parameter	Explanation
Multicast Address	Appears only if **Enable IGMP** check box is checked. Enter the Class D IP multicast address. You also need to enter this IP address in the root access point's IP address list. The Internet Assigned Numbers Authority has allocated 224.0.1.65 for Intermec's inter-access-point 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 Navigation Menu, click **IP Tunnels** > **IP Addresses/DNS Names**. The IP Addresses/DNS Names screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 01:55:10
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
IP Tunnels/IP Addresses/DNS Names/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
IP Addresses/DNS Names
Transmit Frame Type Filters
Predefined Transmit Subtype Filters
Customizable Transmit Subtype Filters
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

IP Address/DNS Name 1

IP Address/DNS Name 2

IP Address/DNS Name 3

IP Address/DNS Name 4

IP Address/DNS Name 5

IP Address/DNS Name 6

IP Address/DNS Name 7

IP Address/DNS Name 8

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

3 Enter the IP addresses or DNS names 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" on page 30.

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” on page 59.

Using IP Tunnel Transmit 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” on page 101.

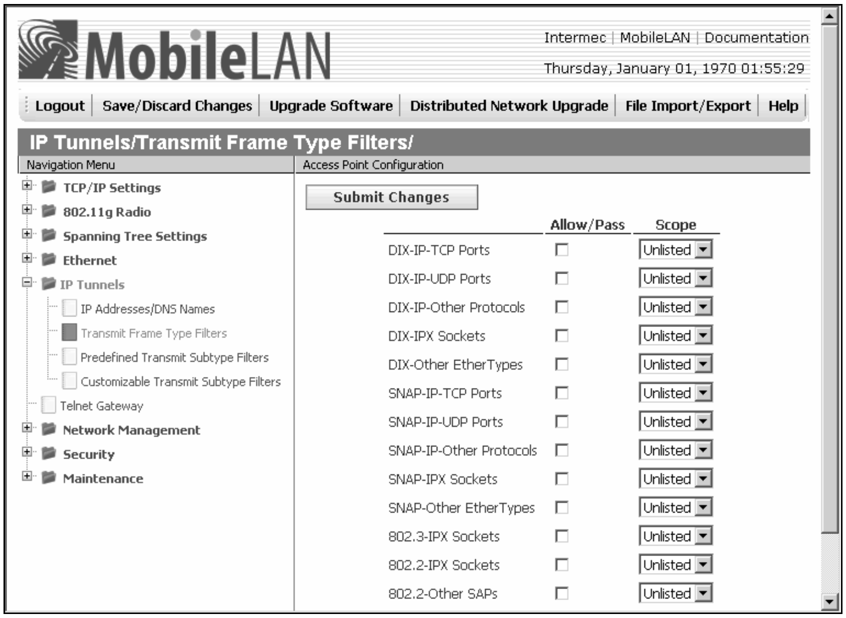
You can set the default action and scope for general and specific frame types:

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 transmit frame type filters

1 From the Navigation Menu, click **IP Tunnels** > **Transmit Frame Type Filters**. The Transmit Frame Type Filters screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 01:55:29
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
IP Tunnels/Transmit Frame Type Filters/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
IP Addresses/DNS Names
Transmit Frame Type Filters
Predefined Transmit Subtype Filters
Customizable Transmit Subtype Filters
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

	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, set the **Scope** field 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" on page 30.

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 Transmit Subtype Filters" on page 102 or "Customizing Transmit Subtype Filters" on page 102.

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.

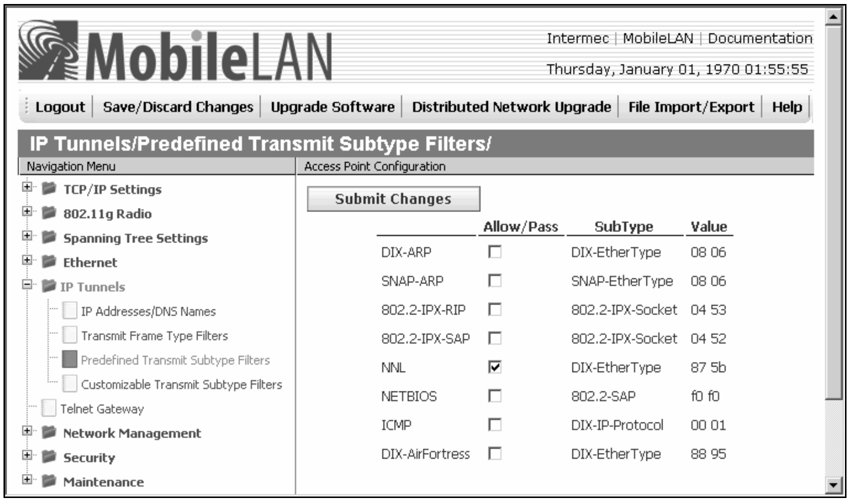
Note: You should not filter HTTP, Telnet, SNMP, and ICMP frames if you are using IP tunnels, because these filters are used for configuring, troubleshooting, and upgrading access points.

Using Predefined Transmit Subtype Filters

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

To configure predefined transmit subtype filters

1 From the main menu, click **IP Tunnels** > **Predefined Transmit Subtype Filters**. The Predefined Transmit Subtype Filters screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 01:55:55
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
IP Tunnels/Predefined Transmit Subtype Filters/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
IP Addresses/DNS Names
Transmit Frame Type Filters
Predefined Transmit Subtype Filters
Customizable Transmit Subtype Filters
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

	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
DIX-AirFortress	□	DIX-EtherType	88 95

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" on page 30.

Customizing Transmit 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:

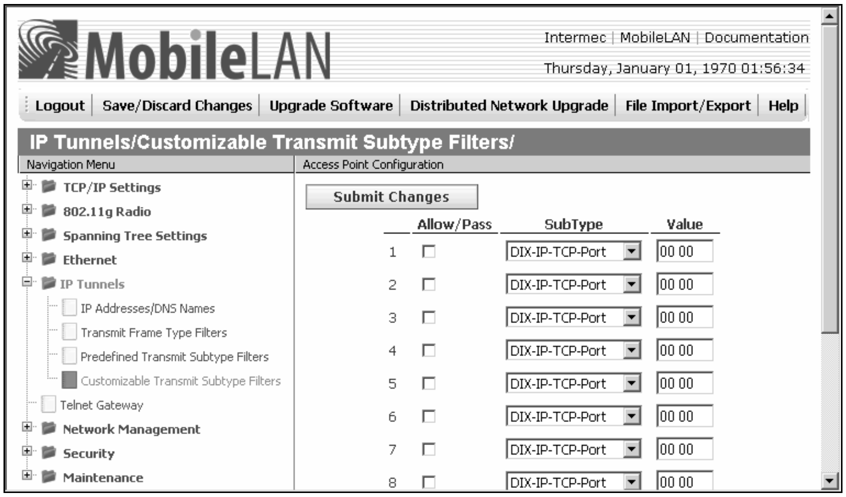
Allow/Pass: Check or clear this check box. Check this check box to pass all frames of the subtype and value. Clear this check box to drop all frames of the subtype and value.

Subtype: Selects the frame subtype you wish to configure.

Value: The next 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 transmit subtype filters

1 From the main menu, click **IP Tunnels** > **Customizable Transmit Subtype Filters**. The Customizable Subtype Filters screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 01:56:34
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
IP Tunnels/Customizable Transmit Subtype Filters/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
IP Addresses/DNS Names
Transmit Frame Type Filters
Predefined Transmit Subtype Filters
Customizable Transmit Subtype Filters
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

	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

2 For each frame subtype field, check or clear the **Allow/Pass** 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 In the **SubType** field, choose the customizable frame subtype. For help, see the next table.

4 In the **Value** field, 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" on page 30.

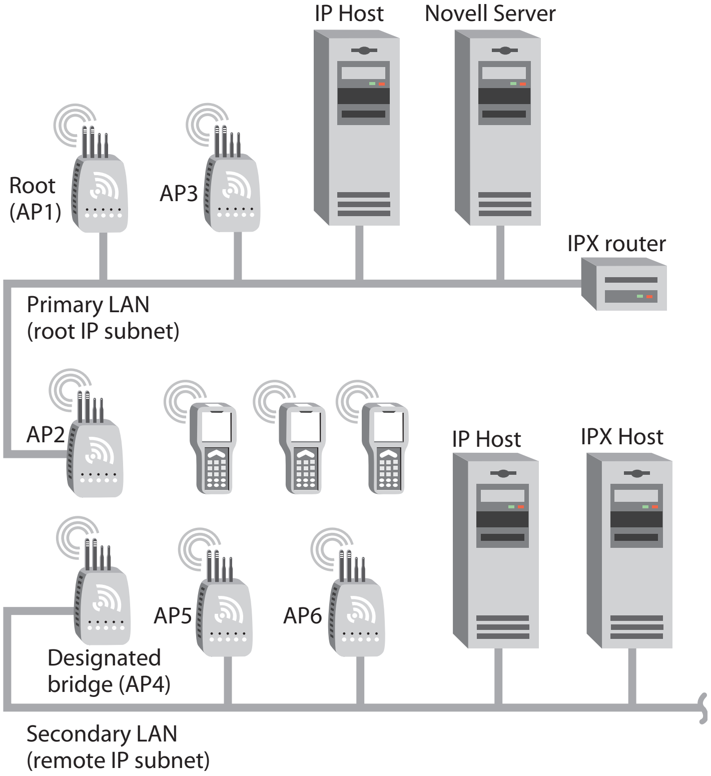
Subtype Filter Descriptions

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.

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.

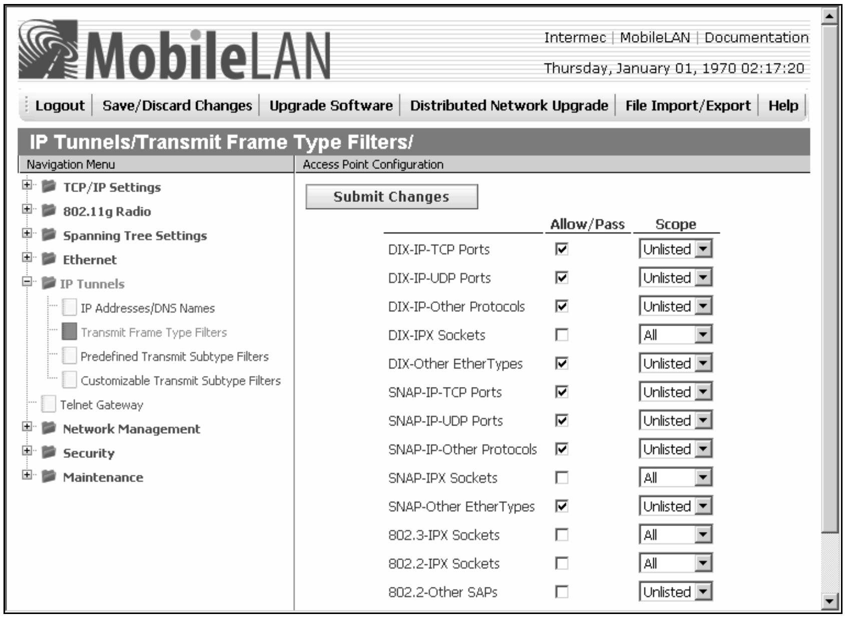


This illustration shows a typical network that will be used in the next examples.

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 Transmit Frame Type Filters screen. No subtype filters are needed.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 02:17:20
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
IP Tunnels/Transmit Frame Type Filters/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
IP Addresses/DNS Names
Transmit Frame Type Filters
Predefined Transmit Subtype Filters
Customizable Transmit Subtype Filters
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

	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

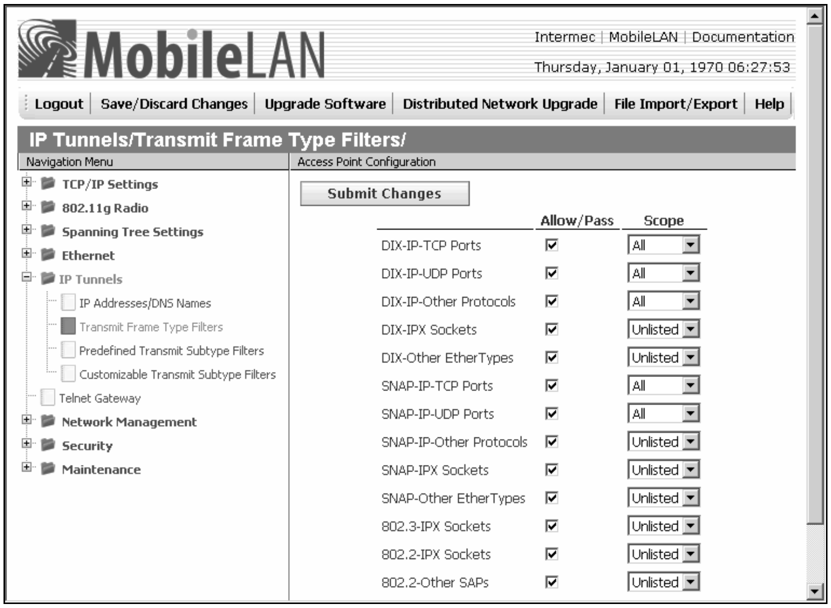
Example 2

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.

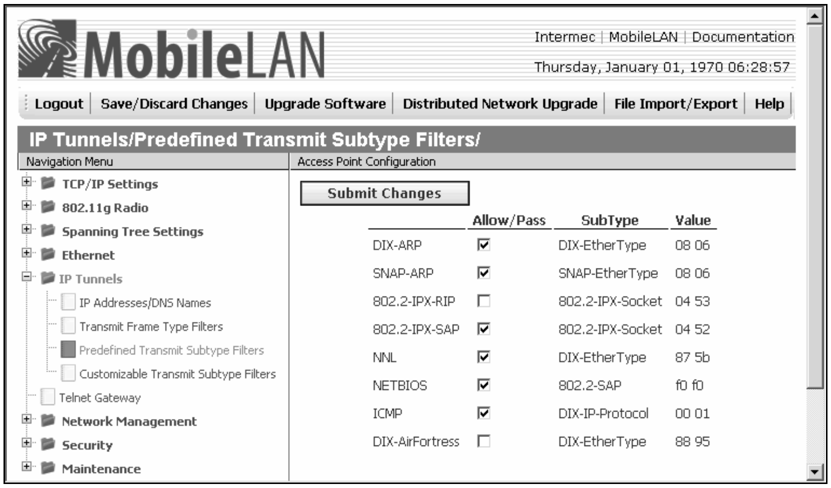
To filter the IPX RIP frames, you need to configure subtype filters. This example sets filters for three different cases: DIX, 802.2, and 802.3 SNAP frames. In many actual networks, only one type of filter is required, because all stations are configured using one of the three options.

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


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 06:27:53
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
IP Tunnels/Transmit Frame Type Filters/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
IP Addresses/DNS Names
Transmit Frame Type Filters
Predefined Transmit Subtype Filters
Customizable Transmit Subtype Filters
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

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


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 06:28:57
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
IP Tunnels/Predefined Transmit Subtype Filters/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
IP Addresses/DNS Names
Transmit Frame Type Filters
Predefined Transmit Subtype Filters
Customizable Transmit Subtype Filters
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

	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
DIX-AirFortress	☐	DIX-EtherType	88 95

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, set these filters to allow for the necessary IP tunneling.

1 On the root access point, set these filters:

- On the IP Tunnels screen, check the **Allow IP Multicast** check box.
- In the IP Tunnel Transmit 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, in the IP Tunnel Transmit 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, set this filter to allow for the necessary IP tunneling:

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

Comparing IP Tunnels to Mobile IP

MobileLAN access WA2XG family of access points 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 handheld 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

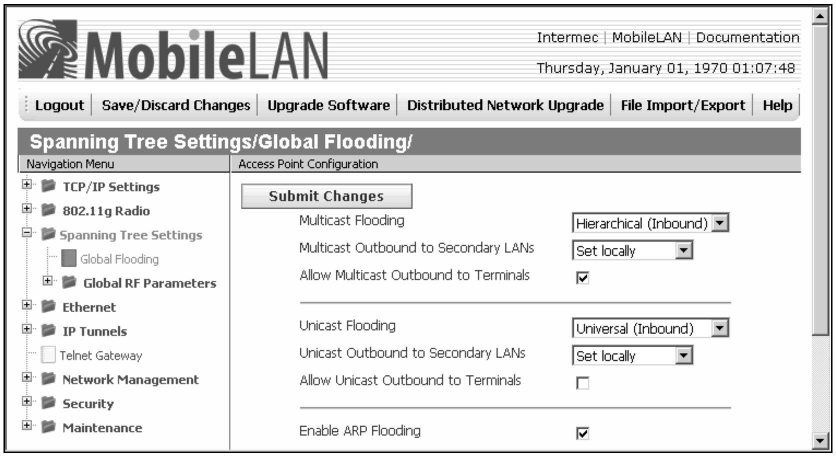
When the destination address is unknown, most bridges flood frames on all ports. Most wireless end devices operate at lower speeds than the Ethernet can support; therefore, indiscriminate flooding from a busy Ethernet network can consume a substantial portion of the available wireless bandwidth and reduce 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 Navigation Menu, click **Spanning Tree Settings** > **Global Flooding**. The Global Flooding screen appears.



Thursday, January 01, 1970 01:07:48

Spanning Tree Settings/Global Flooding/

Multicast Flooding: Hierarchical (Inbound)
Multicast Outbound to Secondary LANs: Set locally
Allow Multicast Outbound to Terminals ☑

Unicast Flooding: Universal (Inbound)
Unicast Outbound to Secondary LANs: Set locally
Allow Unicast Outbound to Terminals ☐

Enable ARP Flooding ☑

2 Configure the Global Flooding 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" on page 30.

Global Flooding Parameter Descriptions

Parameter	Explanation
Multicast Flooding	Determines the flooding structure when this access point receives inbound multicast frames on non-root ports with unknown destination addresses: **Disabled:** You do not want the access point to flood any inbound multicast frames. **Universal:** 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. **Hierarchical:** The access point forwards the multicast frame only to the port to which the root access point is attached.
Multicast Outbound to Secondary LANs	Appears only if **Multicast Flooding** is enabled. Specifies if outbound multicast frames with unknown destination addresses are flooded toward secondary LANs: **Enabled:** 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. **Set Locally:** The designated bridges control flooding on their LANs.
Allow Multicast Outbound to Terminals	Appears only if **Multicast Flooding** is enabled. 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.
Unicast Flooding	Determines the flooding structure when this access point receives inbound unicast frames on non-root ports with unknown destination addresses: **Disabled:** You do not want the access point to flood any inbound unicast frames. **Universal:** The access point forwards the unicast frame to every port. This option uses more bandwidth. **Hierarchical:** The access point forwards the unicast frame only to the port to which the root access point is attached.

Global Flooding Parameter Descriptions (continued)

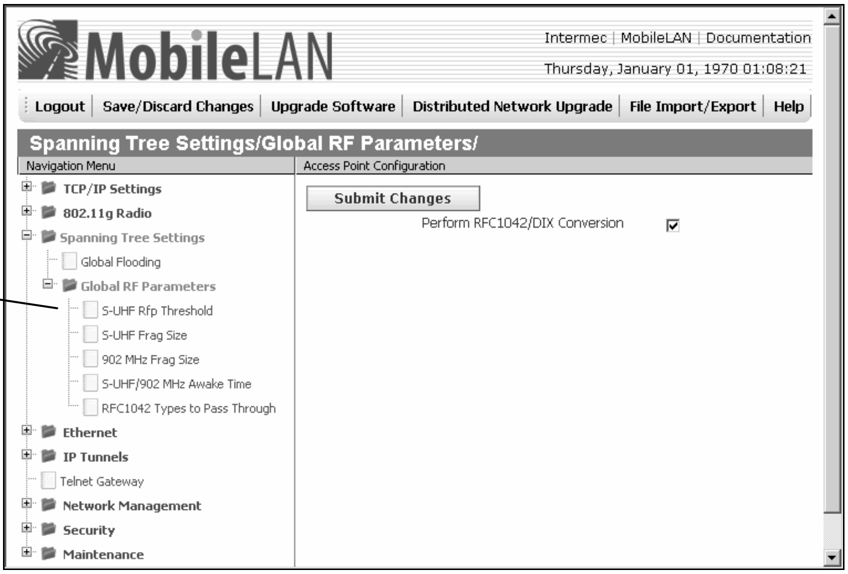
Parameter	Explanation
Unicast Outbound to Secondary LANs	Appears only if **Unicast Flooding** is enabled. Specifies if outbound unicast frames with unknown destination addresses are flooded toward secondary LANs: **Enabled:** The root access point controls flooding for all the designated bridges on secondary LANs. Enabling this parameter makes managing secondary LANs easier because you do not need to set secondary LAN flooding parameters. **Set Locally:** The designated bridges control flooding on their LANs.
Allow Unicast Outbound to Terminals	Appears only if **Unicast Flooding** is enabled. Determines if outbound unicast frames with unknown destination addresses are flooded toward end devices.
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** > **Global RF Parameters**. The Global RF Parameters screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 01:08:21
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Spanning Tree Settings/Global RF Parameters/
Navigation Menu
TCP/IP Settings
802.11g 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
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Submit Changes

Perform RFC1042/DIX Conversion ☑

Click to set the global RF parameters.

2 Configure the global RF parameters. Click the links in the **Global RF Parameters** menu to set more 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" on page 30.

Global RF Parameter Descriptions

Parameter	Explanation
Perform RFC1042/DIX Conversion	Determines how the access point will handle the conversion of RFC1042/DIX frames that are received on its radio 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 type 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 a 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.

Global RF Parameter Descriptions (continued)

Parameter	Explanation
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 (802.11g, 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:

- Understanding security
- Controlling access to access point menus
- Creating a secure spanning tree
- Enabling secure communications between access points and end devices

Understanding Security

MobileLAN access WA2XG family of access points provides 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 WA2XG 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 a password server to manage access point logins	X		
Configure a VLAN for each radio	X		
Use an access control list (ACL)			X
Use WEP 64/128 security		X	
Use an 802.1x security solution	X	X	X
Use Wi-Fi Protected Access (WPA) security	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 configure your wireless network for the maximum possible security that you deem necessary for the integrity of your network.

1 Change the SSID from its default value of INTERMEC and check the **Disallow Network Name of 'ANY'** check box. 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 "Controlling Access to Access Point Menus" on page 124.

3 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).

4 Or change the default login for users who need to configure or manage the access point. For help, see "Setting Up Logins" on page 126.

5 Create a secure spanning tree, which is between access points, and includes secure IAPP and secure wireless hops. For help, see "Creating a Secure Spanning Tree" on page 127.

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)" on page 127.

7 Configure VLANs that separate secure and non-secure communications in your network. For help, see "Configuring VLANs" on page 127.

8 Implement one of these mutually-exclusive security solutions (on each service set) to ensure secure communications between the access points and wireless end devices in your network:

Use 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. 802.11g radios support WEP 64/128 security. For help, see "Configuring WEP 64/128 Security" on page 127.

Use an 802.1x security solution. 802.1x security provides a framework to authenticate user traffic to a protected wireless network. Using 802.1x security provides secure data transmission by creating a secure spanning tree 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 the access point's embedded authentication server (EAS). For help, see "Implementing an 802.1x Security Solution" on page 127.

Use Wi-Fi Protected Access (WPA) security. WPA is a strongly enhanced, interoperable Wi-Fi security that addresses many of the vulnerabilities of Wired Equivalent Privacy (WEP). For help, see "Configuring Wi-Fi Protected Access (WPA) Security" on page 127.

For help troubleshooting security, see "Troubleshooting Security" on page 195.

When You Configure Different SSIDs With Different Security Settings

You can configure each 802.11g radio with up to four SSIDs or service sets. Although each service set shares one physical radio configuration, you can configure each service set for a different security environment. Multiple service sets are used primarily to allow one physical radio to support multiple virtual LANs (VLANs).

For example, you can configure:

- primary service set for WPA-802.1x.
- secondary 1 service set for WPA-PSK and VLAN 13.
- secondary 2 service set for Dynamic WEP/802.1x and VLAN 150.

Note: Enabling multiple services sets is not part of the Wi-Fi standard.

Before you configure different SSIDs with different security settings, verify that your wireless end devices perform active scanning. In active scanning, an end device sends a probe request to the SSID that it wants to associate with. If the probe request matches an SSID that belongs to any of the service sets, then the access point radio sends a probe response from that service set. Probe requests contain a security bit that advertises the type of security the service set is using. If the end device's security setting does not match the probe request's security bit, the end device cannot associate. Intermec's newer end devices with newer 802.11g radios (such as the CK30 and CV60) work in a mixed security environment.

End devices that perform passive scanning do not support a mixed security environment. In passive scanning, an end device listens for beacons (sent by the access point radio's primary service set), picks one that it likes, and associates with it. Beacons are only sent by the primary service set and contain the SSID and security bit that advertises the type of security the primary service set is using.

Note: If the **Disallow SSID (Network Name) of 'ANY'** check box is checked, the beacon does not contain the SSID.

If the end device's security setting does not match the beacon's security bit, the end device cannot associate. Therefore:

- if any type of security is set on the primary service set, then the secondary service sets should also the same type of security.
- if no security is set on the primary service set, then the secondary service sets cannot use any type of security.

For example, you have an access point with an 802.11g radio. You configure the primary service set for WPA-PSK and the secondary 1 service set with no security. An end device with an 802.11b radio is configured with no security and you may expect it to associate with the secondary 1 service set. However, the end device receives a beacon from the access point that indicates that security is being used. Therefore, the end device will not associate with the access point.

Another important consideration is that the service set that allows wireless hops should have the strongest security configuration possible for your environment. Do not enable wireless hops on the ports that have no security. WAPs configured on the other service sets will hear the unencrypted hellos on the wireless hop port and those WAPs will attach to the spanning tree, even though they should not.

When You Include Multiple RADIUS Servers on the RADIUS Server List

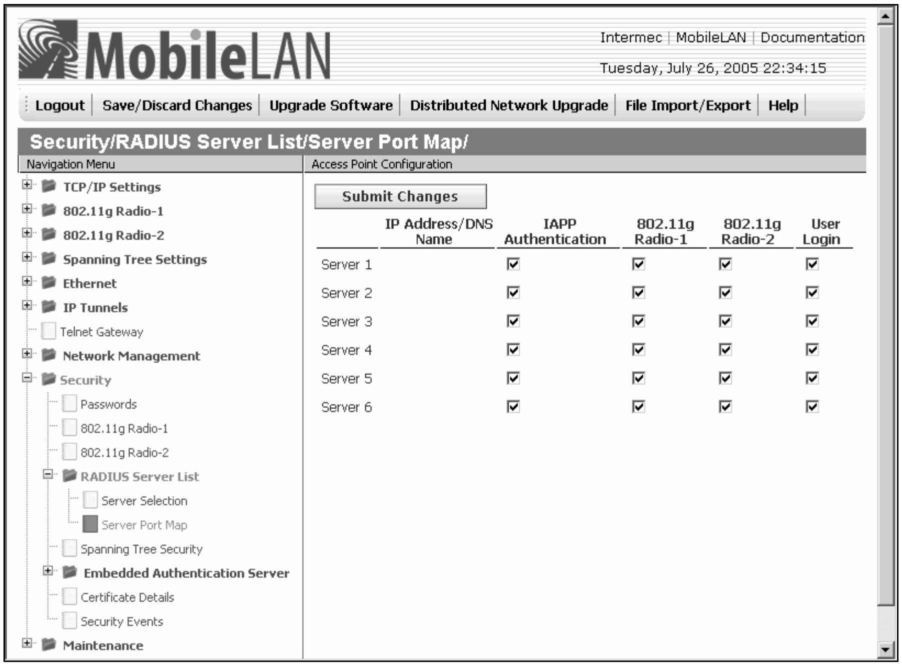
You can use configure multiple RADIUS servers to act as password servers, to support ACLs, to use in an 802.1x security solution as authentication servers, and to use in an WPA-802.1x security solution as authentication servers. If you don't configure the server port map, the access point uses the first RADIUS server (Server 1) in the list as the main server. Other servers are simply backup servers.

- If the first RADIUS server responds and the client's information does not appear in that server's database, the client is blocked. The access point does not check the databases on any other RADIUS servers.
- If the first RADIUS server goes down during the operation and a RADIUS server lookup needs to occur, the authenticator will time out looking for the first server. The authenticator looks for the next server in the list. If the authenticator finds the next server, it stays with that server forever, even if the first server comes back. If the backup server goes down, the authenticator continues looking down the list and eventually wraps around to the first server again.

However, you can configure the server port map so that the access point uses different RADIUS servers to serve different ports.

To configure the server port map

- In the Navigation Menu, click **Security** > **RADIUS Server List** > **Server Port Map**. The Server Port Map screen appears with the **IP Address/DNS Name** column populated with the RADIUS servers that you configured in the Server Selection screen.



	IP Address/DNS Name	IAPP Authentication	802.11g Radio-1	802.11g Radio-2	User Login
Server 1		☑	☑	☑	☑
Server 2		☑	☑	☑	☑
Server 3		☑	☑	☑	☑
Server 4		☑	☑	☑	☑
Server 5		☑	☑	☑	☑
Server 6		☑	☑	☑	☑

For example, a company has a corporate office and a remote distribution center. At each location, the local users have an SSID and security settings that match their local RADIUS server. When users travel to the other site, they still authenticate to their local RADIUS server.

Controlling Access to Access Point Menus

There are several ways that you can manage who can configure and manage the access points in your network:

- Enable/disable access methods.
- Set up individual logins.
- Change the default logins and create a read-only login.

The next sections explain how to implement these strategies.

Enabling Access Methods

There are five 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
- TFTP
- MobileLAN access Utility or another program that uses ICMP echo
- Wavelink Avalanche client management system. For help, see “Using the Wavelink Avalanche Client Management System” on page 166.

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.

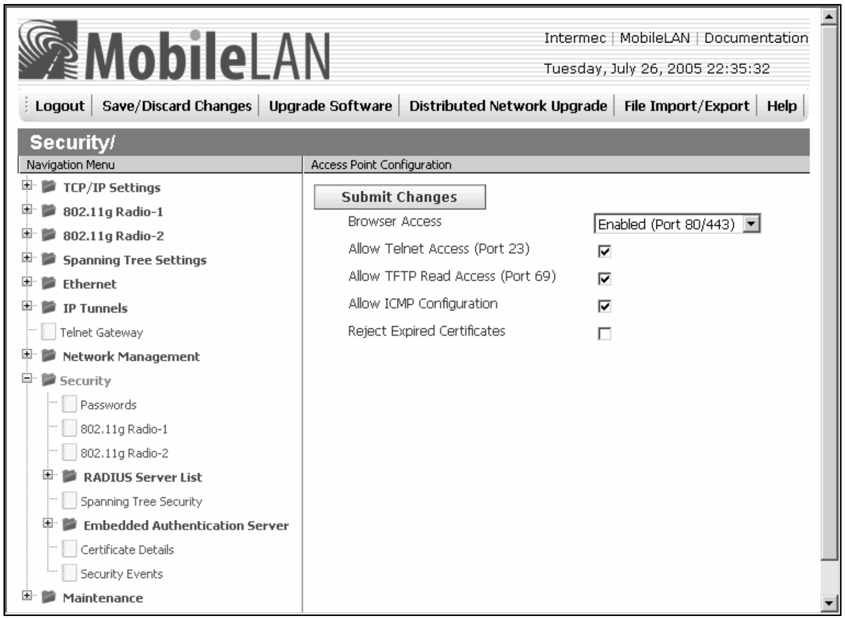
Note: To prevent access by MobileLAN manager or another SNMP management station, in the Navigation Menu, click **Network Management**. Clear the **Enable SNMPv3** check box and the **Enable SNMP v1/v2c** check box.

Note: To prevent access by a Wavelink Avalanche client management system, in the Navigation Menu, click **Network Management**. Clear the **Allow Avalanche Access** check box.

You can also enable or disable the **Reject Expired Certificates** check box. This check box is disabled by default. When enabled, you must make sure that the access point clock is set to the correct date and time. Then, if the access point is acting as an embedded authentication server or if your network is using 802.1x security and the certificate dates of any devices that are trying to communicate to the network have expired, the access point will not allow the devices to communicate with the network.

To enable or disable access methods

1 In the Navigation Menu, click **Security**. The Security screen appears.



Browser Access: Enabled (Port 80/443)
Allow Telnet Access (Port 23) ☑
Allow TFTP Read Access (Port 69) ☑
Allow ICMP Configuration ☑
Reject Expired Certificates □

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" on page 30.

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.
Allow Telnet Access (Port 23)	Determines if users can use a telnet session (or communications program) to configure or manage this access point. Do not clear this check box if you plan to configure the Telnet Gateway and allow wireless clients to upgrade the access point over the telnet port. For details, see page 206.
Allow TFTP Access (Read-Only)	Determines if users can use TFTP clients to exchange files with the access point.
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.
Reject Expired Certificates	Determines if this access point verifies that certificate dates of devices are valid. If a certificate date is not valid, the device is not allowed to communicate with the network.

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 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” on page 127. You can either configure an EAS or you can use an external RADIUS server as a password server.
- access points, which are the RADIUS clients.

If you use a password server, you enable RADIUS for login authorization. That is, when a user attempts to log in to the access point, the user must enter a user name and password. This login is sent through the RADIUS client (access point) to the RADIUS server. The server compares the login to its list of authorized logins. If a match is found, the server returns an access-accept frame and the user is logged in to the access point with read/write privileges.

If no RADIUS server 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.

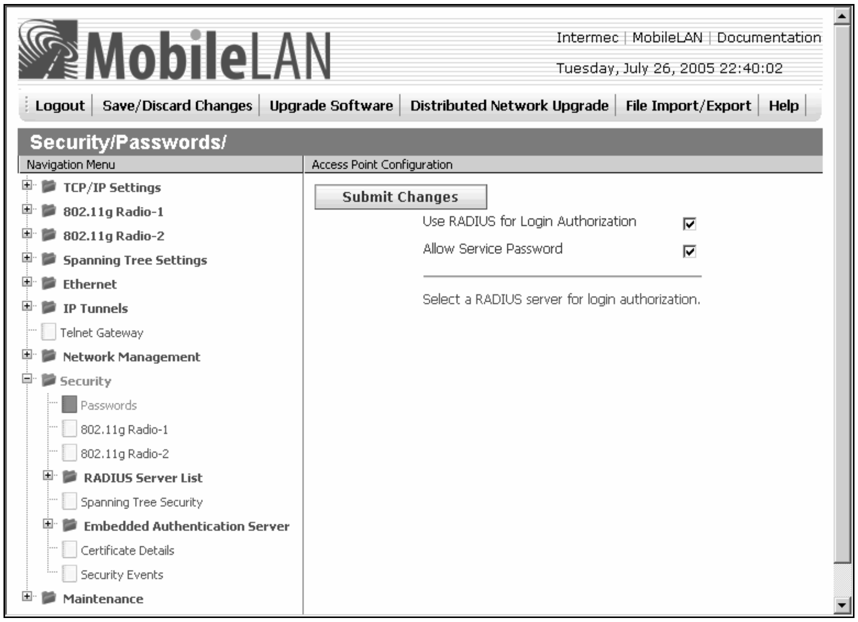
If you do not want to enable RADIUS authorization, you should change the default login user name and password. You may also want to change the read-only password. For help, see “Changing the Default Login” on page 127.

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 EAS or an external RADIUS server.

To configure the access point to use a password server

1 In the Navigation Menu, click **Security** > **Passwords**. The Passwords screen appears.



Use RADIUS for Login Authorization ☑

Allow Service Password ☑

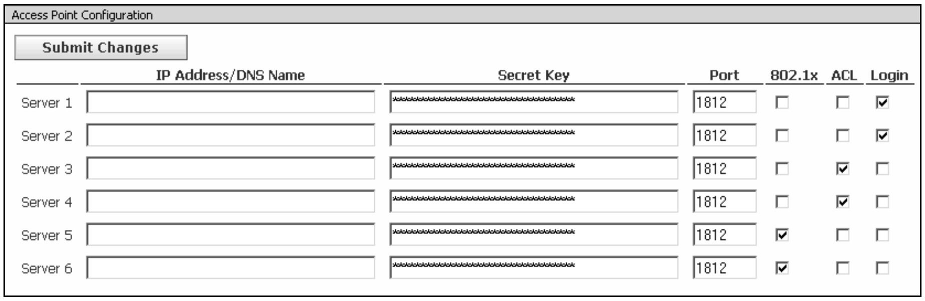
Select a RADIUS server for login authorization.

2 Check the **Use RADIUS for Login Authorization** check box.

3 (Optional) Make sure the **Allow Service Password** check box is checked.

4 Click **Submit Changes** to save your changes.

5 Configure the password server by clicking **Select a RADIUS server for login authorization**. The RADIUS Server List screen appears.



Access Point Configuration

Submit Changes

	IP Address/DNS Name	Secret Key	Port	802.1x	ACL	Login
Server 1		**	1812	□	□	☑
Server 2		**	1812	□	□	☑
Server 3		**	1812	□	☑	□
Server 4		**	1812	□	☑	□
Server 5		**	1812	☑	□	□
Server 6		**	1812	☑	□	□

6 For each password server, enter the IP address or DNS name, enter the shared secret key, port number, and check the **Login** check box.

Note: If you enter more than one password server, see page 123 for a description of how the access point uses the servers.

7 Configure the password server database:

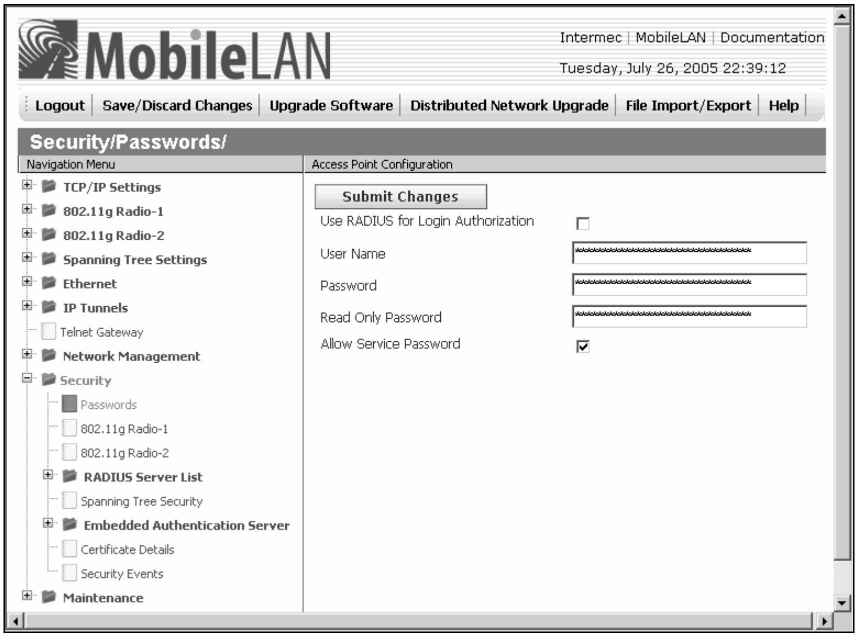
- In the EAS database, in the **Type** field choose Login and then enter the user name and password for each login. For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS).”
- For help configuring an external RADIUS server database, see the documentation that came with your server.

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 and create a read-only password.

To set up logins

1 In the Navigation Menu, click **Security** > **Passwords**. The Passwords screen appears.



Use RADIUS for Login Authorization □

User Name ********************************

Password ********************************

Read Only Password ********************************

Allow Service Password ☑

2 Verify that the **Use RADIUS for Login Authorization** check box is cleared.

3 Click **Submit Changes**.

4 Configure the parameters. 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” on page 30.

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.

Password Parameter Descriptions (continued)

Parameter	Description
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.

Creating a Secure Spanning Tree

When you configure a radio to use 802.1x security, you automatically enable spanning tree security, which can be used for both wired and wireless access points (WAPs). However, if you configure a radio to use another security solution, you may want to still create a secure spanning tree. A secure spanning tree has two functions:

1 To require authentication of any access point attempting to join the spanning tree.

2 To provide encryption of critical Inter-Access Point Protocol (IAPP) frames.

The three authentication methods that you can use to secure the spanning tree: Simple Wireless Authentication Protocol (SWAP), TTLS, or TLS.

SWAP is an Intermec proprietary protocol that is based on the EAP-MD5 challenge. Since it requires less processing power, it requires less memory and you can use it on all access points. Also, SWAP does not require an authentication server so it is easier to configure. With these advantages, SWAP is sufficient for most users. TTLS and TLS are industry standard protocols. However, they require more administrative support.

When deciding on which type of spanning tree security to use, the supplicant access point and the authenticator will negotiate an authentication method that can be used by both. If the **Allow SWAP** check box is checked on both access points, SWAP will always be used. If the **Allow SWAP** check box is cleared on one or both of the access points, either TTLS or TLS will be used, depending on the setting of the **Preferred Protocol** field of the supplicant access point.

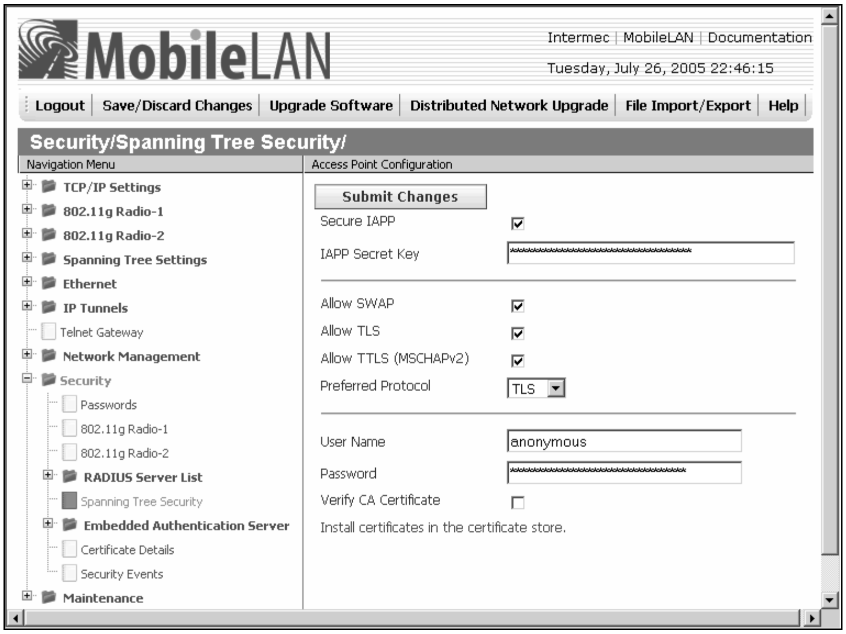
Note this potential problem:

- 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 create a secure spanning tree

Note: You do not need to perform this procedure if you are implementing an 802.1x security solution. 802.1x authentication automatically enables secure IAPP and secure wireless hops. See "Implementing an 802.1x Security Solution" on page 127.

1 In the Navigation Menu, click **Security** > **Spanning Tree Security**. The Spanning Tree Security screen appears.



Secure IAPP ☑

IAPP Secret Key ********************************

Allow SWAP ☑

Allow TLS ☑

Allow TTLS (MSCHAPv2) ☑

Preferred Protocol TLS

User Name anonymous

Password ********************************

Verify CA Certificate □

Install certificates in the certificate store.

2 Check the **Secure IAPP** check box.

3 Click **Submit Changes** to save your changes.

4 In the **IAPP Secret Key** field, enter a secret key. This secret key must be between 16 and 32 bytes.

5 Determine how the access points authenticate to the network:

- Check the **Allow SWAP** check box if you have older access points or you are not implementing an 802.1x security solution.
- Check the **Allow TLS** check box, if you are implementing an 802.1x security solution and you want to use TLS. The access point must have a server certificate loaded on it.

- Check the **Allow TTLS (MSCHAPv2)** check box, if you are implementing an 802.1x security solution and you want to use TTLS. You must also enter a User Name and Password that matches an entry in the authentication server.

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" on page 30.

7 Repeat Steps 1 through 6 for each access point in your spanning tree. All access points must have the same IAPP secret key to communicate with each other.

To obtain information about the relationship of the access point in the spanning tree to the other devices that are connected to the spanning tree, click **Maintenance** > **AP Connections**. The AP Connections screen lists the station radios (including ones in other access points) that are communicating with the root access point. For help, see "Viewing AP Connections" on page 173.

Enabling Secure Communications Between Access Points and End Devices

There are several ways that you can ensure secure communications between access points and wireless end devices in your network:

- Use an access control list (ACL).
- Configure virtual LANs (VLANs).
- Configure WEP 64/128 security.
- Implement an 802.1x security solution.
- Configure Wi-Fi Protected Access (WPA) security.

The next sections explain how to configure these methods.

Using an Access Control List (ACL)

You can use an access control list (ACL) that contains 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:

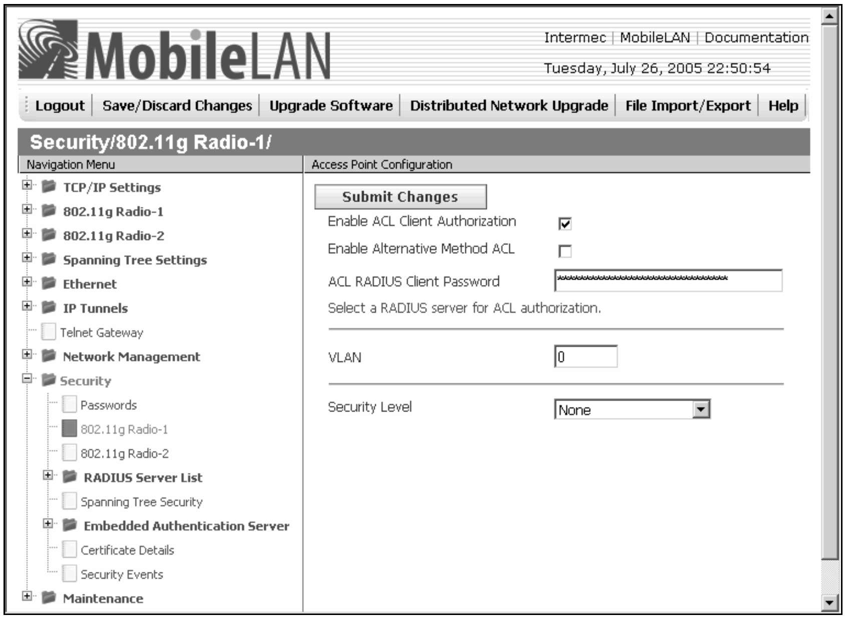
- a RADIUS server on the network that contains the ACL. You can either use an external RADIUS server or you can configure an EAS. For help, see Chapter 7, "Configuring the Embedded Authentication Server (EAS)."
- access points, which are the RADIUS clients.

If the access point has two radios, or if the access point contains one 802.11g radio with multiple service sets, 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 security 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 In the Navigation Menu, click **Security** and then click the radio service set you are configuring. The appropriate radio screen appears.



Enable ACL Client Authorization ☑

Enable Alternative Method ACL □

ACL RADIUS Client Password ******************************

Select a RADIUS server for ACL authorization.

VLAN 0

Security Level None

2 Check the **Enable ACL Client Authorization** check box if you want to use an ACL to authorize end devices to communicate with the network.

3 Click **Submit Changes** to save your changes.

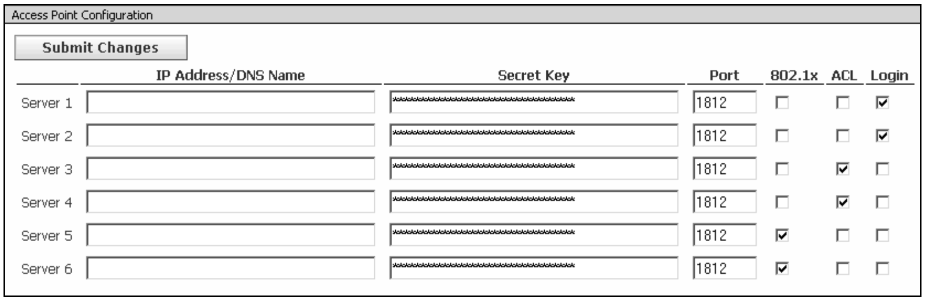
4 Normally, the access point issues RADIUS requests with the password of the end device that is trying to communicate with the network.

Check the **Enable Alternative Method ACL** check box if you want the access point to issue RADIUS requests with the user name and password both set to the MAC address of the end device that is trying to communicate with the network.

5 (External RADIUS server only) In the **ACL RADIUS Client Password** field, enter the password that is used to sign RADIUS access requests for all end devices attached to this access point. This password must match the password that is configured in the RADIUS server.

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” on page 30.

7 Configure the RADIUS server by clicking **Select a RADIUS server for ACL authorization**. The RADIUS Server List screen appears.



	IP Address/DNS Name	Secret Key	Port	802.1x	ACL	Login
Server 1		********************************	1812	□	□	☑
Server 2		********************************	1812	□	□	☑
Server 3		********************************	1812	□	☑	□
Server 4		********************************	1812	□	☑	□
Server 5		********************************	1812	☑	□	□
Server 6		********************************	1812	☑	□	□

8 For each RADIUS server, enter the IP address or DNS name, enter the shared secret key, port number, and check the **ACL** or **Login** check box.

Note: If you enter more than one server, see page 123 for a description of how the access point uses the servers.

9 Configure the database. Enter the MAC address for each end device radio that is allowed to communicate with the network:

- In the EAS database, in the **Type** field choose **ACL** and then enter the MAC address for each end device radio.

  Or, if you checked the **Enable Alternative Method ACL** check box, in the **Type** field choose **Login** and then enter the MAC address for each end device radio in both the user name and password fields.

  For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS).”

- For help configuring an external RADIUS server database, see the documentation that came with your server. In the database, you will also need to enter the ACL RADIUS client password. The default password is `wireless` (case-sensitive).

Configuring VLANs

Virtual LANs (VLANs) make it easy to create and manage logical groups of wireless end devices that communicate as if they were on the same LAN. You can group all wireless users on a particular VLAN in order to manage the IP address space differently. Or, you can use VLANs to separate secure and non-secure traffic. For example, you may grant your employees full access to your network, while routing all traffic from visitors to the Internet. The access points may be configured to participate in a properly configured VLAN.

You can configure each 802.11g radio with up to four SSIDs, creating up to four service sets. Each service set shares one physical radio configuration, but you may customize its security configuration. Therefore, each service set can be configured to support a separate VLAN.

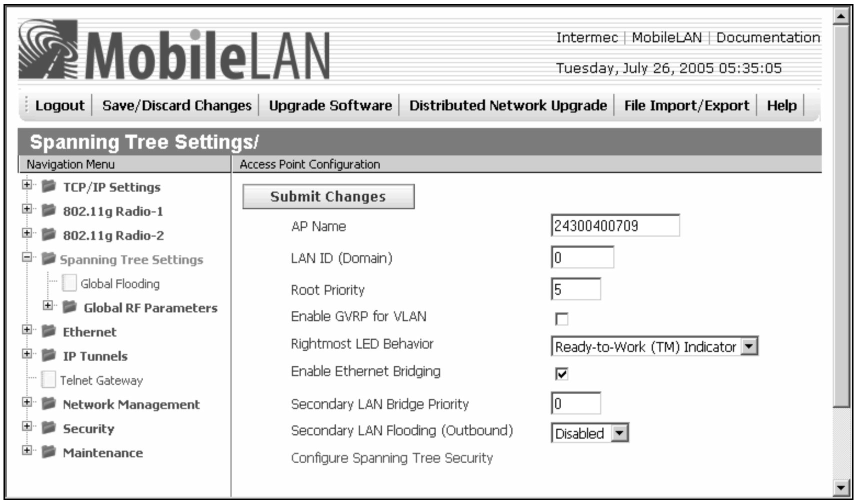
You configure each radio (or each service set) as a master radio with a unique SSID and security solution. Then, you distribute the SSID of the secure network to your end devices and the SSID of the non-secure network to your customers.

The access points support the 802.1Q standard for VLAN tagging. When the access point receives a frame from an end device, it applies the appropriate VLAN tag to the frame and then bridges the VLAN-tagged frame to the wired network. If you configure the VLAN field to 0, no VLAN tag will be applied and the frames will be put on the wired network as normal Ethernet frames. A VLAN-capable Ethernet switch receives the VLAN-tagged frame and routes it appropriately. Only VLAN-aware devices understand frames with VLAN tags; end devices only understand and accept frames that are meant for them that do not have a VLAN tag.

In order for the spanning tree to work, all access points must be on the same Native port on the Ethernet switch. The switch must be able to support a “hybrid” VLAN, which means the switch can support both VLAN-tagged and normal Ethernet frames on the switch port. The access point only encapsulates wireless traffic. Any communication with the access point across the wired network is always normal Ethernet traffic.

To configure a VLAN

1 In the Navigation Menu, click **Spanning Tree Settings**. The Spanning Tree Settings screen appears



AP Name	24300400709
LAN ID (Domain)	0
Root Priority	5
Enable GVRP for VLAN	☐
Rightmost LED Behavior	Ready-to-Work (TM) Indicator
Enable Ethernet Bridging	☑
Secondary LAN Bridge Priority	0
Secondary LAN Flooding (Outbound)	Disabled
Configure Spanning Tree Security	

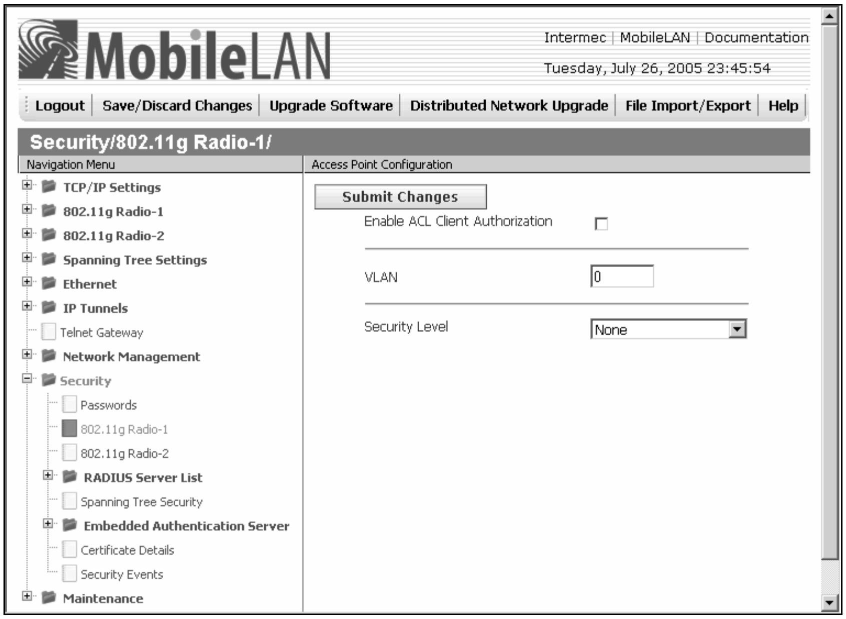
2 Check or clear the **Enable GVRP for VLAN** check box.

- Check the check box if the VLAN switch is configured to dynamically configure its ports based on the end devices' needs.
- Clear the check box if the VLAN switch is statically configured to always forward specific VLANs to specific ports.

3 Click **Submit Changes** to save your changes.

4 In the Navigation Menu, click **Security**. If you have enabled more than the primary service set, you can configure each secondary service set for a different VLAN.

5 Under the **Security** link, click the radio service set you want to configure for the VLAN. This screen appears.



Enable ACL Client Authorization □

VLAN 0

Security Level None

6 In the **VLAN** field, enter the VLAN number that encapsulates all frames received on this radio port. This value must match the values that are set in the VLAN-capable Ethernet switches on the primary LAN.

Note: The value in the **VLAN** field is also called the VLAN tag.

7 Repeat Steps 5 and 6 to assign a unique VLAN tag to each service set that you want to configure to support a VLAN.

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" on page 30.

Configuring WEP 64/128 Security

You can configure static WEP keys 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.

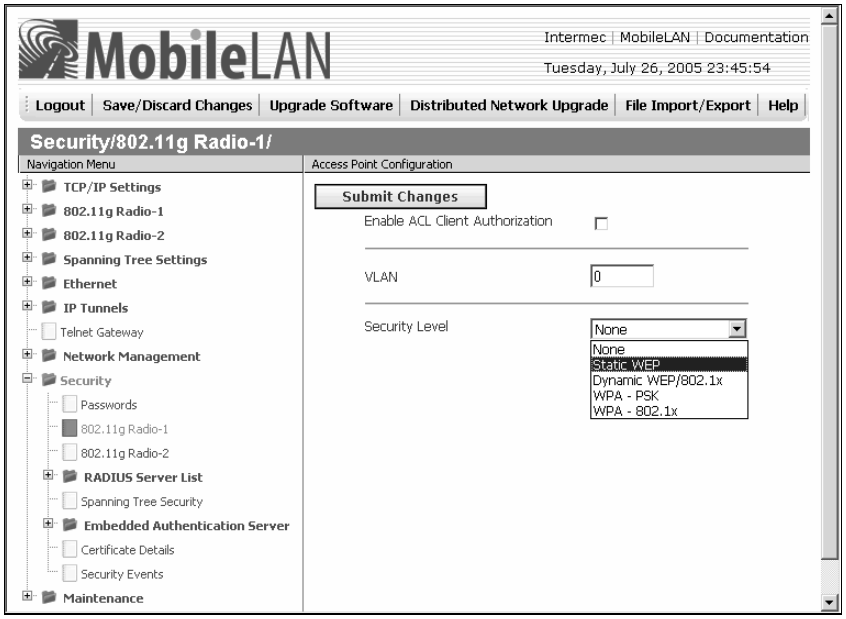
802.11g radios support WEP 64/128 security:

- WEP 64 has four 40-bit encryption keys and one 24-bit initialization vector (IV) key. 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. Enter 13 ASCII characters or hex pairs.

To configure WEP 64/128 security

1 In the Navigation Menu, click **Security** and then click the radio service set you are configuring. The appropriate radio screen appears.

2 In the **Security Level** field, select **Static WEP**.

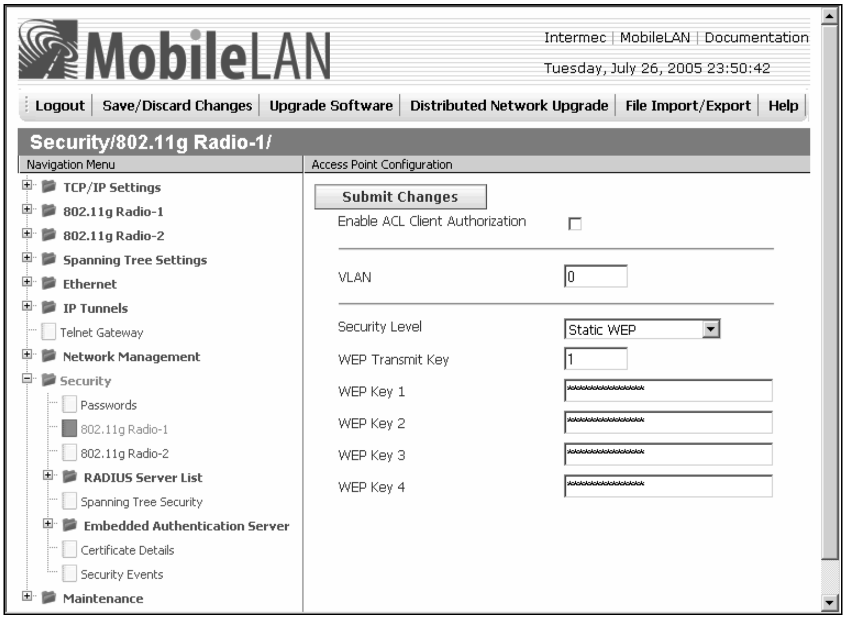


Enable ACL Client Authorization □

VLAN 0

Security Level None

3 Click **Submit Changes** to save your changes. This screen appears.



Enable ACL Client Authorization □

VLAN 0

Security Level Static WEP

WEP Transmit Key 1

WEP Key 1 **************

WEP Key 2 **************

WEP Key 3 **************

WEP Key 4 **************

4 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.

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” on page 30.

WEP Security Parameter Descriptions

Parameter	Explanation
Security Level	Select **Static WEP** from the drop-down menu to use WEP 64/128 security.
WEP Transmit Key	Determines which of the four WEP keys this access point uses to transmit data.
WEP Key 1 WEP Key 2 WEP Key 3 WEP Key 4	For WEP 64, enter five ASCII characters or five hex pairs. For WEP 128, 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.

Implementing an 802.1x Security Solution

You can implement 802.1x security in your 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:

- 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. 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.
- Supplicants, which is software that is running on end devices that are 802.1x-enabled. These end devices have a radio that is 802.1x-enabled and a supplicant (EAP-TLS, EAP-TTLS, or PEAP) loaded on them. Supplicants 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.
- A trusted certificate authority (CA), which issues digital authentication certificates. Intermec and others can provide the service of acting as a CA and can issue certificates. For more information, contact your local Intermec representative.

- The authentication server and end devices with supplicants need certificates. A CA certificate is the root certificate or public key. A server certificate (sometimes referred to as the client certificate) is the private key. For more details, see "About Certificates" on page 152.
  - The authentication server must have both a CA certificate and a server certificate installed on it.
  - An end device with an EAP-TTLS supplicant or a child access point using secure IAPP-TTLS needs only the CA certificate.
  - Any device with an EAP-TLS supplicant (end device or child access point) needs both the CA certificate and the server certificate.
  - If the child access point is using SWAP and is an authenticator, it does not need any certificates loaded on it. Only the authentication server and supplicants need certificates.

If the access point has two radios, or if the access point contains one 802.11g radio with multiple service sets, you can implement 802.1x security on one radio network or both radio networks, as long as the radio supports 802.1x security.

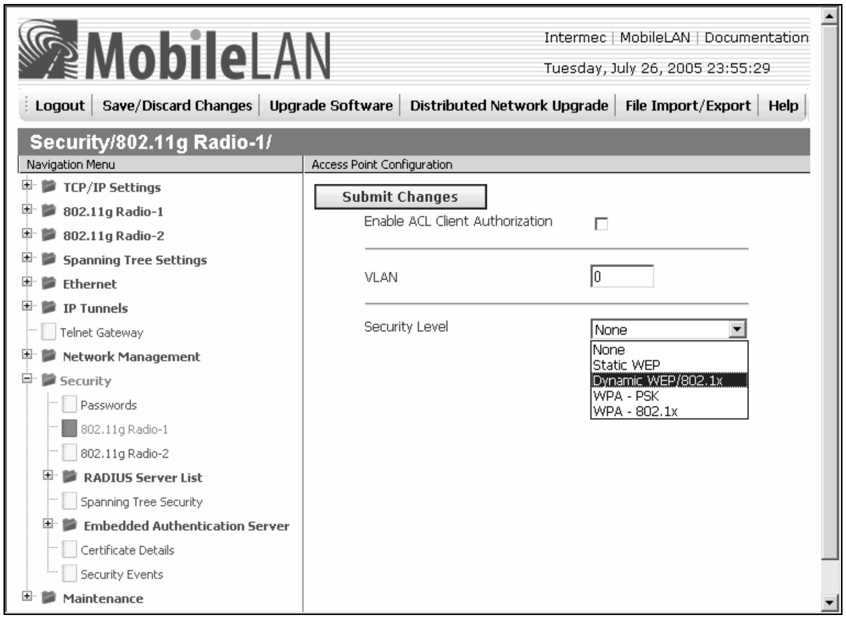
For example, you have an access point with dual 802.11g radios and some end devices that have a supplicant and some end devices that do not have a supplicant. In the access point, you can configure one 802.11g radio to use 802.1x security and the other 802.11g radio to use an ACL.

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. In the Navigation Menu, click **Security** and then click the radio service set that you are configuring. The appropriate radio screen appears.
2. In the **Security Level** field, select **Dynamic WEP/802.1x**.

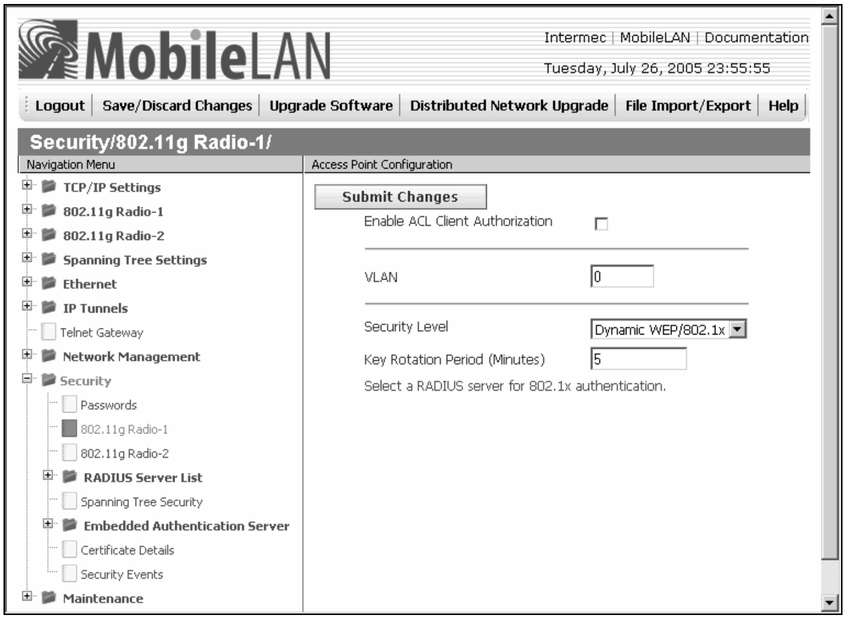


Enable ACL Client Authorization □

VLAN 0

Security Level None

3 Click **Submit Changes** to save your changes. This screen appears.



Enable ACL Client Authorization □

VLAN 0

Security Level Dynamic WEP/802.1x

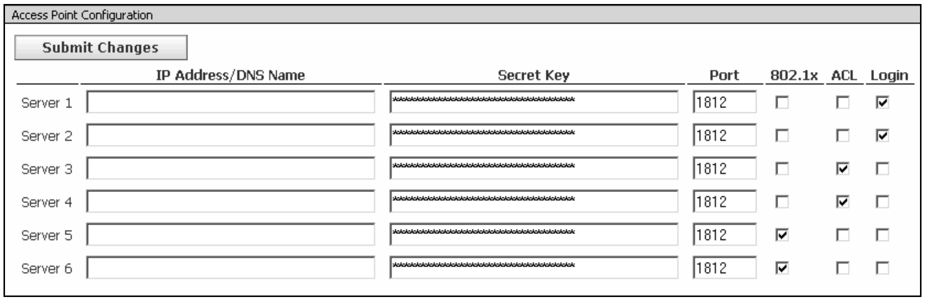
Key Rotation Period (Minutes) 5

Select a RADIUS server for 802.1x authentication.

4 In the **Key Rotation Period (Minutes)** field, enter how often (in minutes) the access point generates a new WEP key to distribute to the end devices.

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” on page 30.

6 Configure the RADIUS server by clicking **Select a RADIUS server for 802.1x authentication**. The RADIUS Server List screen appears.



	IP Address/DNS Name	Secret Key	Port	802.1x	ACL	Login
Server 1		**	1812	□	□	☑
Server 2		**	1812	□	□	☑
Server 3		**	1812	□	☑	□
Server 4		**	1812	□	☑	□
Server 5		**	1812	☑	□	□
Server 6		**	1812	☑	□	□

7 For each authentication server, enter the IP address or DNS name, enter the shared secret key, port number, and check the **802.1x** check box.

Note: If you enter more than one authentication server, see page 123 for a description of how the access point uses the servers.

8 Configure the database. Depending on the authentication type, enter the information for each end device that is allowed to communicate with the 802.1x network:

- In the EAS database, in the **Type** field choose the authentication type and then enter the information for each end device. For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS).”
- For help configuring an external RADIUS server, see the documentation that came with your server. You need to enter each authenticator’s IP address and the shared secret key. In the database, you need to enter the information for each end device.

Enabling Secure Communications Between Access Points

When you configure a radio to use 802.1x security, you automatically enable spanning tree security, which can be used for both wired access points and WAPs. A secure spanning tree has two functions:

1 To require authentication of any access point attempting to join the spanning tree.

2 To provide encryption of critical Inter-Access Point Protocol (IAPP) frames.

There are three authentication methods that you can use to secure the spanning tree: SWAP, TTLS, or TLS.

When the Access Point Is the Supplicant

By default, TTLS is enabled. If you want to use TTLS, you must also enter a user name and password. This login must match an entry in the authentication server database. When the access point is acting as a supplicant and the authentication server offers the TTLS protocol, the access point sends its user name and password.

You can also enable TLS as the authentication method. You must install a server certificate on each access point that will use this method to authenticate to the network. When the access point is acting as a supplicant and the authentication server offers the TLS protocol, the access point sends its certificate credentials.

If you choose to use both TTLS and TLS, you must choose which protocol the access point offers first and the access point must have a login configured and a server certificate.

By default, Secure Wireless Authentication Protocol (SWAP) is also enabled. The access point tells the authenticator that it can perform SWAP. If the authenticator allows SWAP, SWAP is used. SWAP allows access points to authenticate using an EAP-MD5 challenge. If the supplicant or the authenticator does not allow SWAP, the authentication must happen at the authentication server using TTLS or TLS.

When the Access Point Is the Authenticator

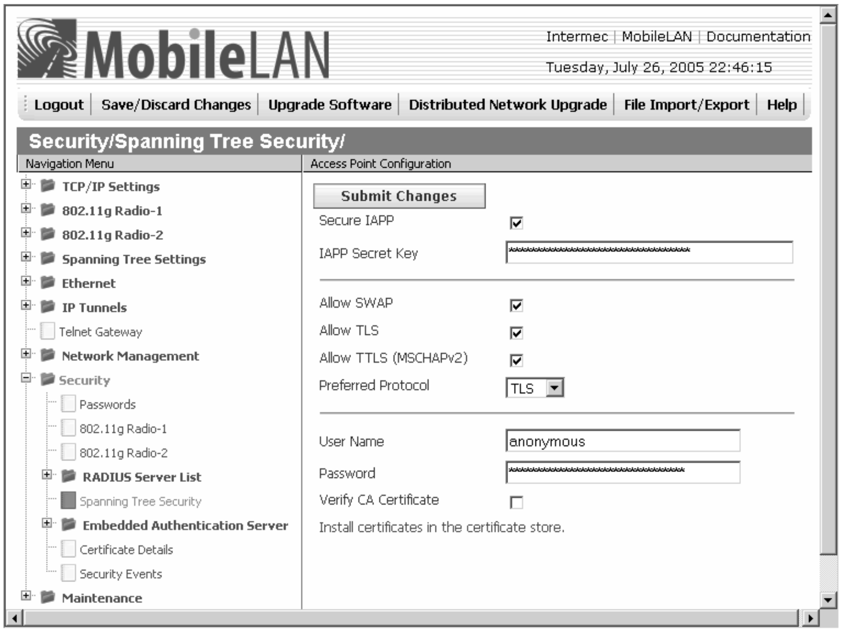
If the **Allow SWAP** check box is cleared, the access point that is acting as the authenticator will not perform any authentications using SWAP. Supplicants will need to authenticate with the authentication server using TTLS or TLS.

However, older access points do not support these authentication methods. If the **Allow SWAP** check box is checked, the access point that is acting as the authenticator will authenticate any supplicants that offer SWAP. Note that SWAP authentication is susceptible to downgrade attacks from rogue supplicants as it is easier to break SWAP than TLS or TTLS.

Configuring Spanning Tree Security

Note: If you are implementing an 802.1x security solution, secure IAPP and secure wireless hops are automatically enabled.

1 In the Navigation Menu, click **Security** > **Spanning Tree Security**. The Spanning Tree Security screen appears.



Secure IAPP ☑

IAPP Secret Key ********************************

Allow SWAP ☑

Allow TLS ☑

Allow TTLS (MSCHAPv2) ☑

Preferred Protocol TLS

User Name anonymous

Password ********************************

Verify CA Certificate □

Install certificates in the certificate store.

2 In the **IAPP Secret Key** field, enter a secret key. This secret key must be between 16 and 32 bytes.

3 Choose which authentication methods you want to use to authorize the access point to communicate with the network. For help, see the next table.

4 Check the **Verify CA Certificate** check box and enter the authentication server common names to verify that the access point is connecting to the correct authentication server. Intermec recommends that you perform this step because it provides another layer of security.

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” on page 30.

6 Repeat Steps 1 through 5 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** > **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” on page 173.

Spanning Tree Security–Authentication Method Descriptions

Parameter	Description
Allow SWAP	Determines if this access point authenticates to other access points using SWAP.
Allow TLS	If the authentication server offers the TLS protocol for the authentication method, this check box determines if this access point can use its server certificate to authenticate to the network.
Allow TTLS (MSCHAPv2)	If the authentication server offers the TTLS protocol for the authentication method, this check box determines if this access point uses a login to authenticate to the network. This login must be in the authentication server database.
Preferred Protocol	If TLS and TTLS are enabled, this field specifies which protocol is sent to the authentication server when it sends an unsupported protocol.
User Name	Enter the user name of the access point when it uses TTLS to authenticate to the network.
Password	Enter the password of the access point when it uses TTLS to authenticate to the network.
Verify CA Certificate	Determines if you want to verify that the access point is connected to the correct authentication server. The server certificate signature is verified against the CA certificate and the server common name is verified against the authentication server common names that are configured in the access point.

Configuring Wi-Fi Protected Access (WPA) Security

Wi-Fi Protected Access (WPA) is a strongly enhanced, interoperable Wi-Fi security that addresses many of the vulnerabilities of Wired Equivalent Privacy (WEP). WPA bundles authentication, key management, data encryption, message integrity checks and counter measures in the event of a message attack into one implementation standard.

WPA provides stronger RC4 encryption over standard WEP with the Temporal Key Integrity Protocol (TKIP). In addition, the Michael algorithm provides forgery protection and message integrity. A four-way handshake between the client and access point ensures the reliable and secure distribution of key material needed for encryption and message integrity checks.

Currently, WPA satisfies some of the requirements in the IEEE 802.11i draft standard. When the standard is finalized, WPA will maintain forward compatibility.

WPA runs in Enterprise (802.1x) mode or PSK (pre-shared key) mode:

- In Enterprise mode, WPA provides user authentication using 802.1x authentication and the Extensible Authentication Protocol (EAP). An authentication server (such as a RADIUS server) must authenticate each device before the device can communicate with the wireless network.

- In PSK mode, WPA provides user authentication using a shared secret key between the access point and the end devices. It does not require an authentication server. WPA-PSK is a good solution for small offices or home offices that do not want to use an authentication server.

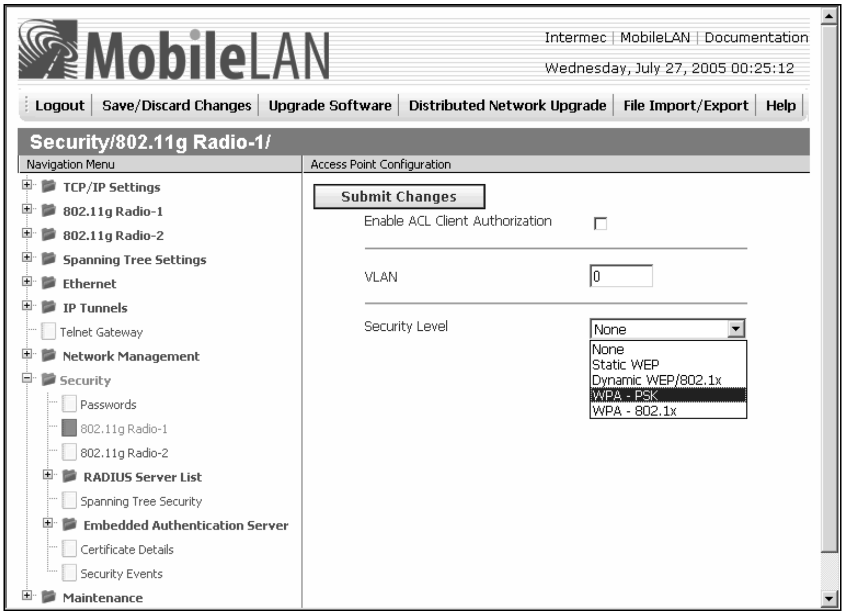
To use WPA security, you need:

- An access point with an radio that supports WPA
- End devices with a radio and software that support WPA
- (Enterprise mode only) An authentication 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. For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS).”

To configure WPA security

1 In the Navigation Menu, click **Security** and then click the radio service set you are configuring. The appropriate radio screen appears.

2 In the **Security Level** field, choose either WPA - PSK or WPA - 802.1x.



Enable ACL Client Authorization □

VLAN 0

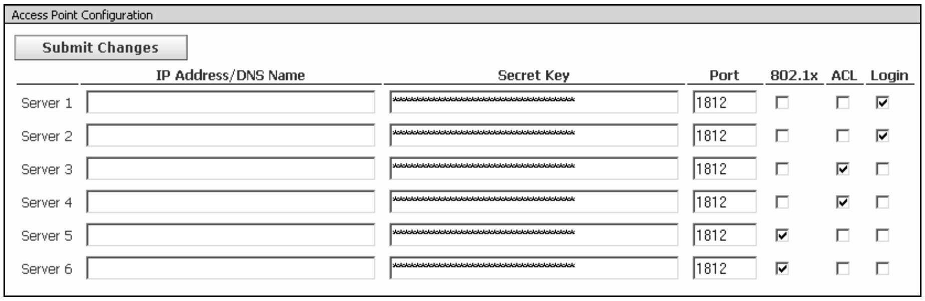
Security Level None

3 Click **Submit Changes** to save your changes. The screen changes, depending on the security level you choose.

4 Fill in the fields. For help, see “Configuring WPA - PSK Security” on page 127 or “Configuring WPA - 80.1x Security” on page 127.

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” on page 30.

6 (WPA – 802.1x mode only) Configure the RADIUS server by clicking **Select a RADIUS server for 802.1x authentication**. The RADIUS Server List screen appears.



Access Point Configuration

	IP Address/DNS Name	Secret Key	Port	802.1x	ACL	Login
Server 1		***********************************	1812	□	□	☑
Server 2		***********************************	1812	□	□	☑
Server 3		***********************************	1812	□	☑	□
Server 4		***********************************	1812	□	☑	□
Server 5		***********************************	1812	☑	□	□
Server 6		***********************************	1812	☑	□	□

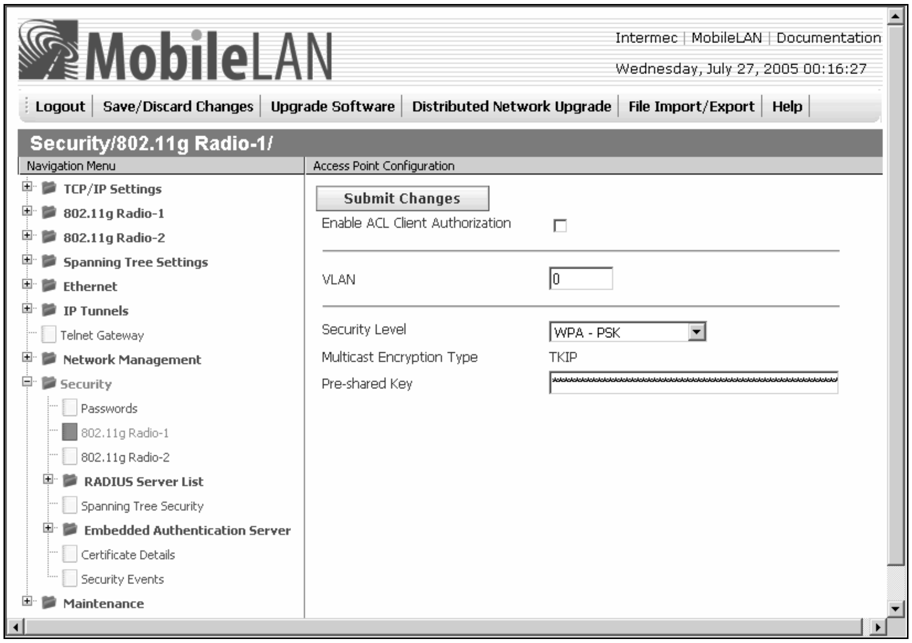
7 (WPA – 802.1x mode only) For each authentication server, enter the IP address or DNS name, enter the shared secret key, port number, and check the **802.1x** check box.

Note: If you enter more than one authentication server, see page 123 for a description of how the access point uses the servers.

8 (WPA – 802.1x mode only) Configure the database. Depending on the authentication type, enter the information for each end device that is allowed to communicate with the 802.1x network:

- In the EAS database, in the **Type** field choose the authentication type and then enter the information for each end device. For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS).”
- For help configuring an external RADIUS server, see the documentation that came with your server. You need to enter each authenticator’s IP address and the shared secret key. In the database, you need to enter the information for each end device.

Configuring WPA - PSK Security



Enable ACL Client Authorization □

VLAN 0

Security Level WPA - PSK

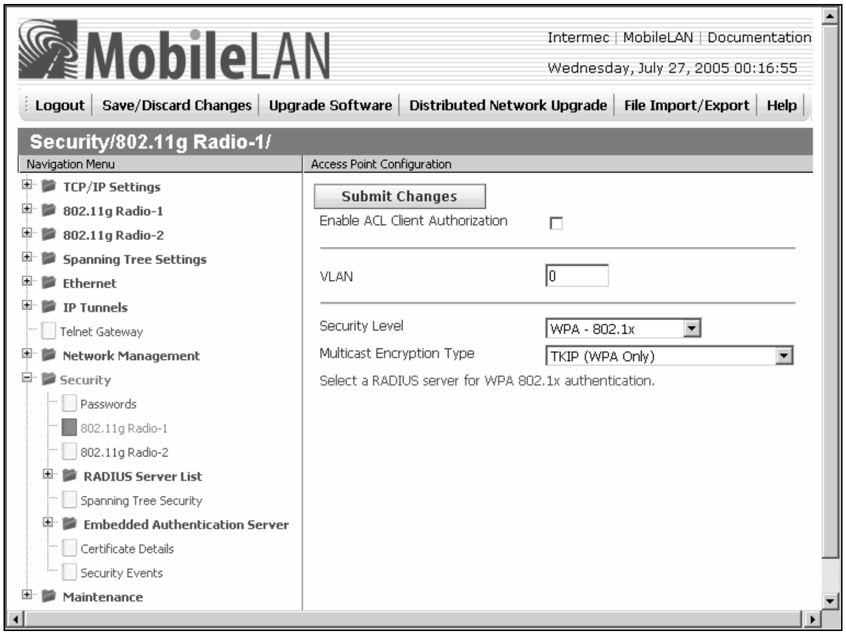
Multicast Encryption Type TKIP

Pre-shared Key **

WPA - PSK Security Parameter Descriptions

Parameter	Explanation
Multicast Encryption Type	Indicates that TKIP is used as the data encryption method for broadcast and multicast for this radio port. A station connected to this port may not select a weaker encryption method to exchange unicast frames.
Pre-shared Key	Allows you to enter the pre-shared key for WPA. You can enter up to a 256 (32 byte) hexadecimal value or up to a 63 character ASCII passphrase. To enter a hexadecimal key, start the value with 0x and follow it with 64 hexadecimal digits. If you omit the 0x, the value is treated as an ASCII passphrase and the key is derived from the passphrase using the PBKDF2 algorithm. A longer PSK is more secure than a short PSK.
Key Rotation Period (Minutes)	Allows you to specify the key rotation policy for encryption keys when using WEP in 802.1x and for TKIP group keys when using WPA. The value represents key duration in minutes. The default value is 5 minutes.

Configuring WPA - 802.1x Security



Enable ACL Client Authorization □

VLAN 0

Security Level WPA - 802.1x

Multicast Encryption Type TKIP (WPA Only)

Select a RADIUS server for WPA 802.1x authentication.

WPA - 802.1x Security Parameter Descriptions

Parameter	Explanation
Multicast Encryption Type	Allows you to select the data encryption method for broadcast and multicast for this radio port. A station connected to this port may not select a weaker encryption method to exchange unicast frames.
Key Rotation Period (Minutes)	Allows you to specify the key rotation policy for encryption keys when using WEP in 802.1x and for TKIP group keys when using WPA. The value represents key duration in minutes. The default value is 5 minutes.

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 embedded authentication server (EAS)
- About certificates
- Configuring the EAS

About the Embedded Authentication Server (EAS)

MobileLAN access WA2XG family of access points have 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, TTLS, and PEAP clients to connect to the network.

If you use the EAS, you may not need to buy an external RADIUS server. An EAS supports up to 128 database entries. If you need more database entries, 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 with unique security credentials.

Maximum Number of Simultaneous Authentications Supported

Type of RADIUS Server	Maximum Authentications
Password server	128
ACL authentication server	128
802.1x authentication server	60

About Certificates

Certificates encrypt communication between the internal RADIUS server, RADIUS clients, and the supplicants and HTTPS clients.

There are two types of certificates:

- The trusted certificate authority (CA) certificate (commonly referred to as the “root certificate” or “root cert”) is the public key. 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 2Kb.

- The server certificate (sometimes referred to as the client certificate) is the private key. Server certificates can be in either PKCS12 (*.P12/*.PFX) or *.PEM format.

Understanding Which Access Points Need Certificates

The next table summarizes when an access point needs to have a CA certificate and/or a server certificate installed on it.

Access Point	CA Certificate Needed	Server Certificate Needed
If you want to use the secure web browser (HTTPS) on this access point	No	Yes
If this access point is an authentication server in your WPA-802.1x network	Yes	Yes
If this access point is an authentication server in your 802.1x-enabled network	Yes	Yes
If this access point is a supplicant EAP-TTLS client	Yes	No
If this access point is a supplicant EAP-TLS client	Yes	Yes
If this access point is a backup RADIUS server	No	Yes
If the child access point is using SWAP and is an authenticator access point	No	No

Understanding Which Certificates Are Installed by Default

Your access point comes with 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.

Intermec can provide the service of acting as a certificate authority and can issue certificates. For more information, contact your local Intermec representative. Or you can install certificates from a third-party certificate authority.

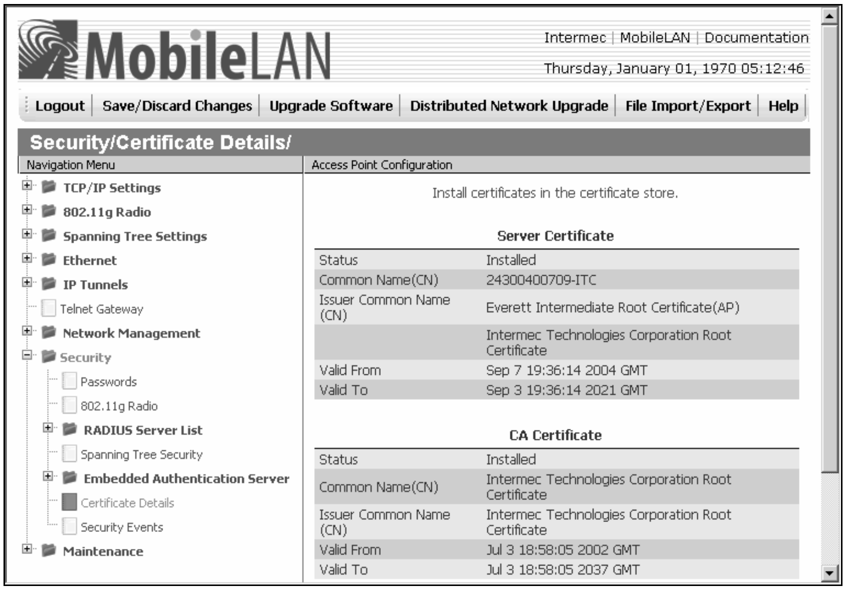
Note: Access points also come with a default server certificate (ValidforHTTPSOnly). This default certificate supports the secure web browser interface and provides basic security for clients running the TTLS authentication type. As described in the previous section, you may also need to a trusted CA certificate and/or a unique server certificate, depending on how you use the access point.

Viewing the Certificates Installed on an Access Point

You can view the Certificate Details screen to determine which certificates are installed on the access point.

To view the certificates

- In the Navigation Menu, click **Security** > **Certificate Details**. The Certificate Details screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 05:12:46
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Security/Certificate Details/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Passwords
802.11g Radio
RADIUS Server List
Spanning Tree Security
Embedded Authentication Server
Certificate Details
Security Events
Maintenance
Access Point Configuration
Install certificates in the certificate store.

Server Certificate

Status	Installed
Common Name(CN)	24300400709-ITC
Issuer Common Name (CN)	Everett Intermediate Root Certificate(AP)
	Intermec Technologies Corporation Root Certificate
Valid From	Sep 7 19:36:14 2004 GMT
Valid To	Sep 3 19:36:14 2021 GMT

CA Certificate

Status	Installed
Common Name(CN)	Intermec Technologies Corporation Root Certificate
Issuer Common Name (CN)	Intermec Technologies Corporation Root Certificate
Valid From	Jul 3 18:58:05 2002 GMT
Valid To	Jul 3 18:58:05 2037 GMT

The Server Certificate table lists the server certificate that is installed, and the CA Certificate table lists the trusted CA certificate that is installed.

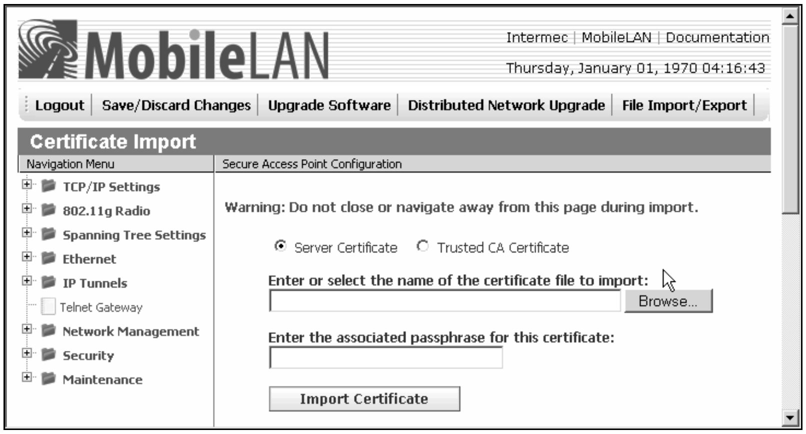
Installing and Uninstalling Certificates

Once you have determined that you need to install a certificate, use this procedure.

To install certificates

1. In the Navigation Menu, click **Security** > **Certificate Details**. The Certificate Details screen appears.
2. Click **Install certificates in the certificate store**. The Import Certificate screen appears.

Note: If you are not using the secure web browser, you will be prompted to log in again. Click **A secure session is available** and log in to the access point. If a Security Alert dialog box appears, click **Yes** to proceed. Repeat Steps 1 and 2.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 04:16:43
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export
Certificate Import
Navigation Menu
Secure Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Browse...
Import Certificate

Warning: Do not close or navigate away from this page during import.

● 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 In the Navigation Menu, click **Security** > **Certificate Details**. The Certificate Details screen appears.

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” on page 154.
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” on page 158.
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” on page 127.
    - “Using an Access Control List (ACL)” on page 132.
    - “Configuring the Access Point as an Authenticator” on page 140.

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 should 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 Embedded Authentication Server screen, enter the default secret key. For each access point, in the RADIUS Server List screen, enter the EAS IP address, enter the default secret key and check the **802.1x** check box.

If you want to use a different secret key for communications between the EAS and each access point, you need to add each access point to the EAS database as a RADIUS client. For each access point, in the RADIUS Server List, enter the EAS IP address, enter the secret key and check the **802.1x** check box.

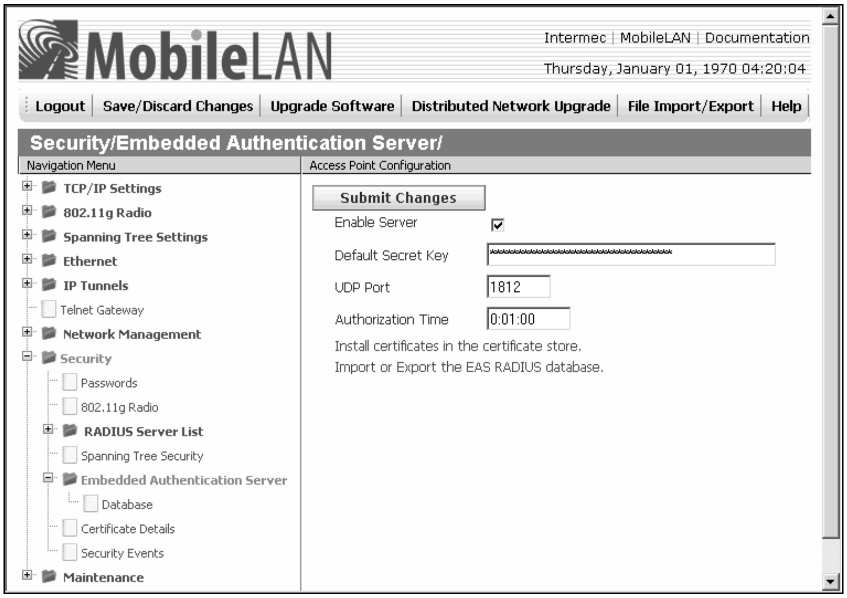
To enable the EAS

1 Log in to the access point whose EAS you are enabling.

2 In the Navigation Menu, click **Security** > **Embedded Authentication Server**. The Embedded Authentication Server screen appears.

3 Check the **Enable Server** check box.

4 Click **Submit Changes** to save your changes.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 04:20:04
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Security/Embedded Authentication Server/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Passwords
802.11g Radio
RADIUS Server List
Spanning Tree Security
Embedded Authentication Server
Database
Certificate Details
Security Events
Maintenance
Access Point Configuration
Submit Changes

Enable Server ☑

Default Secret Key ********************************

UDP Port 1812

Authorization Time 0:01:00

Install certificates in the certificate store.

Import or Export the EAS RADIUS database.

5 (Optional) In the **Default Secret Key** field, enter a default secret key that is used between the EAS and all 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.

6 In the **UDP Port** field, enter the UDP port number on which the EAS listens. Port number assignments are administered by the Internet Assigned Number Authority (IANA). If you change this value you should choose a number between 49152 and 65535.

7 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 zeros, the RADIUS server will only authenticate a RADIUS client the first time it connects.

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” on page 30.

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**.

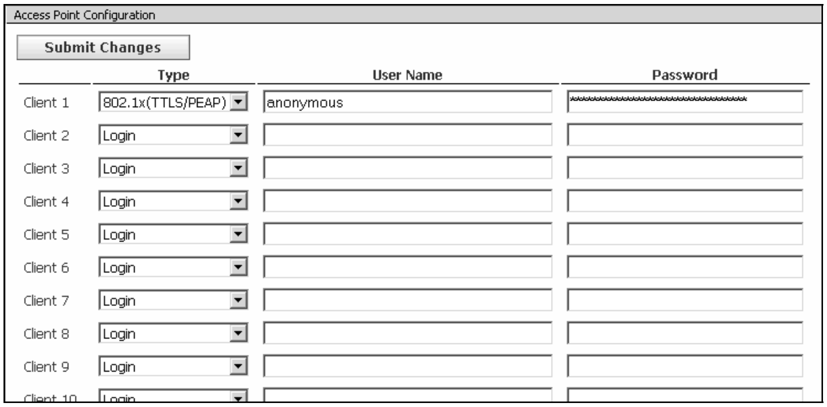
You can also create a database (using Microsoft Excel or Notepad) and then import it. Or you can configure one database, export it, and import it to an EAS in another RADIUS server. For help, see “Exporting and Importing Databases” on page 161.

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” on page 161.

To configure the database

1 Log in to the access point whose EAS you are using.

2 In the Navigation Menu, click **Security** > **Embedded Authentication Server** > **Database**. The Database screen appears.



	Type	User Name	Password
Client 1	802.1x(TTLS/PEAP)	anonymous	********************************
Client 2	Login		
Client 3	Login		
Client 4	Login		
Client 5	Login		
Client 6	Login		
Client 7	Login		
Client 8	Login		
Client 9	Login		
Client 10	Login		

3 In the **Type** field, choose the type of client you are entering in the database. For help, see the next table.

4 Click **Submit Changes** to save your changes.

5 Enter the appropriate user name and password, if applicable. User names and passwords can be from 1 to 32 characters. For help, see the next table.

6 Click **Submit Changes** to save your changes.

7 Repeat Steps 3 through 6 for each client.

8 Click **Save/Discard** changes, and then click **Save Changes without Reboot**.

Embedded Authentication Server Entry Descriptions

Type Field	Description	User Name Field	Password Field
Login	Enter user names and passwords for users who are authorized to configure and maintain access points using the password server. If you enabled the alternative method ACL, enter the MAC address in the user name and password field (no punctuation) for all end devices that are authorized to communicate with the network.	User name	User password
RADIUS	Enter an IP address/DNS name and 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. However, for more security, you should change the default secret key.	RADIUS client IP address or DNS name	Secret key
ACL	Enter the end device radio MAC address for all end devices that are authorized to communicate with the network.	MAC address	None
802.1x (TTLS/PEAP)	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 Log in to the access point whose EAS you are using.

2 In the Navigation Menu, click **Security** > **Embedded Authentication Server** > **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, PEAP/MSCHAP-V2, PEAP/GTC, 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 TTLS/PAP and PEAP/GTC 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** > **Save/Discard Changes** > **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

To clear the rejected list, you can either reboot the access point or perform these steps.

1. Click **Select All Entries**. A check box appears next to all entries.
2. Click **Clear Selected Entries**.

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:

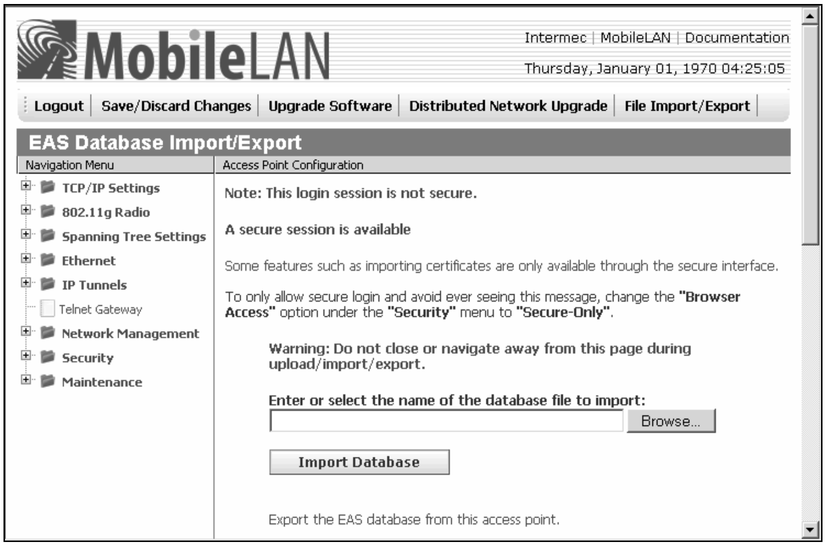
```
ACL, 11-22-33-44-55-66
TTLS, username, password
TLS, commonname
LOGIN, username, password
RADIUS, 0.0.0.0, secretkey
```

Note: PEAP entries are imported and exported as TTLS entries, since they require the same parameters.

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. Log in to the access point whose EAS you are using.
2. From the menu bar, click **File Import/Export** > **Read or write the EAS RADIUS database**. The EAS Database Import/Export screen appears.
3. If you are not using the secure web browser, click **A secure session is available**. Repeat Steps 1 and 2.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 04:25:05
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export
EAS Database Import/Export
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Browse...
Import Database

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.

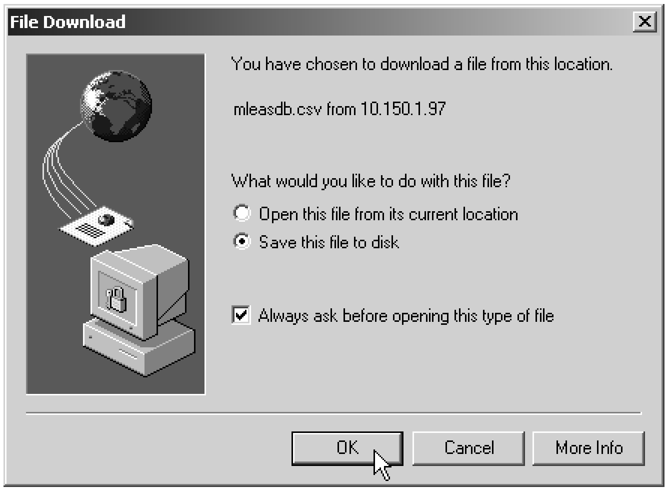
To only allow secure login and avoid ever seeing this message, change the **"Browser Access"** option under the **"Security"** menu to **"Secure-Only"**.

Warning: Do not close or navigate away from this page during upload/import/export.

Enter or select the name of the database file to import:

Export the EAS database from this access point.

4 Click **Export the EAS database from this access point**. A File Download dialog box appears.



You have chosen to download a file from this location.

mleasdb.csv from 10.150.1.97

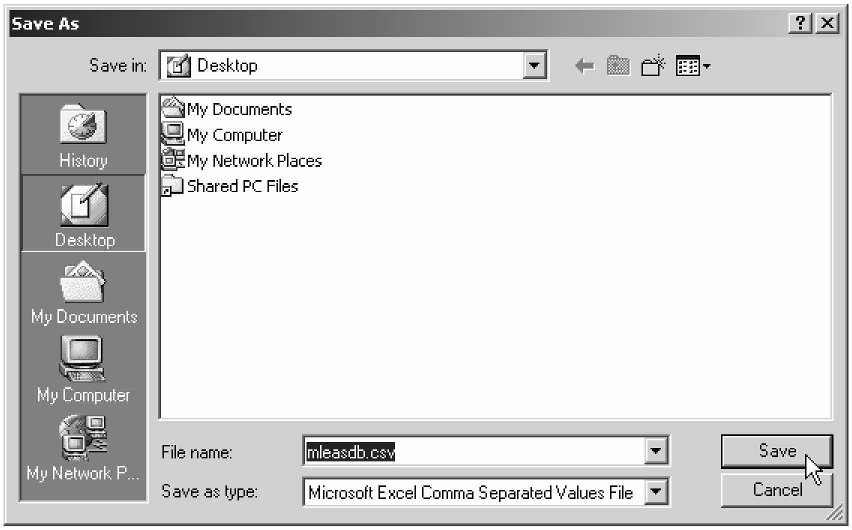
What would you like to do with this file?

○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file

5 Make sure **Save this file to disk** is selected, and then click **OK**. The Save As dialog box appears.



Save in: Desktop

File name: mleasdb.csv

Save as type: Microsoft Excel Comma Separated Values File

6 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.

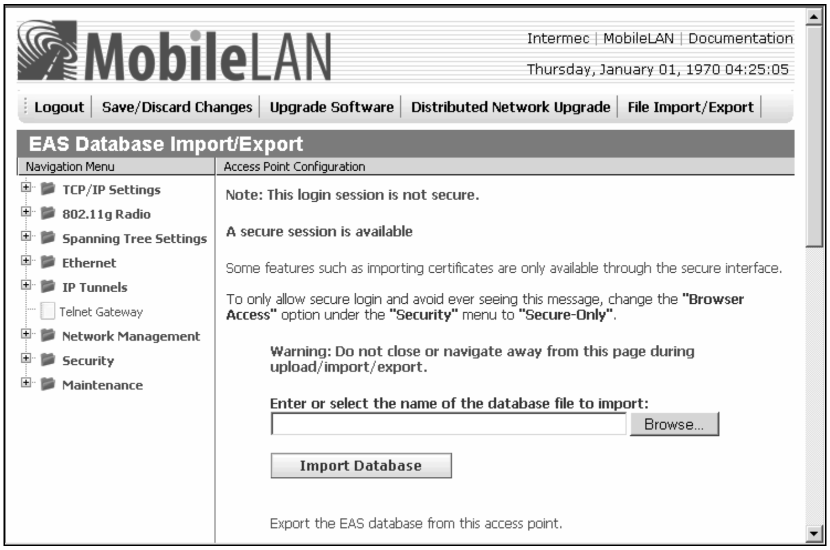
7 Click **Save**.

To import a database

Note: As soon as you import the database, it is active.

1 Log in to the access point whose EAS you are using.

2 From the menu bar, click **File Import/Export** > **Read or write the EAS RADIUS database**. The EAS Database Import/Export screen appears.



Thursday, January 01, 1970 04:25:05

EAS Database Import/Export

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"**.

Warning: Do not close or navigate away from this page during upload/import/export.

Enter or select the name of the database file to import:

Export the EAS database from this access point.

3 If you are not using the secure web browser, click **A secure session is available**. Repeat Steps 1 and 2.

4. Enter the path and filename of the database. Or click **Browse** to locate the file.
5. Click **Import Database**.

8 Managing, Troubleshooting, and Upgrading Access Points

This chapter explains how to manage, maintain, troubleshoot, and upgrade the MobileLAN access WA2XG family of access points. This chapter covers these topics:

- Managing the access points
- Maintaining the access points
- Troubleshooting the access points
- Upgrading the access points

Managing the Access Points

There are several methods that you can use to manage the access points:

Wavelink Avalanche client management system: You can install the Wavelink Avalanche system to help you manage your wireless network. To use Avalanche, you need Avalanche Manager v3.0 or later. For help, see “Using the Wavelink Avalanche Client Management System” in the next section.

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 www.intermec.com.

Web browser: For help, see “Using a Web Browser Interface” on page 25.

Communications program (such as HyperTerminal): For help, see “Using a Communications Program” on page 23.

Telnet session: Go to an MS-DOS prompt and type `telnet` *`IPaddress`*. In an IPv4 network, the IP address has the form *x.x.x.x*, where *x* is a number from 0 to 255. For help understanding IPv6 addresses, see “IP Address” in the Glossary. For more help, see “Using a Communications Program” on page 23. The interface looks similar.

SNMP management station: For help, see “Using Simple Network Management Protocol (SNMP)” on page 170.

Using the Wavelink Avalanche Client Management System

The Wavelink Avalanche client management system uses three main components to help you easily manage your wireless network.

Component	Description
Enabler	Resides on all devices managed by the Avalanche system. It communicates information about the device to the Avalanche Agent and manages software applications on the device.
Agent	Automatically detects and upgrades all devices in the Avalanche system and manages the daily processing functions.
Console	The administrative user interface that lets you configure and communicate with the Avalanche Agent. From the console, you can configure and monitor devices and build and install software packages and software collections.

The enabler is already installed on access points with software release 2.0 or later. You can install the agent and the console on the same PC. Avalanche uses a hierarchical file system organized into software packages and software collections:

- Software packages are groups of files for an application that resides on the device.
- Software collections are logical groups of software packages.

For more information about software packages and software collections, see the Wavelink Avalanche documentation and online help. Or, visit the Wavelink web site at www.wavelink.com.

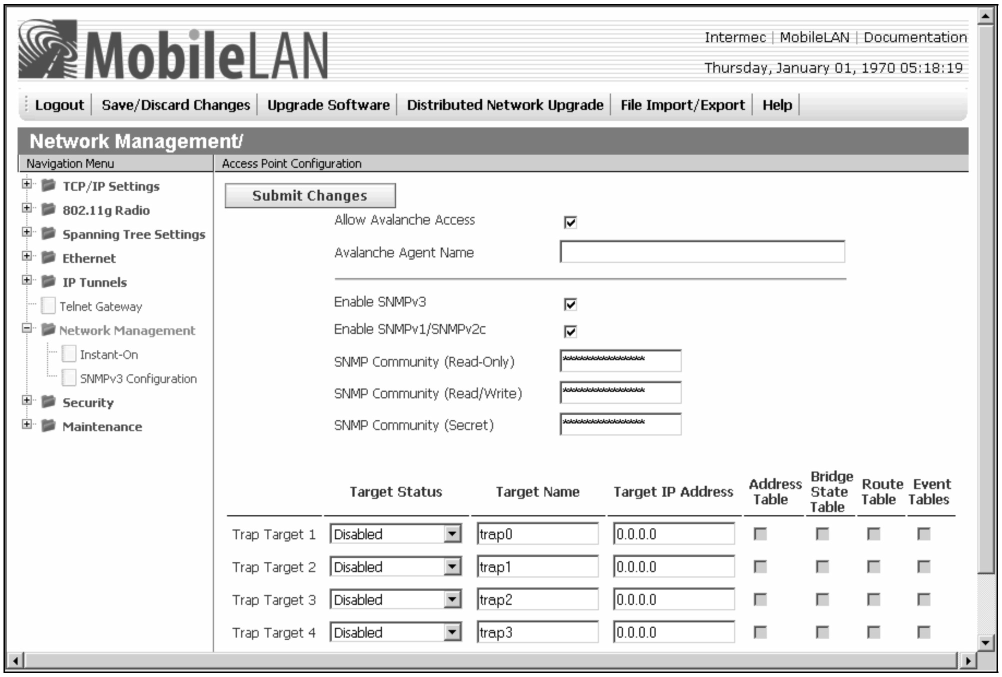
Configuring Your Access Points to Use Avalanche

The first time an access point is assigned an IP address, either manually or from a DHCP server, it attempts to connect to the Avalanche Management Console through the Avalanche Agent. Once it finds the agent, it automatically configures the console IP address.

Note: The access points that you want Avalanche to configure and manage must be on the same subnet as the agent.

To configure your access points to use Avalanche

1 In the Navigation Menu, click **Network Management**. The Network Management page appears.



Allow Avalanche Access ☑

Avalanche Agent Name

Enable SNMPv3 ☑

Enable SNMPv1/SNMPv2c ☑

SNMP Community (Read-Only) ****************

SNMP Community (Read/Write) ****************

SNMP Community (Secret) ****************

	Target Status	Target Name	Target IP Address	Address Table	Bridge State Table	Route Table	Event Tables
Trap Target 1	Disabled	trap0	0.0.0.0	□	□	□	□
Trap Target 2	Disabled	trap1	0.0.0.0	□	□	□	□
Trap Target 3	Disabled	trap2	0.0.0.0	□	□	□	□
Trap Target 4	Disabled	trap3	0.0.0.0	□	□	□	□

2 Verify that the **Allow Avalanche Access** check box is checked.

3 Click **Submit Changes**.

4 In the **Avalanche Agent Name** field, enter the IP address or DNS name of the console.

Or, leave this field blank and the access point sends out a broadcast request looking for any available agent.

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" on page 30.

6 Repeat Steps 1 through 5 for each access point.

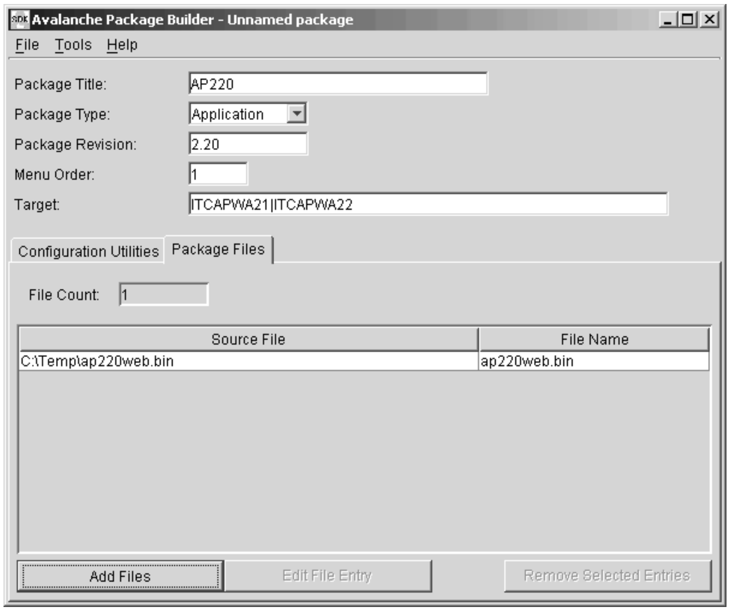
Managing Your Access Points Using Avalanche

Each time the access point is rebooted, it attempts to connect to the Avalanche Agent. When the access point connects to the agent, the agent determines whether an update is available and immediately starts the software upgrade, file transfer, or configuration update. You can also schedule these updates or you can manually initiate an update.

Note: The first time the access point locates the agent, it needs to synchronize with the Avalanche system. On the agent, you must have installed a software package that can be downloaded to the access point.

To use Avalanche to manage your access points

1 Start Avalanche Package Builder on your PC. This screen appears:



Package Title: AP220
Package Type: Application
Package Revision: 2.20
Menu Order: 1
Target: ITCAPWA21|ITCAPWA22

File Count: 1

Source File	File Name
C:\Temp\ap220web.bin	ap220web.bin

2 Create a software package (.ava file) that includes the latest software release (.bin file) using Avalanche Package Builder. For help, see the next table.

3 Install the software package using the Avalanche Management Console.

4 Schedule access point updates or manually initiate an update using the console.

For more information on using the Wavelink Avalanche client management system, see the Wavelink Avalanche documentation and online help. Or, visit the Wavelink web site at www.wavelink.com.

Avalanche Package Builder Parameter Descriptions

Parameter	Explanation
Package Title	A descriptive title of the application. For example, enter AP300.
Package Type	Choose Application.
Package Revision	The package version number. For example, enter 3.00.
Menu Order	Enter 1.

Target	Specifies which access points can receive this application. Enter a | between each ModelName.
	ModelName=ITCAPWA21
	ModelName=ITCAPWA22

Package Files	The files that are included in this package. For example, ap300web.bin.

Important Information When Using Avalanche

- If an access point is a DHCP server and Avalanche contains a network profile for the access point that assigns IP addresses from a DHCP server, the access point will lose its static IP address. Any devices that were supposed to receive an IP address from the access point will not succeed.

- If you are using the MobileLAN access Utility to recover a failed access point and you are using Avalanche to manage the access point, the recovery process may fail.

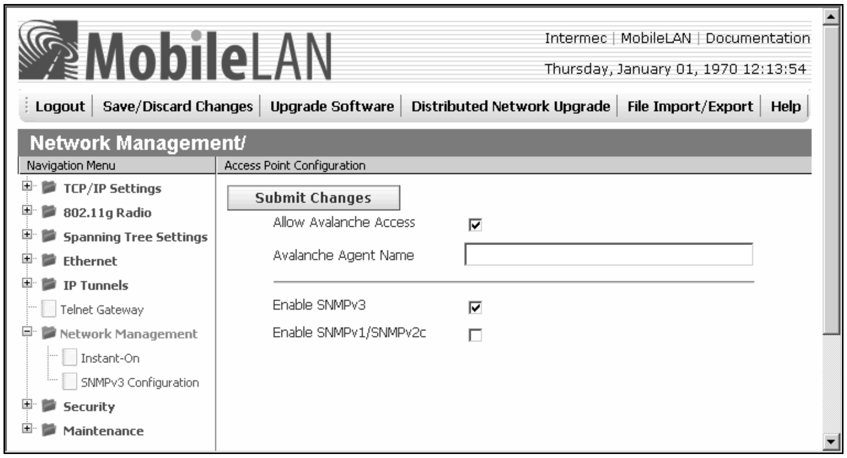
- If you change security parameters in your wireless network and you are using Avalanche, make sure that you update the security parameters on your end devices before you update the security parameters on your access point. Otherwise, you will lose connectivity between your end devices and your access point.

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. The access point supports SNMPv3 and older SNMPv1/SNMPv2c. Contact your Intermec representative if you need to obtain a copy of the MIB.

To configure the SNMPv3

1 In the Navigation Menu, click **Network Management**. The Network Management screen appears.



Allow Avalanche Access ☑

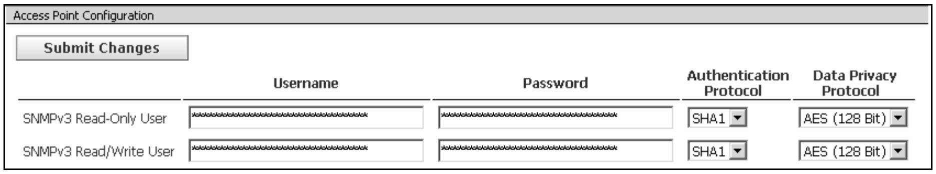
Avalanche Agent Name

Enable SNMPv3 ☑

Enable SNMPv1/SNMPv2c □

2 Check the **Enable SNMPv3** check box and then click **Submit Changes**.

3 In the Navigation Menu, click **Network Management** > **SNMPv3 Configuration**. The SNMPv3 Configuration screen appears.



	Username	Password	Authentication Protocol	Data Privacy Protocol
SNMPv3 Read-Only User	********************************	********************************	SHA1	AES (128 Bit)
SNMPv3 Read/Write User	********************************	********************************	SHA1	AES (128 Bit)

4 Configure the SNMPv3 parameters. For help, see the next table.

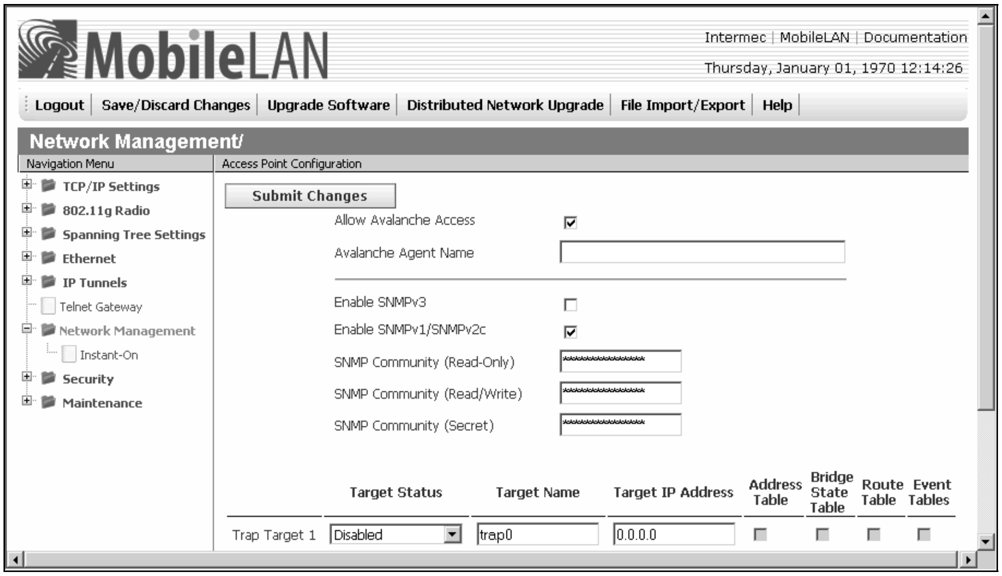
5 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see “Saving Configuration Changes” on page 30.

SNMPv3 Parameter Descriptions

Parameter	Description
Username	Specify a username that provides read-only access and another username that provides read and write access. This password can be from 1 to 15 characters and is case sensitive.
Password	Specify a password that provides read-only access and another password that provides read and write access. This password can be from 1 to 15 characters and is case sensitive.
Authentication Protocol	Specifies the authentication protocol that authenticates SNMPv3 messages. The management station must support the protocol. Intermec recommends using SHA1. Note that this option specifies the minimum level of authentication required for this username and password.
Data Privacy Protocol	Specifies the privacy protocol that is used to encrypt SNMPv3 messages. The management station must support the protocol. Intermec recommends using AES (128 Bit).

To configure SNMPv1 or SNMPv2c

1 In the Navigation Menu, click **Network Management**. The Network Management screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 12:14:26
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Network Management/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Instant-On
Security
Maintenance
Submit Changes

Allow Avalanche Access ☑
Avalanche Agent Name

Enable SNMPv3 □
Enable SNMPv1/SNMPv2c ☑
SNMP Community (Read-Only) ****************
SNMP Community (Read/Write) ****************
SNMP Community (Secret) ****************

	Target Status	Target Name	Target IP Address	Address Table	Bridge State Table	Route Table	Event Tables
Trap Target 1	Disabled	trap0	0.0.0.0	□	□	□	□

2 Check the **Enable SNMPv1/SNMPv2c** check box and then click **Submit Changes**.

3 Configure the SNMPv1/SNMPv2c parameters. For help, see the next table.

SNMPv1/SNMPv2c Parameter Descriptions

Parameter	Description
Enable SNMPv3	Determines if SNMPv3 is enabled.
Enable SNMPv1/SNMPv2c	Determines if SNMPv1 and SNMPv2c are enabled.
SNMP Read Community	Specify a password that provides read-only access. This password can be from 1 to 15 characters and is case sensitive. The default is public.
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. The default is CR52401.
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. The default is Secret.
Target Status	Choose the status of this trap target: **Disabled:** This trap target will not receive any traps. **Deleted:** This trap target is marked to be erased and it can be reused by another SNMP management station. **Enabled:** This trap target will receive standard SNMPv1 traps. **Enabled (Reliable):** Used by MobileLAN manager. These traps will be periodically sent by the access point until they are acknowledged by the management station. This trap target will receive standard SNMPv1 traps. Also, it will receive enterprise-specific traps that must be acknowledged by reading the appropriate table.
Target Name	Specifies the authoritative name of this trap target. This name can be from 1 to 15 characters.
Target IP Address	Enter the IPv4 address of this trap target.
Address Table	If the **Target Status** field is set to **Enabled (Reliable)**, you can check this check box if this trap target receives reliable traps when the address table changes.
Bridge State Table	If the **Target Status** field is set to **Enabled (Reliable)**, you can check this check box if this trap target receives reliable traps when the bridge state table changes.
Route Table	If the **Target Status** field is set to **Enabled (Reliable)**, you can check this check box if this trap target receives reliable traps when the route table changes.
Event Tables	If the **Target Status** field is set to **Enabled (Reliable)**, you can check this check box if this trap target receives reliable traps when the event table changes.

Maintaining the Access Points

The Maintenance menu lets you 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.

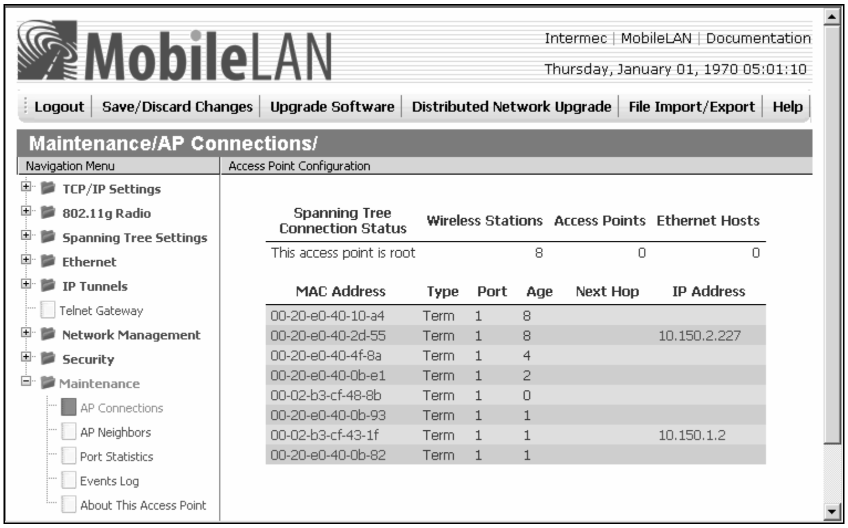
You can also view security events that are in the Security Events log, and then you can export them to a file.

Viewing AP Connections

The AP Connections screen shows information about how the access point is connected to the spanning tree and other devices that are connected through the spanning tree.

To view AP connections

- In the Navigation Menu, click **Maintenance** > **AP Connections**. The AP Connections screen appears. For help interpreting the information on this read-only screen, see the next table.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 05:01:10
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Maintenance/AP Connections/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
AP Connections
AP Neighbors
Port Statistics
Events Log
About This Access Point
Access Point Configuration

Spanning Tree Connection Status	Wireless Stations	Access Points	Ethernet Hosts
This access point is root	8	0	0

MAC Address	Type	Port	Age	Next Hop	IP Address
00-20-e0-40-10-a4	Term	1	8		
00-20-e0-40-2d-55	Term	1	8		10.150.2.227
00-20-e0-40-4f-8a	Term	1	4		
00-20-e0-40-0b-e1	Term	1	2		
00-02-b3-cf-48-8b	Term	1	0		
00-20-e0-40-0b-93	Term	1	1		
00-02-b3-cf-43-1f	Term	1	1		10.150.1.2
00-20-e0-40-0b-82	Term	1	1		

AP Connections Screen Fields

Display Field	Description
Spanning Tree Connection Status	Indicates the current status of this access point in relation to the spanning tree: **This access point is root:** This access point has formed a spanning tree and is serving as root. **Connected to root:** This access point is participating in a spanning tree as a child directly connected to the root access point. Or, this access point has found a spanning tree and is negotiating with the root access point to join the tree. **Connected to non-root:** This access point is participating in a spanning tree as a child that is not directly connected to the root. Or, this access point has found a spanning tree and is negotiating with a non-root to join the tree. **Not connected:** This access point is currently searching for a spanning tree, cannot find a spanning tree, or is unable to form its own spanning tree.
Wireless Stations	Displays the number of devices for which this access point provides connectivity via its radio ports.
Access Points	Displays the number of other access points to which this access point has a direct link in the spanning tree.
Ethernet Hosts	Displays the number of Ethernet devices for which this access point is bridging, if this access point is providing bridging for an IP tunnel or wireless LAN segment via its Ethernet network.
ACL/802.1x	Indicates which devices are passed or blocked if you are using an ACL or 802.1x security. If an access point or WAP is blocked and should be allowed to pass, you need to re-enter the IAPP secret key in both devices.
MAC Address	Shows the address of the connected device. If another access point is connected to this access point, you see the Ethernet MAC address. If a WAP is connected to this access point, you see the radio MAC address. Click the hyperlink to perform a MAC ping or display a radio link statistics screen.

AP Connections Screen Fields (continued)

Display Field	Description
Type	Indicates the nature of the connection: **Root/Parent or Parent:** Indicates an access point serving as root access point or parent, to which this access point is connected. **Pending Root:** Indicates that this access point has found a suitable spanning tree and is attempting to join the tree. **AP:** Indicates an access point linked to this root access point via the Ethernet. **AP Wireless:** Indicates an access point bridging for a wireless secondary LAN linked to this access point. **AP Tunnel:** Indicates an access point bridging for an IP tunnel linked to this root access point. **AP Remote:** Indicates an access point serving as a child on a secondary LAN. **Term:** Indicates a wireless end device connected to a radio port on this access point. **EHost:** Indicates a secondary LAN Ethernet device for which this access point provides bridging to the spanning tree.
Port	Displays the port through which the connection is established: **E**: Ethernet port **1**, **1:1**, **1:2**, or **1:3**: First radio slot (primary, secondary 1, secondary 2, or secondary 3). **2**, **2:1**, **2:2**, or **2:3**: Second radio slot (primary, secondary 1, secondary 2, or secondary 3). **I:** IP tunnel port.
Age	Displays the number of minutes since last contact with this device.
Next Hop	Displays the path to the root access point of the spanning tree via this connection.
IP Address	The IP address associated with this device, if discovered by the access point. Click the hyperlink to perform the ICMP Echo ping.

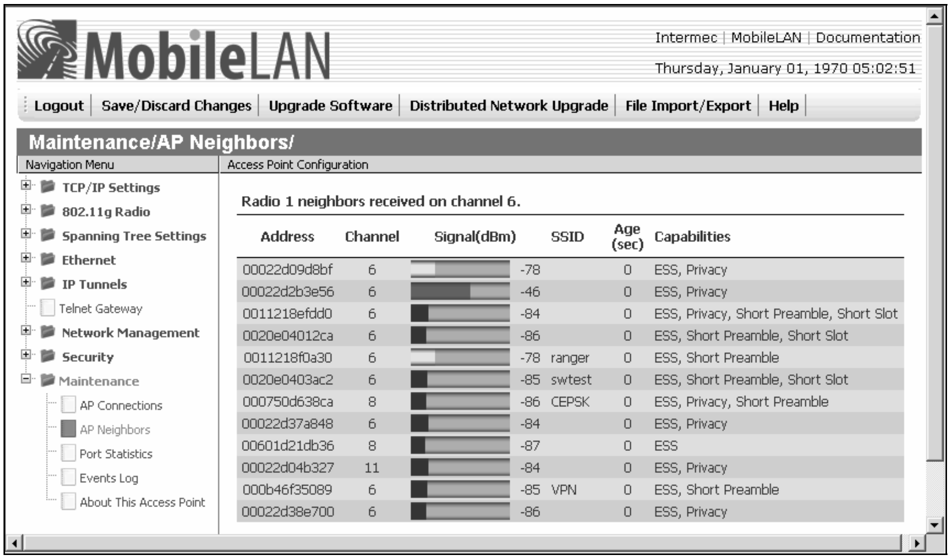
Viewing AP Neighbors

The AP Neighbors screen provides information on all the access points (even hidden access points) in the area. It displays information gathered by the radios receiving beacons from other sources as it operates on a specific channel. You can use this screen to help you:

- distribute channels for maximum wireless network performance.
- identify interference problems.

To view AP neighbors

- In the Navigation Menu, click **Maintenance** > **AP Neighbors**. The AP Neighbors screen appears. For help interpreting the information on this read-only screen, see the next table.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 05:02:51
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Maintenance/AP Neighbors/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
AP Connections
AP Neighbors
Port Statistics
Events Log
About This Access Point

Radio 1 neighbors received on channel 6.

Address	Channel	Signal(dBm)	SSID	Age (sec)	Capabilities
00022d09d8bf	6	-78		0	ESS, Privacy
00022d2b3e56	6	-46		0	ESS, Privacy
0011218efdd0	6	-84		0	ESS, Privacy, Short Preamble, Short Slot
0020e04012ca	6	-86		0	ESS, Short Preamble, Short Slot
0011218f0a30	6	-78	ranger	0	ESS, Short Preamble
0020e0403ac2	6	-85	swtest	0	ESS, Short Preamble, Short Slot
000750d638ca	8	-86	CEPSK	0	ESS, Privacy, Short Preamble
00022d37a848	6	-84		0	ESS, Privacy
00601d21db36	8	-87		0	ESS
00022d04b327	11	-84		0	ESS, Privacy
000b46f35089	6	-85	VPN	0	ESS, Short Preamble
00022d38e700	6	-86		0	ESS, Privacy

AP Neighbors Screen Fields

Display Field	Description
Address	Displays the MAC address of the originator of the contact.
Channel	Displays the channel advertised in the beacon.
Signal (dBm)	Displays the power level of reception measured in dBm. Graph colors red, yellow, green indicate poor, adequate, good signal levels for communication, respectively.
SSID	Displays the SSID advertised in the beacon. This field may or may not be advertised by the originator of the contact.
Age (sec)	Displays the amount of time in seconds that has elapsed since the last contact from the originator.

AP Neighbors Screen Fields (continued)

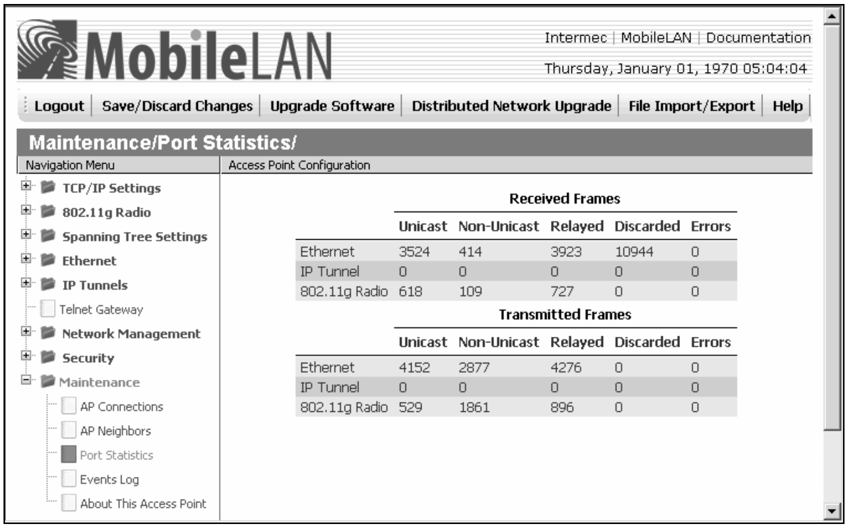
Display Field	Description
Capabilities	This information is derived from the capability information sent in the beacon. Capabilities may include: **ESS:** Set for an access point and cleared for an end device or ad-hoc device. **IBSS:** Cleared for an access point and set for an end device or ad-hoc device. **Privacy:** Indicates that encryption is required on this service set. **Short Preamble:** Indicates that short preambles may be used for frame transmission on this service set. **OFDM Allowed:** Use of DSSS-OFDM is allowed within this BSS. **Short Slot:** Indicates that short slot timing is being used on this service set. If this field is not present, then longer slot timing is being used for backward compatibility. **CFPoll:** Access point uses point coordination function for delivery and polling. **CFReq:** Access point uses point coordination function for delivery but does not support polling.

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. You can also view graphs of inbound and outbound packets for the port.

To view port statistics

- In the Navigation Menu, click **Maintenance** > **Port Statistics**. The Port Statistics screen appears. This screen is read-only.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 05:04:04
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Maintenance/Port Statistics/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
AP Connections
AP Neighbors
Port Statistics
Events Log
About This Access Point

Received Frames

	Unicast	Non-Unicast	Relayed	Discarded	Errors
Ethernet	3524	414	3923	10944	0
IP Tunnel	0	0	0	0	0
802.11g Radio	618	109	727	0	0

Transmitted Frames

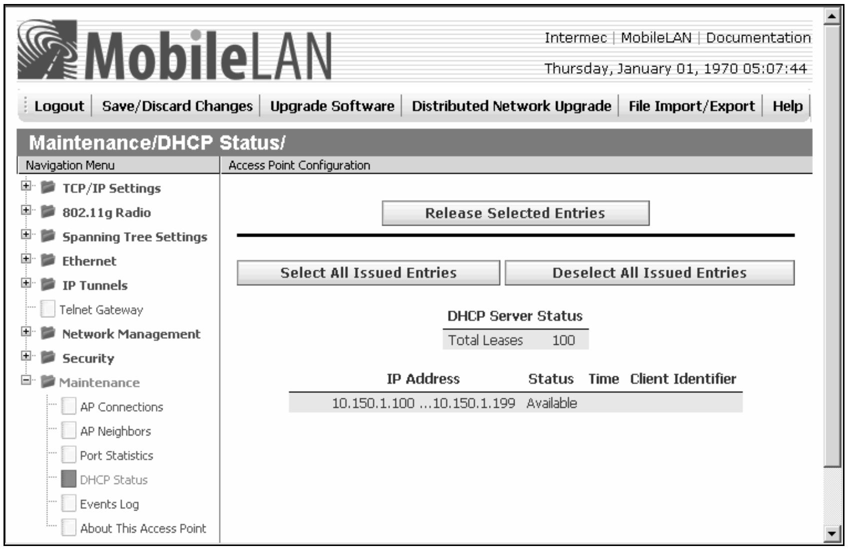
	Unicast	Non-Unicast	Relayed	Discarded	Errors
Ethernet	4152	2877	4276	0	0
IP Tunnel	0	0	0	0	0
802.11g Radio	529	1861	896	0	0

Viewing DHCP Status

The DHCP Status screen shows a status report for the DHCP client or DHCP server. If the access point is a DHCP server and if the **Permanently Save IP Address Mappings** check box is checked, you can delete entries from the server's permanent address map.

To view DHCP status

- In the Navigation Menu, click **Maintenance** > **DHCP Status**. The DHCP Status screen appears.



DHCP Server Status

Total Leases	100

IP Address	Status	Time	Client Identifier
10.150.1.100 ...10.150.1.199	Available		

Viewing the Events Log

The Events Log screen shows a the events that have been logged by this access point. These events are cleared when the access point loses power or is rebooted.

To view the Events Log

- In the Navigation Menu, click **Maintenance** > **Events Log**. For help understanding the events on this read-only screen, see the next table.

Events Log Description

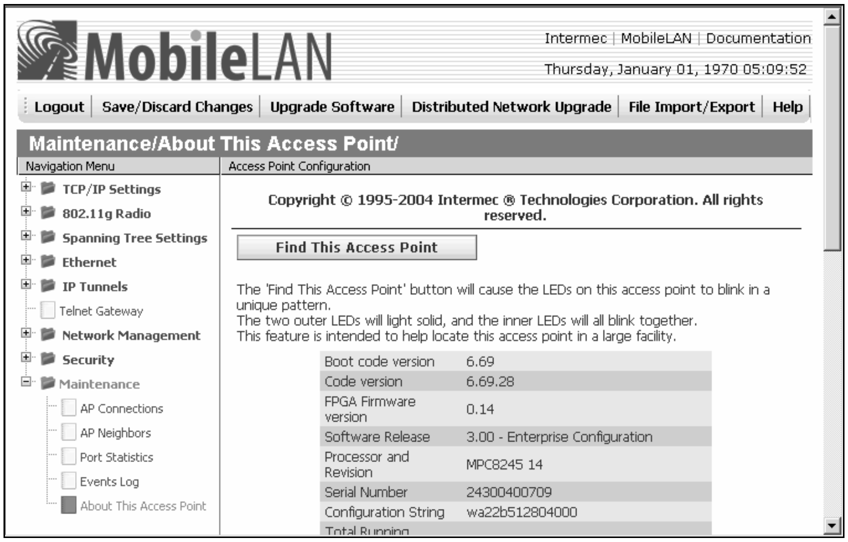
Column	Description
MAC Address	Indicates the Ethernet MAC address of the device that caused the event.
IP Address	Indicates the IP address of the device that caused the event.
Priority	Indicates the priority of the event: Critical, High, Low, and Informative. Critical and High priority events generate an SNMP trap.
Trap?	Indicates whether an SNMP trap is sent for this particular event type.
Count	Indicates the number of times the event occurred.
Type	Indicates a description of the event.
Additional Data	Indicates extra event-specific information.
Age	Indicates the amount of time that has passed since the event occurred.

Viewing the About This Access Point Screen

This screen shows information about the access point, such as the software version, radio versions, and MAC addresses. It also provides a configuration summary section, which can either show you the configuration settings that are different from the factory default settings or it can show you all the configuration settings.

To view About This Access Point

1 In the Navigation Menu, click **Maintenance** > **About This Access Point**. The About This Access Point screen appears. This screen is read-only.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 05:09:52
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Maintenance/About This Access Point/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
AP Connections
AP Neighbors
Port Statistics
Events Log
About This Access Point
Find This Access Point

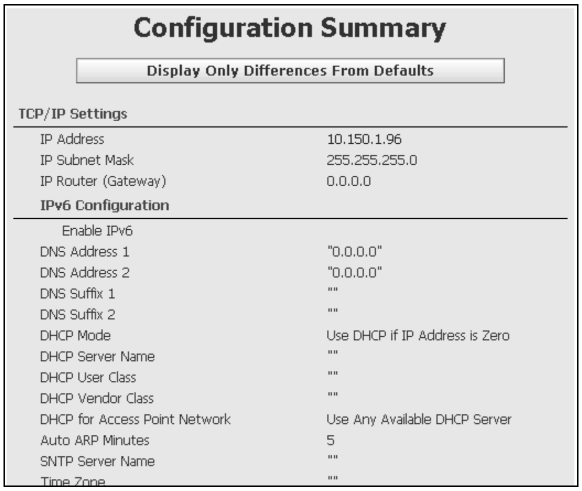
Copyright © 1995-2004 Intermec ® Technologies Corporation. All rights reserved.

The 'Find This Access Point' button will cause the LEDs on this access point to blink in a unique pattern.
The two outer LEDs will light solid, and the inner LEDs will all blink together.
This feature is intended to help locate this access point in a large facility.

Boot code version	6.69
Code version	6.69.28
FPGA Firmware version	0.14
Software Release	3.00 - Enterprise Configuration
Processor and Revision	MPC8245 14
Serial Number	24300400709
Configuration String	wa22b512804000
Total Running	

2 Scroll down to view more information about the access point.

3 Continue scrolling down until you see the subtitle **Configuration Summary**.



Configuration Summary

TCP/IP Settings

IP Address	10.150.1.96
IP Subnet Mask	255.255.255.0
IP Router (Gateway)	0.0.0.0

IPv6 Configuration

Enable IPv6	
DNS Address 1	"0.0.0.0"
DNS Address 2	"0.0.0.0"
DNS Suffix 1	""
DNS Suffix 2	""
DHCP Mode	Use DHCP if IP Address is Zero
DHCP Server Name	""
DHCP User Class	""
DHCP Vendor Class	""
DHCP for Access Point Network	Use Any Available DHCP Server
Auto ARP Minutes	5
SNTP Server Name	""
Time Zone	""

4 Click the button under the Configuration Summary title to switch between displaying all configuration settings and displaying the configuration settings that are different from the factory default settings.

Using the LEDs to Locate Access Points

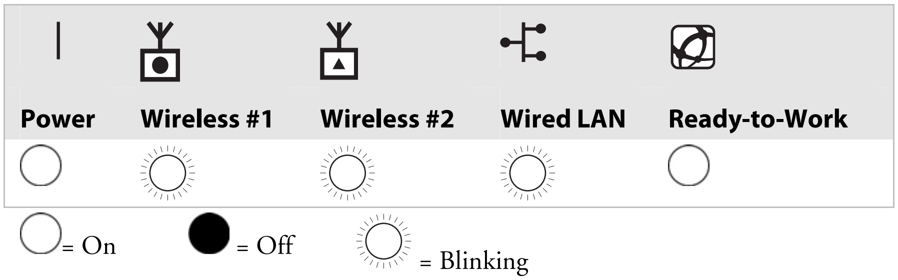
You can use the LEDs to help you locate a specific access point in your building.

To locate an access point

1 In the Navigation Menu, click **Maintenance** > **About this Access Point**. The About this Access Point screen appears.

2 Click the **Find This Access Point** button. The access point LEDs start blinking, as shown in the next table.

Find This Access Point



3 The LEDs continue to blink until you click the **Finished Finding Access Point** button.

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 Appendix B, “Default Settings.” To restore the access point to the default configuration, you can use:

- MobileLAN access Utility v2.0 (or later). For help, see “Using the MobileLAN access Utility” in the next section.
- Web browser interface. For help, see “Using the Web Browser Interface” on page 182.

Using the MobileLAN access Utility

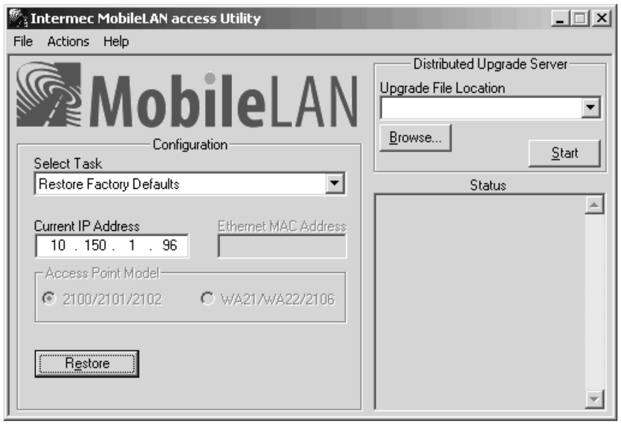
Note: If you are using IPv6 addressing, you must use a web browser interface. For help, see “Using the Web Browser Interface” on page 182.

For help installing the MobileLAN access utility, see “Using the MobileLAN access Utility” on page 21.

To restore the access point to the default configuration

1 Start the utility.

2 In the **Select Task** field, choose **Restore Factory Defaults**.



Select Task: Restore Factory Defaults

Current IP Address: 10 . 150 . 1 . 96

Access Point Model: ● 2100/2101/2102 ○ WA21/WA22/2106

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.

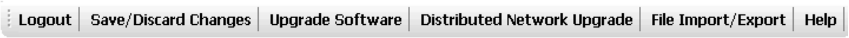
5 Immediately click **Restore**. The **Status** box lets you know when the default configuration has been restored. You will need to reconfigure your network settings.

6 To close the utility, from the **File** menu choose **Exit**.

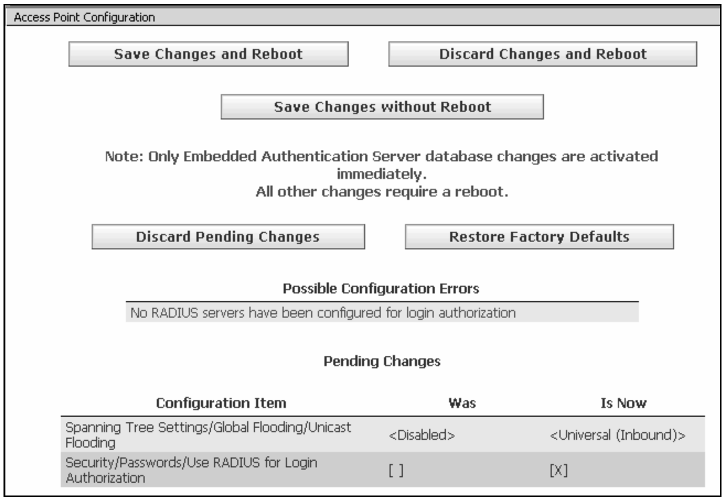
For more help using the utility, from the **Help** menu choose **Contents**.

Using the Web Browser Interface

1 In the menu bar, click **Save/Discard Changes**.



This screen appears.


Access Point Configuration
Save Changes and Reboot
Discard Changes and Reboot
Save Changes without Reboot
Discard Pending Changes
Restore Factory Defaults

Note: Only Embedded Authentication Server database changes are activated immediately.
All other changes require a reboot.

Possible Configuration Errors

No RADIUS servers have been configured for login authorization

Pending Changes

Configuration Item	Was	Is Now
Spanning Tree Settings/Global Flooding/Unicast Flooding	<Disabled>	<Universal (Inbound)>
Security/Passwords/Use RADIUS for Login Authorization	[ ]	[X]

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 Points

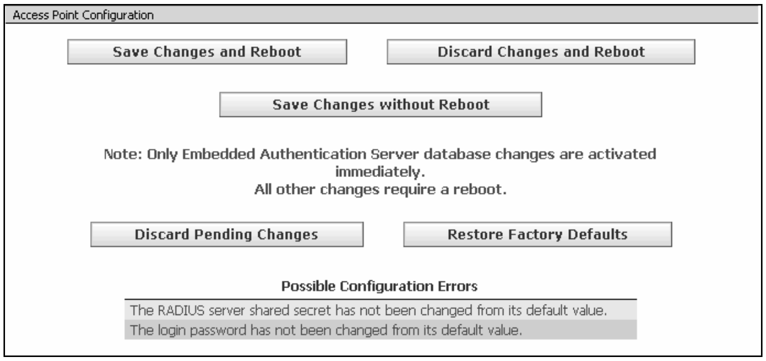
This section provides you with information on the installation, configuration, and operation of the access point.

Using the Configuration Error Messages

When you click **Save/Discard Changes**, the access point checks for potential problems with the network configuration and security settings. The access point displays error messages under the Possible Configuration Errors heading. Each error message is a hyperlink, which you can click to go to the screen where you can fix the possible configuration error.

You can save the configuration changes without resolving any of the possible configuration errors, but the access point may not operate as expected.

Note: The access point can only check its own configuration for possible errors. It cannot check to see if the SSIDs, passwords, shared secret keys, and other settings are all the same or compatible on other devices.



Access Point Configuration

Note: Only Embedded Authentication Server database changes are activated immediately.
All other changes require a reboot.

Possible Configuration Errors

The RADIUS server shared secret has not been changed from its default value.
The login password has not been changed from its default value.

Screen Showing Possible Configuration Errors

To resolve possible configuration errors

1 Using your web browser, click **Save/Discard Changes** on the menu bar.

2 Review the error messages listed under the Possible Configuration Errors heading.

3 Click each error message to jump to the configuration screen where you can resolve the possible configuration error.

The configuration error messages are listed in the next table. Most are self explanatory, but a few require additional information.

Alphabetized List of Configuration Error Messages

Configuration Error Message	Additional Information
A RADIUS entry in the RADIUS database has a IP address but no secret key (password).	
A RADIUS entry in the RADIUS database has a secret key (password) but no IP address.	
A RADIUS server entry points at this access point but the Embedded Authentication Server is not enabled.	
A RADIUS server entry points at this access point but the shared secret does not match that of the Embedded Authentication Server.	The Default Secret Key for the EAS does not match the secret key value in the RADIUS Server List. For help, see “Enabling the EAS” on page 156.
A RADIUS server entry points at this access point but the UDP port number does not match that of the Embedded Authentication Server.	The UDP port number in the EAS does not match the port number entered in the RADIUS Server List. For help, see “Enabling the EAS” on page 156.

Alphabetized List of Configuration Error Messages (continued)

Configuration Error Message	Additional Information
A secure service set is available, but wireless hops are allowed on an insecure service set.	
A username/password entry in the RADIUS database has a password but no username.	
A username/password entry in the RADIUS database has a username but no password.	
All SSID values must be unique per physical radio.	While configuring multiple service sets, you did not specify a unique SSID (network name) for each service set. For help, see “Configuring the 802.11g Radio” on page 76.
An entry in the RADIUS server list is using a default secret key.	Intermec recommends that you change the secret key from the default for security reasons.
At least one 802.1x supplicant protocol must be enabled.	
Matching WEP keys will merge VLAN multicast.	
No RADIUS servers have been configured for 802.1x authentication.	Click the message and check the **802.1x** check box for at least one server in the RADIUS Server List.
No RADIUS servers have been configured for ACL authorization.	Click the message and check the **ACL** check box for at least one server in the RADIUS Server List.
No RADIUS servers have been configured for login authorization.	Click the message and check the **Login** check box for at least one server in the RADIUS Server List.
The 802.1x username and password have not been changed from their default values.	
The access point is set to originate IP tunnels but no there are no tunnel IP addresses.	On the IP Tunnels screen, **Mode** is set to **Originate if Root**, but no IP addresses have been added to the IP Addresses screen. Either change the mode or add some addresses. For help, see “Configuring IP Tunnels” on page 102 and “Configuring the IP Address List” on page 103.
The address range for the DHCP server is invalid.	On the TCP/IP Settings > DHCP Server Setup screen, the **Low Address** and **High Address** are not set correctly. For help, see the DHCP Server Setup Parameter Descriptions table on page 56.

Alphabetized List of Configuration Error Messages (continued)

Configuration Error Message	Additional Information
The DHCP server is enabled with an address range that is too large. If saved, the range will be truncated to the maximum number of addresses.	On the TCP/IP Settings > DHCP Server Setup screen, the **Low Address** and **High Address** are not set correctly. For help, see the DHCP Server Setup Parameter Descriptions table on page 56.
The DHCP server requires a non-zero IP address.	For help, see “Configuring the Access Point as a DHCP Server” on page 53.
The DHCP server subnet mask is invalid.	For help, see the DHCP Server Setup Parameter Descriptions table on page 56.
The IAPP secret key has not been changed from its default value.	Intermec recommends that you change the IAPP secret key from the default for security reasons.
The IP Address is zero.	For help, see “Configuring the TCP/IP Settings” on page 48.
The IP Address and IP Router must share the same subnet.	For help, see “Configuring the TCP/IP Settings” on page 48.
The IP Subnet Mask is invalid.	For help, see “Configuring the TCP/IP Settings” on page 48.
The IP Subnet Mask should not be zero.	For help, see “Configuring the TCP/IP Settings” on page 48.
The login password has not been changed from its default value.	
The RADIUS server shared secret has not been changed from its default value.	
The read-only password has the same value as the read-write password.	
There are TLS entries in the embedded authentication server database but no CA certificate is installed.	You need to install a trusted CA certificate. For help, see “Installing and Uninstalling Certificates” on page 154.
This device is configured as a login RADIUS server but no login database entries exist.	For help, see the Embedded Authentication Server Entry Descriptions table on page 159.
You have chosen to reject expired certificates but you have not enabled SNTP to keep your system clock up-to-date.	For help, see “Setting the Clock” on page 28.
You have elected to verify the server certificate but no CA certificate is installed in the certificate store.	You need to install a trusted CA certificate. For help, see “Installing and Uninstalling Certificates” on page 154.
You have elected to verify the server certificate but the authentication server common name is blank.	

Alphabetized List of Configuration Error Messages (continued)

Configuration Error Message	Additional Information
You have enabled Secure Credential Creation for Instant-On, but no 802.1x-enabled RADIUS servers have been selected.	
You have enabled the embedded authentication server but you have not installed a server certificate to identify this device.	You need to install a server certificate. For help, see “Installing and Uninstalling Certificates” on page 154.
You have enabled TLS authentication but you have not installed a server certificate to identify this device.	You need to install a server certificate. For help, see “Installing and Uninstalling Certificates” on page 154.
You have enabled WPA pre-shared key for a radio port but the pre-shared key for that port is empty.	For help, see the WPA - PSK Security Parameter Descriptions table on page 148.

Calling Intermec Technical Support

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” on page 180.

You should have the information on the About this Access Point screen available when you call Intermec Technical Support. To contact Intermec Technical Support, see Global Services and Support on page vii.

Troubleshooting With the LEDs

When the access point boots, it performs internal diagnostics and the LEDs display the pattern shown in the next table.

WA2XG LED Boot Sequence

Power	Wireless #1	Wireless #2	Wired LAN	Ready-to-Work	Description
●	●	○	●	●	Checksum Test starts
●	○	○	●	●	Checksum Test fails
○	●	●	●	●	Monitor Load
○	○	○	●	●	PCI Bus Test starts
○	○	●	●	●	PCI Bus Test fails
●	●	●	○	●	RAM Test starts
○	●	○	●	●	RAM Test fails
○	☼ (Wireless #1 and #2 blink in unison.)	☼	☼	●	Only Boot ROM code is available on access point. Load new files.

○ = On ● = Off ☼ = Blinking

WA2XG Normal LED Pattern After Booting

○	☼ (Blinks for wireless data traffic.)	☼ (Blinks if a radio is installed.)	☼ (Blinks for wired data traffic.)	○

General Troubleshooting

Problem/Question	Possible Solution/Answer
The Wireless #1, Wireless #2, and/or Wired LAN LEDs are on solid at the end of the boot process.	An error occurred during the booting process. Consult the previous section to determine which test failed. Connect the access point to a PC with an RS-232 cable, reboot the access point, and watch the error messages. The access point may have a hardware problem. Call Intermec Technical Support.
The Power LED is not on.	1. Make sure the power cable is firmly plugged into the WA21G and the power source. Or make sure the Ethernet cable is firmly plugged into the WA22G and the power over Ethernet bridge. 2. Verify that the power injector has power and will work with another access point at the port in question. 3. Make sure all eight wires in the Ethernet cable are connected, or the power over Ethernet option won't work. 4. 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. 5. The access point may have a hardware problem. Call Intermec Technical Support.
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 sign on screen appears.
You cannot connect to the access point using a web browser.	1. Verify that you are not using a crossover cable if connected to a hub or a switch. Verify that you are using a crossover cable if connected directly to the PC or server. 2. Verify that you did not disable the Browser Access field in the Security screen. 3. 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. 4. Depending on the security configuration of your network, your PC may need to be located on the same subnet as the access point.

General Troubleshooting (continued)

Problem/Question	Possible Solution/Answer
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” on page 197.
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.	• In 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.	Verify that the end device and the access point have the same SSID (network name) and security.
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 help, see “About Ethernet Bridging/Data Link Tunneling” on page 89.
The end devices are unable to roam between a MobileLAN access product and 011X devices.	Set the **Unicast Flood Mode** to Hierarchical. For help, see “Configuring Global Flooding” on page 113.
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.

General Troubleshooting (continued)

Problem/Question	Possible Solution/Answer
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** > **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 help, see “Configuring IP Tunnel Filters” on page 104.
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.

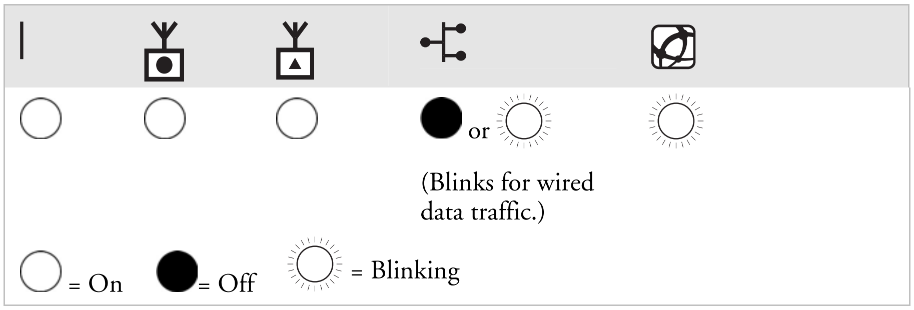
Troubleshooting the Radios

If you are having problems communicating with your wireless network, you can use the access point LEDs, error messages, Radio MAC Ping, or ICMP Echo to 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.

WA2XG LEDs



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. Contact your local Intermec representative to help you correct the problem.

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.

Radio Error Messages

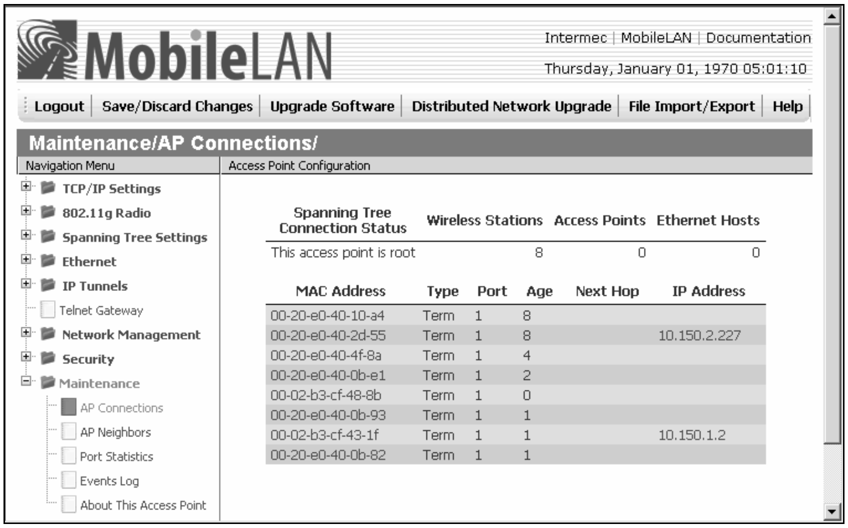
Error Message	Explanation
Couldn’t read country code from radio A	The radio may be faulty.
Invalid country code in string for radio A	The country code in the configuration matrix string does not match the country code in the radio in the access point.
Radio A has unknown country code	The radio may have 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

Radio MAC Ping runs at the MAC sublayer of the Data Link layer, thus allowing you to ping any 802.11g device that is connected to the access point. Radio MAC Ping can help you determine the connectivity and signal strength of an 802.11g radio.

To use radio MAC ping

1 In the Navigation Menu, click **Maintenance** > **AP Connections**. The AP Connections screen appears. All devices that support a radio MAC ping will have their MAC address listed with a hyperlink.

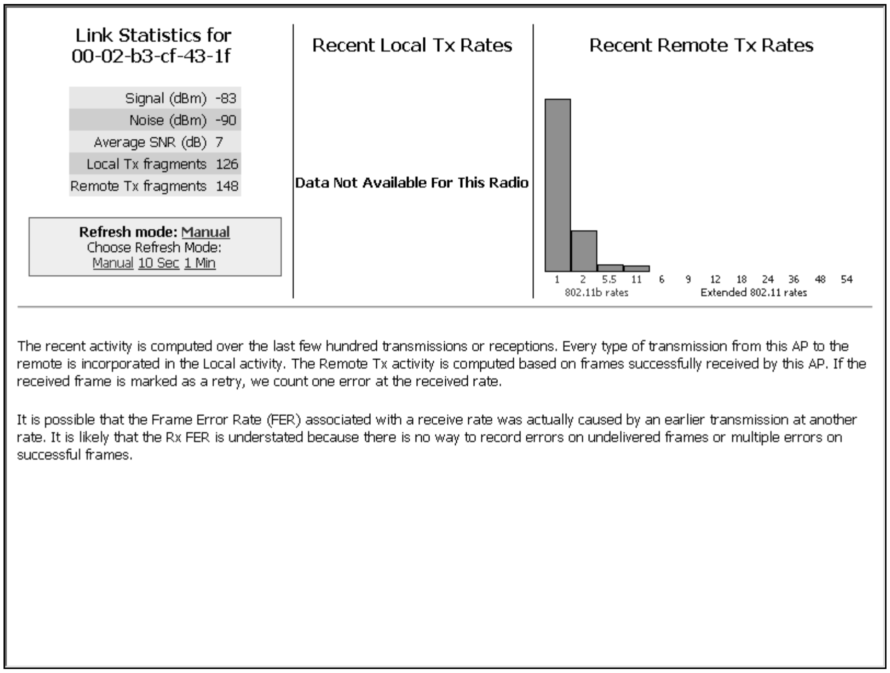


Maintenance/AP Connections/

Spanning Tree Connection Status	Wireless Stations	Access Points	Ethernet Hosts
This access point is root	8	0	0

MAC Address	Type	Port	Age	Next Hop	IP Address
00-20-e0-40-10-a4	Term	1	8		
00-20-e0-40-2d-55	Term	1	8		10.150.2.227
00-20-e0-40-4f-8a	Term	1	4		
00-20-e0-40-0b-e1	Term	1	2		
00-02-b3-cf-48-8b	Term	1	0		
00-20-e0-40-0b-93	Term	1	1		
00-02-b3-cf-43-1f	Term	1	1		10.150.1.2
00-20-e0-40-0b-82	Term	1	1		

2 Click a MAC address hyperlink. The access point pings the device, and then this screen appears showing the results.



Link Statistics for
00-02-b3-cf-43-1f

Signal (dBm)	-83
Noise (dBm)	-90
Average SNR (dB)	7
Local Tx fragments	126
Remote Tx fragments	148

Refresh mode: Manual
Choose Refresh Mode:
Manual 10 Sec 1 Min

The recent activity is computed over the last few hundred transmissions or receptions. Every type of transmission from this AP to the remote is incorporated in the Local activity. The Remote Tx activity is computed based on frames successfully received by this AP. If the received frame is marked as a retry, we count one error at the received rate.

It is possible that the Frame Error Rate (FER) associated with a receive rate was actually caused by an earlier transmission at another rate. It is likely that the Rx FER is understated because there is no way to record errors on undelivered frames or multiple errors on successful frames.

By default, the **Refresh Mode** is **Manual**. To configure the software to refresh automatically at a set interval, click **10 Sec** or **1 Min**.

By default, the **Pings per refresh** is **None**. To increase the number of pings that occur after each refresh, click **25** or **100**.

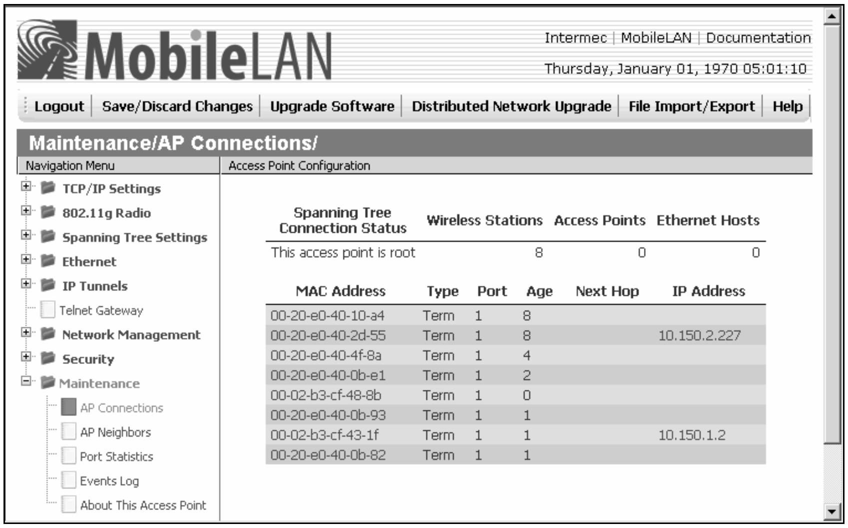
3 Click the **X** in the upper right corner of the window to return to the AP Connections screen.

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

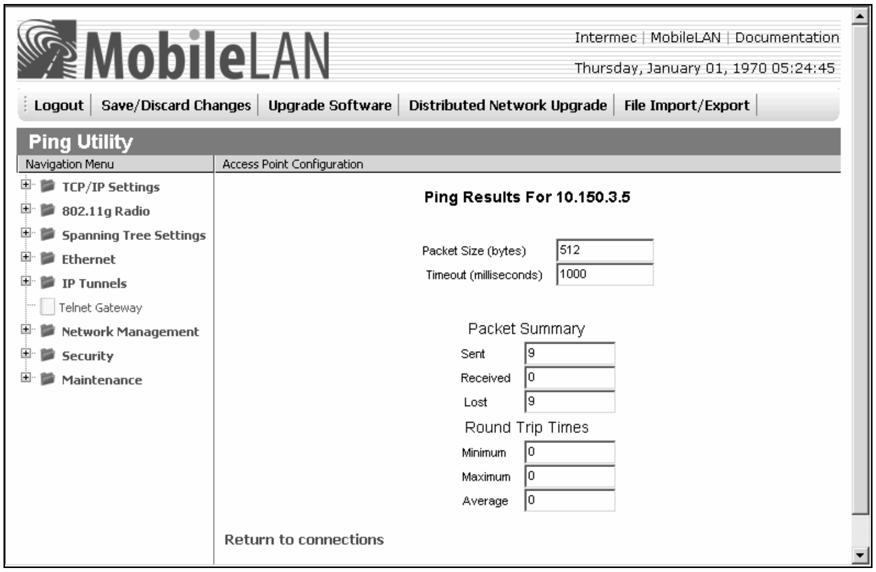
1 In the Navigation Menu, click **Maintenance** > **AP Connections**. The AP Connections screen appears.



Spanning Tree Connection Status	Wireless Stations	Access Points	Ethernet Hosts
This access point is root	8	0	0

MAC Address	Type	Port	Age	Next Hop	IP Address
00-20-e0-40-10-a4	Term	1	8		
00-20-e0-40-2d-55	Term	1	8		10.150.2.227
00-20-e0-40-4f-8a	Term	1	4		
00-20-e0-40-0b-e1	Term	1	2		
00-02-b3-cf-48-8b	Term	1	0		
00-20-e0-40-0b-93	Term	1	1		
00-02-b3-cf-43-1f	Term	1	1		10.150.1.2
00-20-e0-40-0b-82	Term	1	1		

2 Click an IP address hyperlink. The access point pings the device, and then the Ping Utility screen appears showing the results.



Ping Results For 10.150.3.5

Packet Size (bytes) 512
Timeout (milliseconds) 1000

Packet Summary
Sent 9
Received 0
Lost 9

Round Trip Times
Minimum 0
Maximum 0
Average 0

Note: The information on this screen varies with the type of request sent and the capabilities of the medium through which it is sent. Echo requests sent through different radios may report different results.

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.

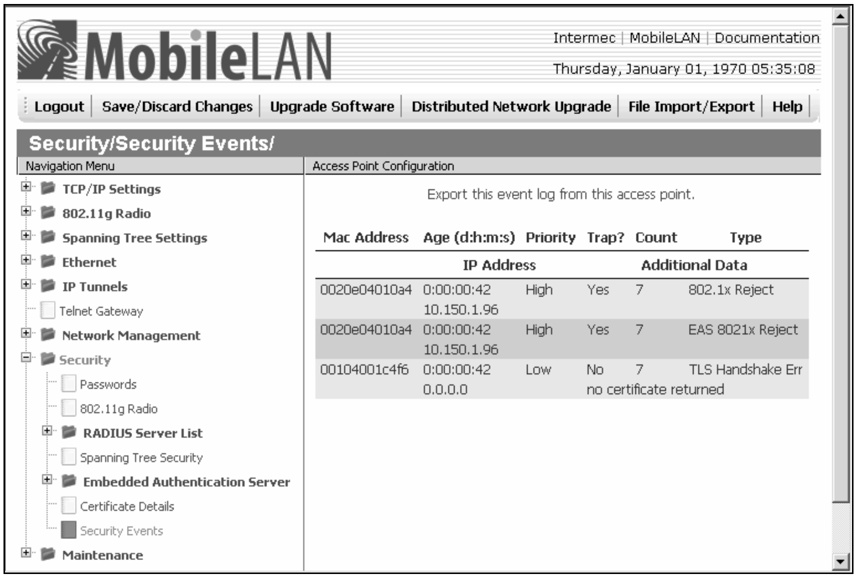
Viewing the Security Events Log

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

- In the Navigation Menu, click **Security** > **Security Events**. The Security Events log appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 05:35:08
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Security/Security Events/
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Passwords
802.11g Radio
RADIUS Server List
Spanning Tree Security
Embedded Authentication Server
Certificate Details
Security Events
Maintenance
Access Point Configuration

Export this event log from this access point.

Mac Address	Age (d:h:m:s)	Priority	Trap?	Count	Type
	IP Address		Additional Data		
0020e04010a4	0:00:00:42	High	Yes	7	802.1x Reject
	10.150.1.96				
0020e04010a4	0:00:00:42	High	Yes	7	EAS 8021x Reject
	10.150.1.96				
00104001c4f6	0:00:00:42	Low	No	7	TLS Handshake Err
	0.0.0.0		no certificate returned		

For help understanding the events, see the next table.

Security Events Log Description

Column	Description
MAC Address	Indicates the Ethernet MAC address of the device that caused the event.
IP Address	Indicates the IP address of the device that caused the event.
Priority	Indicates the priority of the event: Critical, High, Low, or Informative Critical and High priority events generate an SNMP trap.
Trap?	Specifies if the event generated an SNMP-reliable trap.
Count	Indicates the number of times the event occurred.
Type	Includes details of the event that occurred.
Additional Data	Includes extra event-specific information.
Age	Indicates the 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.

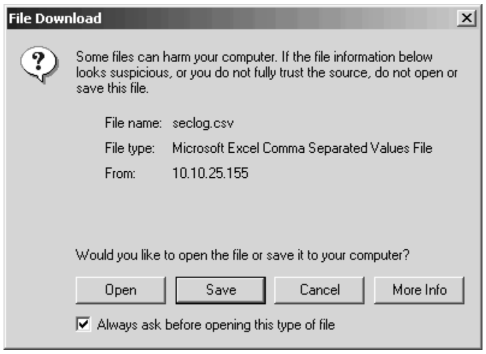
Exporting the Security Events Log

You can export the Security Events log from the web browser interface to a comma-separated file. You can open this file using Microsoft Excel or Notepad.

To export the security events log

1 In the Navigation Menu, click **Security** > **Security Events**. The Security Events log appears.

2 Click **Export this event log from this access point**. A File Download box may appear.



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: seclog.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

3 Click **Save**. The Save As dialog box appears.

4 Choose where you want to save the SECLOG.CSV file and click **Save**.

General Security Troubleshooting

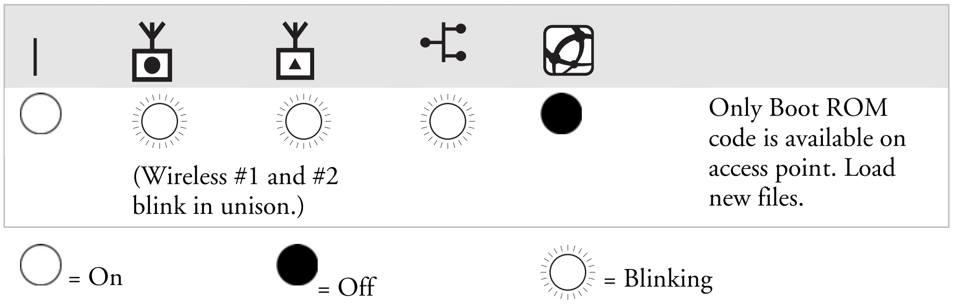
This section provides you with information on getting help with your secure network and some problems and solutions.

Problem/Question	Possible Solution/Answer
You enabled secure IAPP in your network, but the access points do not communicate with the root access point.	• 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** > **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 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 help, see "Upgrading the Access Points" on page 200.

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, you cannot ping the access point, you cannot establish a telnet session to the access point, and the LEDs display this pattern.


(Wireless #1 and #2 blink in unison.)
Only Boot ROM code is available on access point. Load new files.
○ = On
● = Off
☼ = Blinking

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 NT4/2000/XP PC.

Using the MobileLAN access Utility

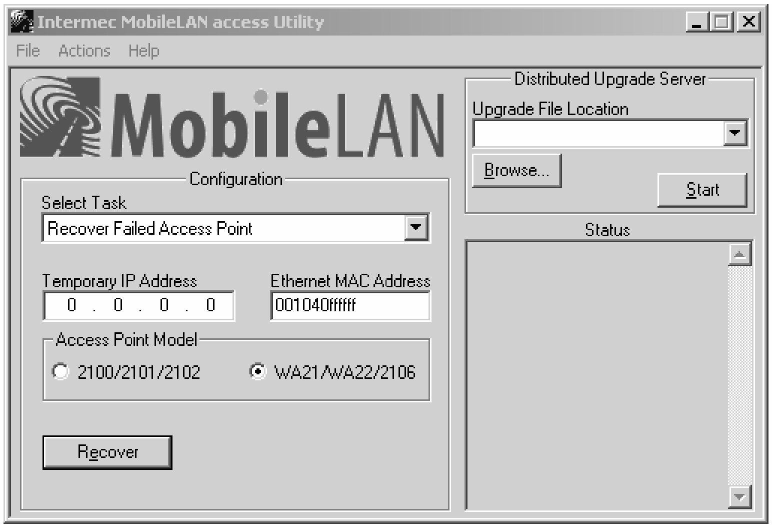
The MobileLAN access Utility v2.0 (or later) enables your PC to recover an access point that is not functioning. For help installing the MobileLAN access utility, see “Using the MobileLAN access Utility” on page 21.

To recover a failed access point

1 Download the upgrade software to your PC.

2 Start the utility.

3 In the **Select Task** field, choose **Recover Failed Access Point**.



Select Task: Recover Failed Access Point

Temporary IP Address: 0 . 0 . 0 . 0

Ethernet MAC Address: 001040ffffff

Access Point Model: ○ 2100/2101/2102 ● WA21/WA22/2106

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; for example, ap301web.bin.

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 NT4/2000/XP PC

If you do not have the MobileLAN access Utility, you can use a Windows NT4/2000/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 AP3XX.DNL file.

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 IPv4 address that you want to assign the access point. For help with IPv6 addressing, see “IP Address” in the Glossary.

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 AP3XX.DNL file to the access point. Make sure the Transfer mode is binary.

```
tftp –i IPaddress put AP824X.dnl
```

where *IPaddress* is the access point IP address you assigned in Step 1.

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 AP3XX.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

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 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:

- Wavelink Avalanche client management system. For help, see “Using the Wavelink Avalanche Client Management System” on page 166 and the Wavelink Avalanche documentation and online help. Or, you can visit the Wavelink web site at www.wavelink.com.
- 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” on page 203.

To copy the upgrade file to your PC

1. Using a web browser, navigate to www.intermec.com.
2. From the **Service & Support** menu, choose **Downloads**.
3. Select the MobileLAN access product that you are upgrading.
4. Click the software link to save the upgrade file on your PC.

Using the MobileLAN access Utility

Note: If you are using IPv6 addressing, you must use a web browser interface. For help, see “Using a Web Browser Interface” on page 203.

The MobileLAN access Utility enables your PC to act as a distributed upgrade server. 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.

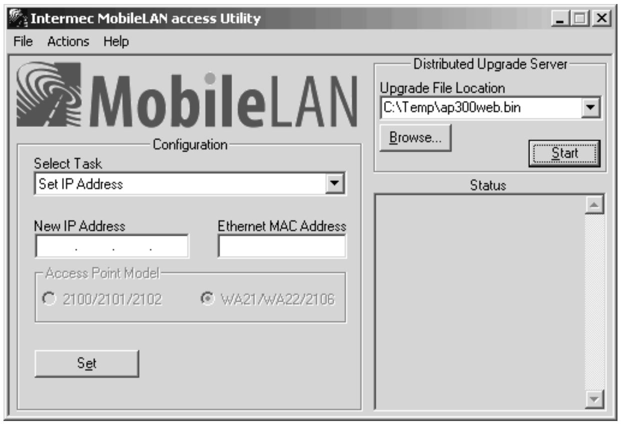
If you use this utility, you only need to configure the root access point and all access points will be upgraded. However, when the access points request the upgrade software, the utility must be active.

Note: The PC that is running the MobileLAN access Utility does not need to be on the same IP subnet as the access points.

For help installing the MobileLAN access utility, see “Using the MobileLAN access Utility” on page 21.

To upgrade the access point software

1. Start the utility.
2. In the **Upgrade File Location** field, type the path and filename of the upgrade file (ap*web.bin) or click **Browse** to find the file. For example, ap301web.bin.



Select Task: Set IP Address

Upgrade File Location: C:\Temp\ap300web.bin

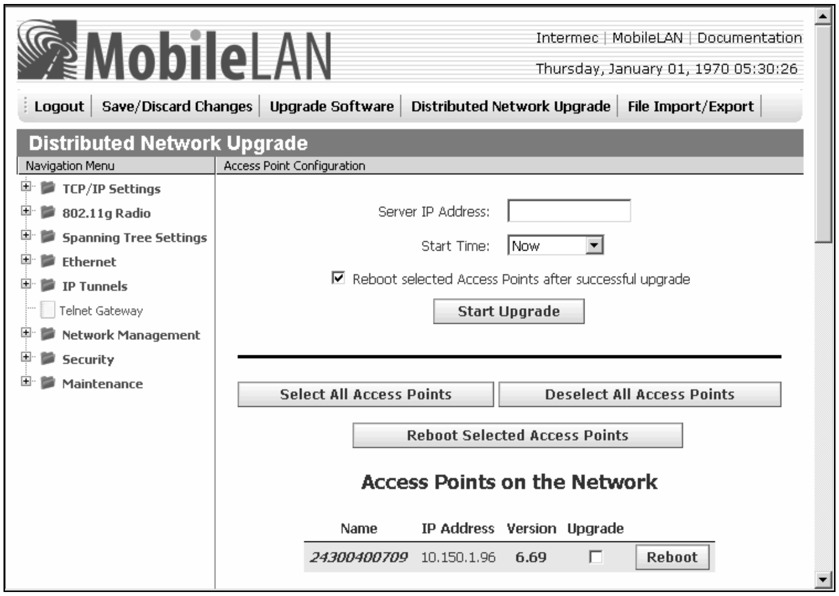
Note: If you have not already copied the upgrade file to your PC, follow the instructions on page 201.

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.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 05:30:26
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export
Distributed Network Upgrade
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Access Point Configuration
Start Upgrade
Select All Access Points
Deselect All Access Points
Reboot Selected Access Points

Server IP Address:

Start Time: Now

☑ Reboot selected Access Points after successful upgrade

Access Points on the Network

Name	IP Address	Version	Upgrade	
24300400709	10.150.1.96	6.69	□	Reboot

c In the **Server IP Address** field, enter the IP address of the PC that contains the software release and that is running the utility.

d In the **Start Time** field, choose when you want the upgrade to start.

e Check the **Reboot selected Access Points after successful upgrade** check box if you want the access points to run the upgraded software after it is downloaded.

If you 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 upgraded 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.

c To select all the access points that are listed, click the **Select All Access Points** button. Or to deselect all the 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.

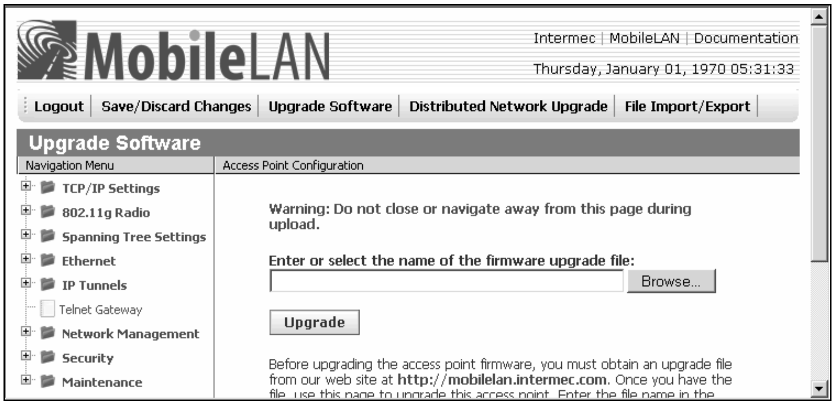
Using a Web Browser Interface

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.



Warning: Do not close or navigate away from this page during upload.

Enter or select the name of the firmware upgrade file:

Before upgrading the access point firmware, you must obtain an upgrade file from our web site at **http://mobilelan.intermec.com**. Once you have the file, use this page to upgrade this access point. Enter the file name in the

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, ap301web.bin.

Note: If you have not already copied the upgrade file to your PC, follow the instructions on page 201.

4 Click **Upgrade** to start the upgrade. The upgrade may take up to 3 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 3 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 5 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 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 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 WA2XG family of access points. This chapter covers these topics:

- Configuring and managing the Telnet Gateway Appliance (TGAP)
- Using the Instant On server (EasyADC only)
- Understanding transparent files
- Using the AP monitor
- Using Console Command mode
- Creating script files
- Copying files to and from the access point

Configuring and Managing the Telnet Gateway Appliance (TGAP)

The MobileLAN access WA2X products can work as a Telnet Gateway APpliance (TGAP). The TGAP supports VT, 5250, 3270, and Norand Native emulation and it provides these features:

- Supports end devices running TE 2000 clients v7.49 or later. You can configure the gateway to allow clients to communicate with up to eight different TCP/IP hosts. The gateway supports up to 100 clients.
- Allows client session persistence. If a TE 2000 client loses connectivity for any reason (roams out of range, was powered off, or lost battery power), the gateway keeps the client's session alive to its TCP/IP host.
- If you are running a TE 2000 application and using the Norand Native data stream, the TGAP can replace the Intermec Application Server.

If you configure the TGAP so that more than one host communicates with TE 2000 clients on the same terminal port number, a menu is sent to the client when it first connects. The user must choose with which host they want to communicate.

If you configure the TGAP so that a host communicates with TE 2000 clients on terminal port 23, the "This AP" option appears in the menu that is sent to the clients that are configured to use terminal port 23. The user must choose between connecting to a port 23-defined host that is listed in the TGAP host table or connecting to the access point itself (because it is also running a telnet client). Intermec recommends that you do not use a client to configure the access point. To prevent this option from appearing in the menu, from the access point main menu, click the **Security** link and clear the **Allow Telnet Access (Port 23)** check box.

The TGAP is transparent to both the TE 2000 client and the host. It listens for connections from clients. When a client connects, the gateway establishes and maintains the connection to a host for the client. If the client loses connectivity, the gateway holds the host connection open until the client can reconnect.

When configuring the TE 2000 clients, you configure the host name to be the IP address. Also, you need to set the parameters in the next table.

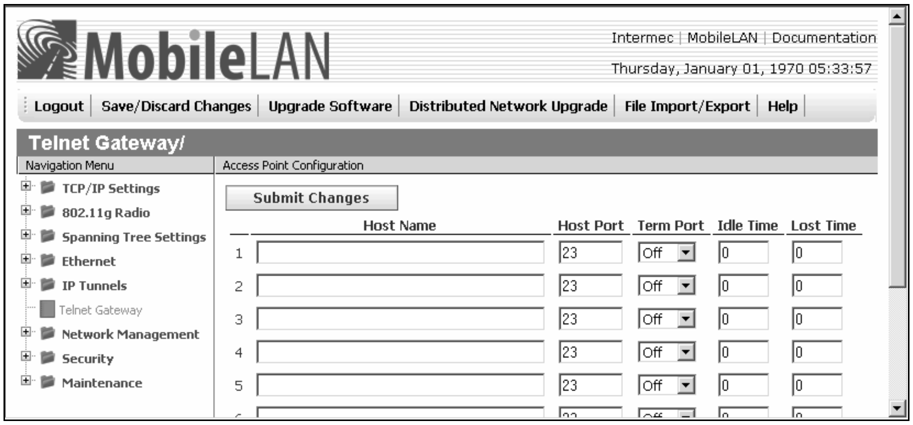
Note: Currently, the TE 2000 clients cannot run an auto-login script to log into the TGAP.

TE 2000 Host Parameter Descriptions

Parameter	Description
Host Name	Enter the TGAP IP address.
Port Number	Enter the port number that matches the TGAP Term Port number.
Emulation	Choose the emulation type.
RTC over TCP	Enable this option

To configure the TGAP

1 In the Navigation Menu, click **Telnet Gateway**. The Telnet Gateway screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 05:33:57
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Telnet Gateway/
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Submit Changes

	Host Name	Host Port	Term Port	Idle Time	Lost Time
1		23	Off	0	0
2		23	Off	0	0
3		23	Off	0	0
4		23	Off	0	0
5		23	Off	0	0

2 Configure the parameters for up to eight TCP/IP hosts. 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” on page 30.

Telnet Gateway Screen Parameters

Parameter	Description
Host Name	Enter the IP address or the DNS name of the host.
Host Port	Enter the TCP port number of the host server. Communications between the gateway and the host occur on the host port. This port is usually 23, unless the host has been specially configured.
Term Port	Enter the TCP port number that the TE2000 client uses to connect to the gateway. Communications between the client and the gateway occur on the Term Port. If this port is on, it is usually set to 23, unless the client has been specially configured. **Off:** The Term Port is disabled (default). **23:** The TCP port reserved by the IANA for telnet servers. The client will be able to connect normally. **5000** to **5009:** Optional TCP ports to which a specially-configured client may connect.

Telnet Gateway Screen Parameters (continued)

Parameter	Description
Idle Time	Enter the number of minutes that the gateway maintains the host connection while a client is idle or disconnected. This timeout is useful if the host does not have an inactivity timer. You can enter a number from 1 to 255. However, this number must be greater than the number of minutes set in the Lost Time field plus 11 minutes. To disable the timeout, set it to zero. If you disable this timeout, the gateway never ends the telnet session, regardless of how long the client is idle or disconnected.
Lost Time	Enter the number of minutes that the gateway maintains the host connection while a client is disconnected. Values longer than Idle Time serve no purpose. This timeout is useful because it provides a shorter timeout for a client that has lost its connection than for an idle client. You can enter a number from 1 to 255. To disable the timeout, set it to zero. If you disable this timeout, the gateway never ends the telnet session, regardless of how long the client is disconnected. Note that if the gateway cannot communicate with the client for approximately 10 minutes, it will disconnect the client.

To manage the TGAP

- In the Navigation Menu, click **Maintenance** > **Telnet Connections**. For help, see the next table.

Telnet Connections Screen Parameters

Parameter	Description	
Term #	The row number of this table.	
Host #	A number from 1 to 8, indicating the host (as configured on the Telnet Gateway screen) to which the client is connecting.	
Terminal IP	The IP address of the client.	
Protocol	The protocol being used for the connection: 3270, 5250, ANSI, or Native.	
Status	Indicates the status of the host and client and may include:	
	Host Invalid	**Term Connect**
	Host Connecting	**Term Closed**
	Host No Route	**Term Lost**
	Host Missing	**Term Idle**
	Host Refused	**Term Disconnect**
	Host Closed	**Term Sent**
	Host Sent	
Age	The number of minutes since the last contact with the client.	

Using the Instant On Server (EasyADC Only)

Currently, the Instant On server is only used in EasyADC systems. The Instant On server provides device-level distribution of firmware, applications, and settings to up to 128 wireless end devices that have the Instant On client installed.

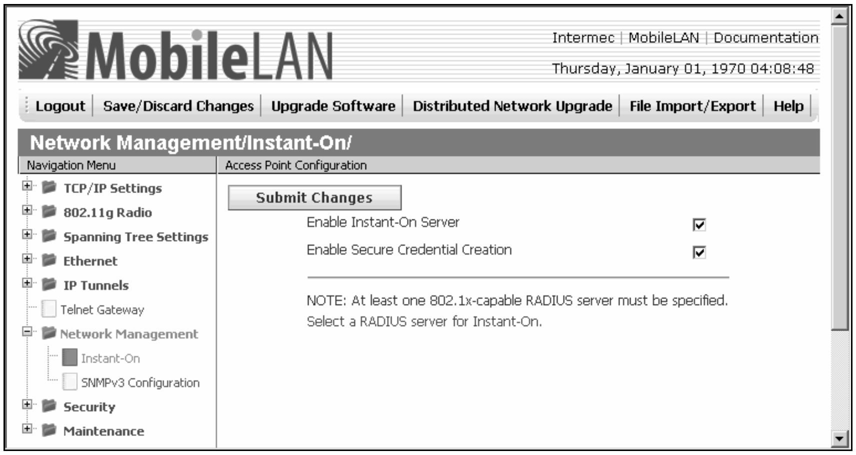
Access point that are part of EasyADC systems also contain an optional memory card in radio slot 2.

Verifying the Instant On Server is Enabled

The EasyADC Configuration Wizard enables and launches the Instant On server so you should not have to perform any system administration tasks.

To verify the Instant On server is enabled

1 In the Navigation Menu, click **Network Management** > **Instant-On**. The Instant-On screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 04:08:48
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export | Help
Navigation Menu
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Instant-On
SNMPv3 Configuration
Security
Maintenance
Access Point Configuration
Submit Changes

Network Management/Instant-On/

Enable Instant-On Server ☑

Enable Secure Credential Creation ☑

NOTE: At least one 802.1x-capable RADIUS server must be specified. Select a RADIUS server for Instant-On.

2 Verify that the **Enable Instant-On Server** check box is checked. If this check box is clear, the Instant On server capabilities have not been enabled in this access point.

3 Check or clear the **Enable Secure Credential Creation** check box. If you check this check box, the Instant On server creates of TTLS or PEAP security credentials for Instant On clients requesting this service.

Accessing the Memory Card

Access points that are shipped with EasyADC systems contain a mini-PCI flash memory card in radio slot 2. This memory card contains files required for the EasyADC system. You can access this memory card using some of the Service Mode commands described in this chapter if you include the segment name app: to indicate the memory card.

Commands for Accessing the Memory Card

Command	Description
`FD app:`	To display the contents of the memory card.
`FDEL app:`*`filename`*	To “delete” a file from the memory card.
`FE app:`	To erase all the files on the memory card.

Understanding Transparent Files

The WA2XGs support transparent files, which are files without file headers. Transparent files all have the date May 14, 2002 (5-14-2002) and have no version.

The advantage of using file headers is that the date and file versions are correct when you use the FD command to view the directory. All Intermec-provided .DNL files have file headers. All files to be uploaded by script files must have file headers.

For help using the TFTP GET command with transparent files, see page 207.

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.

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.

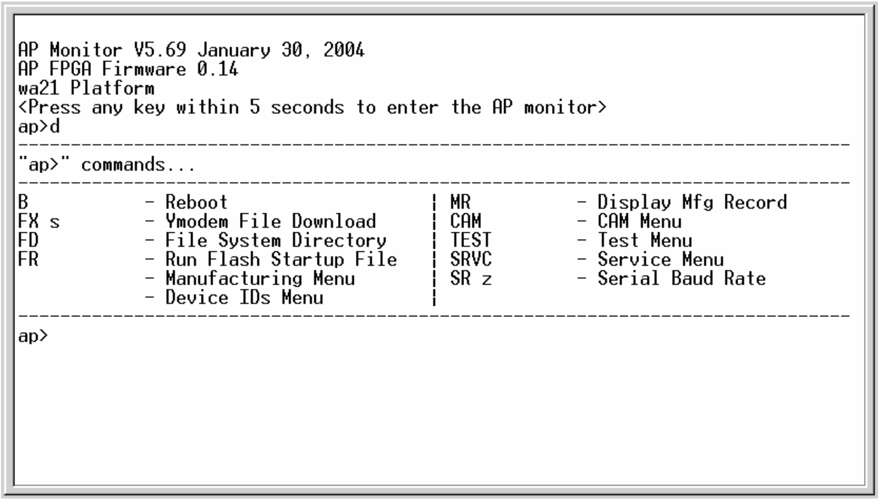
3 When you see the message <Press any key within 5 seconds to enter the AP monitor> during the boot process, press Enter. The ap prompt (ap>) appears.

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 V5.69 January 30, 2004
AP FPGA Firmware 0.14
wa21 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.

Syntax: `FX 1`

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 wireless end device. 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 supports data rates significantly higher than the radio ports, all frames cannot be forwarded from 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.

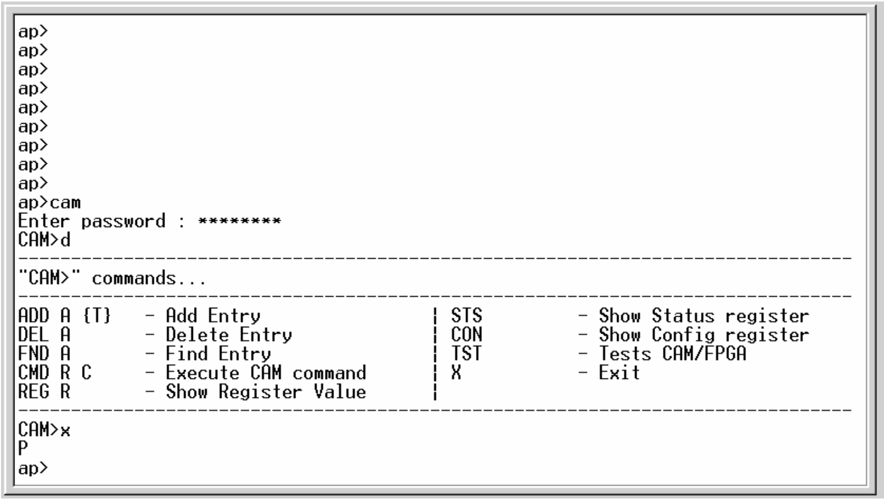
To exit CAM mode

- At the CAM prompt, type `X` and press **Enter**.

You return to 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>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>cam
Enter password : ********
CAM>d
-------------------------------------------------------------------------------
"CAM>" commands...
-------------------------------------------------------------------------------
ADD A {T}   - Add Entry              | STS        - Show Status register
DEL A       - Delete Entry           | CON        - Show Config register
FND A       - Find Entry             | TST        - Tests CAM/FPGA
CMD R C     - Execute CAM command    | X          - Exit
REG R       - Show Register Value    |
-------------------------------------------------------------------------------
CAM>x
P
ap>
```

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.

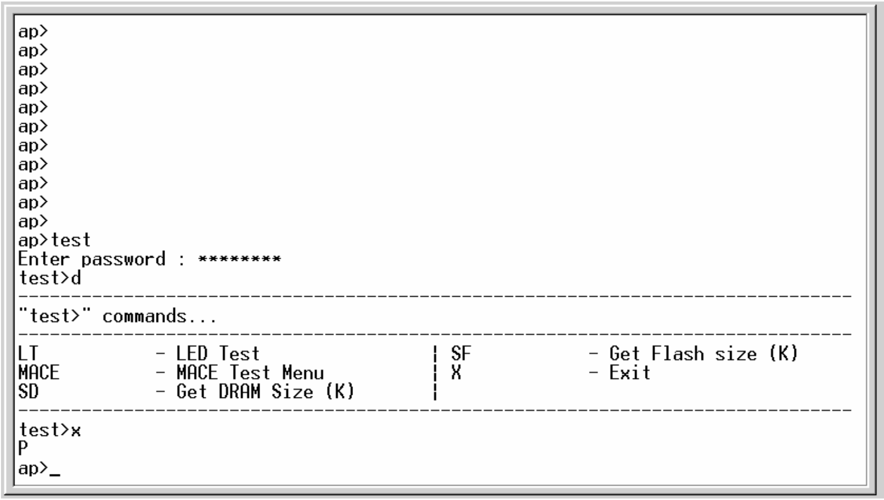
To exit Test mode

- 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>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>test
Enter password : ********
test>d
---------------------------------------------------------------------------
"test>" commands...
---------------------------------------------------------------------------
LT          - LED Test              | SF          - Get Flash size (K)
MACE        - MACE Test Menu        | X           - Exit
SD          - Get DRAM Size (K)     |
---------------------------------------------------------------------------
test>x
P
ap>_
```

Using Service Mode Commands

In Service mode, you can perform file functions, flash memory functions, and optional memory card functions. For example, you can deleting a file, downloading a file using the Ymodem protocol, and erasing flash memory.

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.

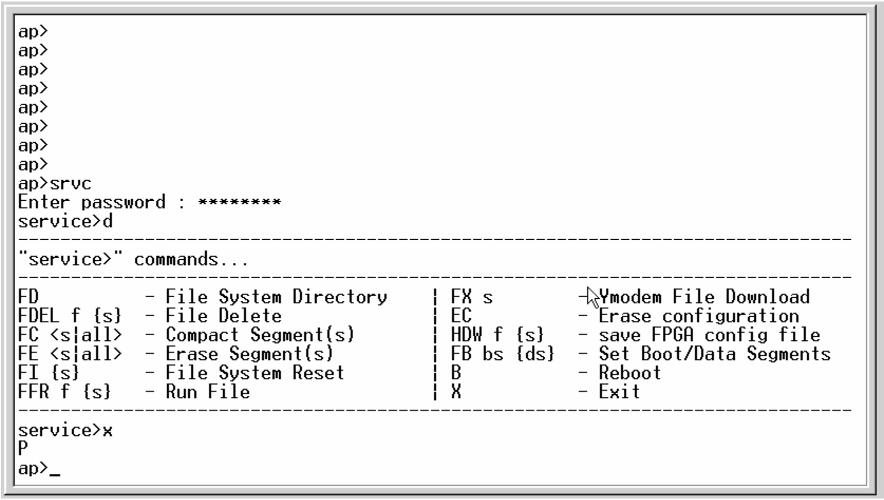
To exit Service mode

- 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>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
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>x
P
ap>_
```

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`

FC

Purpose: Compacts the files.

Syntax: `FC 1`

FD

Purpose: Displays the flash file system directory, including information about the boot file and the file type: E (executable), D (data), and T (transparent). For information about transparent files, see page 207.

Syntax: `FD`

Example: To display the contents of the flash memory, enter:

```
FD
```

To display the contents of the memory card, enter:

```
FD APP:
```

FDEL

Purpose: Deletes a particular file.

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 use the FE command to erase the flash memory.

Syntax:

```
FDEL filename
```

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

Example: To delete the file AP824X.PRG from the flash memory, enter:

```
FDEL 1:AP824X.PRG
```

To delete the file FILE.DAT from the optional memory card, enter:

```
FDEL APP:FILE.DAT
```

FE

Purpose: Erases all the files in the flash memory, including those that have been “deleted” with FDEL. 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 1
```

Example: To erase the contents of the flash memory, enter:

```
FE 1
```

To erase the contents of the memory card, enter:

```
FE APP:
```

FFR

Purpose: Runs a program *f*.

Syntax:

```
FFR filename
```

where *filename* is the program name.

Example: To run program UAPBOOT.PRG from the flash memory, enter:

```
FFR UAPBOOT.PRG 1
```

FI

Purpose: Reinitializes the access point file system. If the access point file system becomes corrupt, use this command to reset it.

Syntax:

```
FI
```

FX

Purpose: Downloads a file using Ymodem batch protocol into the flash memory.

Syntax: `FX 1`

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 filename`

where *filename* is the FPGA configuration filename.

Using Command Console Mode

You can use the Command Console mode to manipulate some access point files, flash memory, and the optional memory card. You can also use Command Console mode to upgrade access points using TFTP and script files.

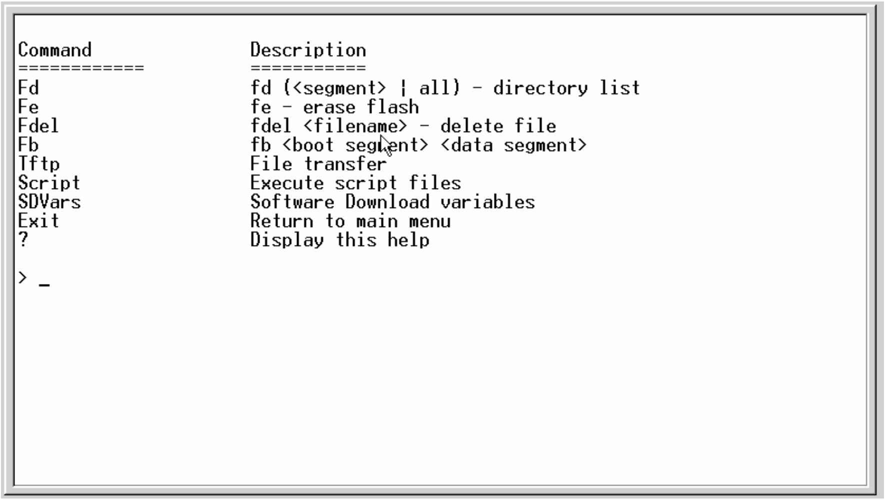
You access the Command Console mode through the serial port using a communications program or over the network using a telnet session. You cannot access Command Console mode using a web browser interface.

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” on page 23.

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 commands require that you enter filenames. These commands may specify that you precede the filename with a 1 followed by a colon. For example, `1:ap824x.prg`.

FD

Purpose: Displays the flash file system directory, which includes information about the boot file and file type: E (executable), D (data), and T (transparent). Use this command to ensure that the correct version of the file is in the active boot segment. For information about transparent files, see page 207.

Syntax:

```
FD
```

Example: To display the files loaded in the flash memory, enter:

```
FD 1
```

Note: If the flash memory 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.

To show the files loaded in the memory card, enter:

```
FD app:
```

FDEL

Purpose: Deletes a particular file.

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 filename
```

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

Example: To delete the file AP824X.PRG from the flash memory, enter:

```
FDEL 1:AP824X.PRG
```

To delete the file FILE.DAT from the memory card, enter:

```
FDEL APP:FILE.DAT
```

FE

Purpose: Erases all the files, including those that have been “deleted” with FDEL. 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 1
```

Example: To erase the contents of the flash memory, enter:

```
FE 1
```

To erase the contents of the memory card, enter:

```
FE app:
```

SCRIPT

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

Syntax:

```
SCRIPT filename
```

where *filename* is the name of the script file to be executed.

For more information about using the script command, see “Creating Script Files” on page 207.

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.

Syntax:

```
TFTP GET IPaddress foreignfilename localfilename
```

where:

IPaddress is the IP address or DNS name of the server. You can use an asterisk (*) here if you want to use the value in the internal variable serveripaddress (as defined on page 207).

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 begin with a segment number or name followed by a colon. You may or may not have to specify a filename after the colon: if the file has a header, the filename is optional; if the file does not have a header, the filename is required.

Example: If the file has a header, you do not have to include a filename as part of the *localfilename* because the filename is set to the filename embedded in the file header on the server:

```
TFTP GET * file.dat 1:
```

If the file is a transparent file (without a header), you must include a filename as part of the *localfilename*:

```
TFTP GET * file.dat 1:file.dat
```

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 flash memory on the WA2XG.

```
TFTP GET 1.2.3.4 C:\STARTUP\UAP.DNL 1:
```

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.

TFTP GET (*continued*)

Error Message	Explanation
Can’t write file	The file may be too big. The file may not have an 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 or DNS name of the server. You can use an asterisk (*) here if you want to use the value in the internal variable serveripaddress (as defined on page 207).

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 AP824X.PRG that is saved in the active boot drive on the access point client and stores it in the flash memory on the WA2XG server that has IP address 1.2.3.4.

```
TFTP PUT 1.2.3.4 IB:AP824X.PRG 1:AP824X.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.

TFTP PUT (*continued*)

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` *`access`*

where *access* is blank for read-only access (default), or rw for read/write access. TFTP does not require any authentication, so a read/write TFTP server is very insecure and should be used only briefly. When the access point boots, read-only access is restored.

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 should be read from the client perspective.

TFTP SERVER STOP (*continued*)

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 an 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.

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 1

sdvars set checkpoint 2

TFTP get * ap824x.prg 1

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 set nextpoweruptime to 0 if it has not already been reached by the countdown. By resetting nextpoweruptime to 0, the timer stops so the access point 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 and

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 executes a series of commands. For example, when you upgrade the WA2XG, you typically need to erase the flash memory, 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 an LF or CR.
- You can only have one command per line.
- Any file that is to be uploaded by script must have a file header. This does not include the script file itself.
- 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.

This sample script will upgrade an access point. This script is based on upnopath.dnl, which is included in the access point upgrade package. A header file is not required. All files are copied into segment 1: on the access point.

Sample Script File for Upgrading an Access Point

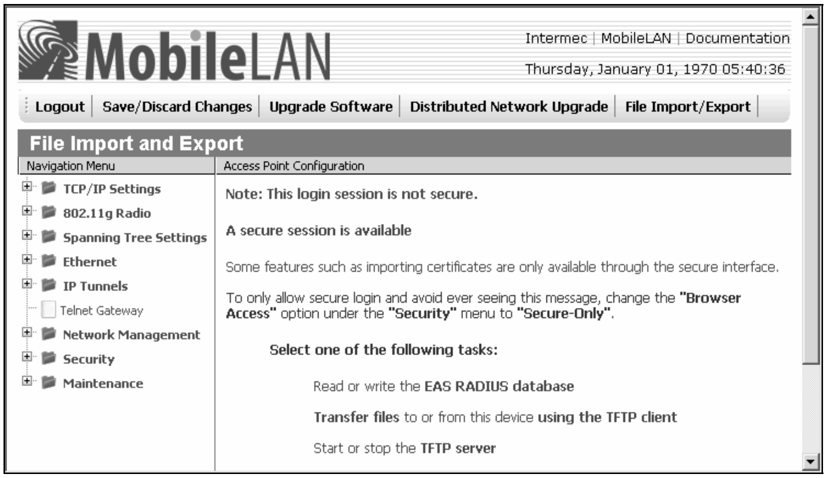
```
file sdvars set checkpoint 1
file fe 1:
file sdvars set checkpoint 2
file tftp get * software\ap824x.dnl 1:
file tftp get * software\boot824x.dnl 1:
file tftp get * software\act.dnl 1:
file tftp get * software\ap3890.dnl 1:
file tftp get * software\applets.dnl 1:
file tftp get * software\cert.dnl 1:
file tftp get * software\closed.dnl 1:
file tftp get * software\discinca.dnl 1:
file tftp get * software\easdb.dnl 1:
file tftp get * software\echo.dnl 1:
```

Sample Script File for Upgrading an Access Point (continued)

```
file tftp get * software\favicon.dnl 1:
file tftp get * software\file.dnl 1:
file tftp get * software\fileimp.dnl 1:
file tftp get * software\filemenu.dnl 1:
file tftp get * software\fpga8245.dnl 1:
file tftp get * software\fsys.dnl 1:
file tftp get * software\help.dnl 1:
file tftp get * software\hlp.dnl 1:
file tftp get * software\jsutil.dnl 1:
file tftp get * software\login.dnl 1:
file tftp get * software\logo.dnl 1:
file tftp get * software\logo2.dnl 1:
file tftp get * software\menu.dnl 1:
file tftp get * software\netdwnl.dnl 1:
file tftp get * software\open.dnl 1:
file tftp get * software\sftdwnl.dnl 1:
file tftp get * software\sta3890.dnl 1:
file tftp get * software\stastats.dnl 1:
file tftp get * software\tbldata.dnl 1:
file tftp get * software\tftpcl.dnl 1:
file tftp get * software\tftpsrv.dnl 1:
file tftp get * software\welcome.dnl 1:
file sdvars set checkpoint 5
file sdvars set NextPowerUpTime 00:00:00:5
```

Copying Files To and From the Access Point

You can accomplish a variety of file import/export tasks from the File Import/Export screen. In the menu bar, click **File Import/Export**, and the File Import and Export screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 05:40:36
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export
File Import and Export
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance

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"**.

Select one of the following tasks:

Read or write the **EAS RADIUS database**

Transfer files to or from this device **using the TFTP client**

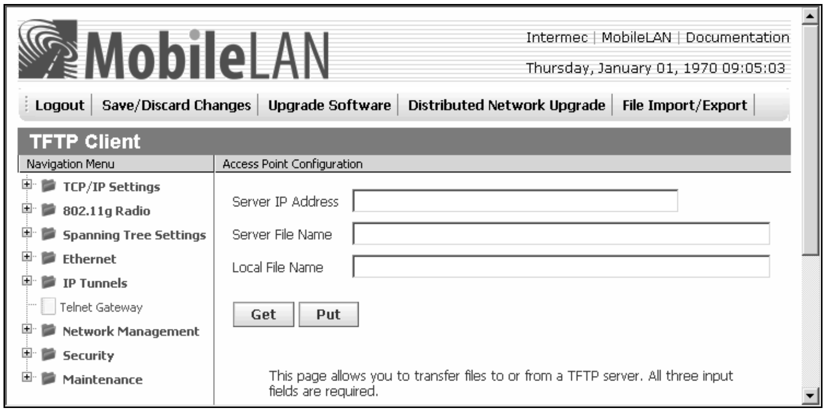
Start or stop the **TFTP server**

From this screen you can perform these tasks:

- To import or export an EAS RADIUS database file. For help, see “Exporting and Importing Databases” on page 161.
- To transfer files to and from a TFTP server
- To start or stop the TFTP server

To transfer files to and from a TFTP server

1 Click **Transfer files to or from this device using the TFTP client**. The TFTP Client screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 09:05:03
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export
TFTP Client
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Get
Put

Server IP Address

Server File Name

Local File Name

This page allows you to transfer files to or from a TFTP server. All three input fields are required.

2 In the **Server IP Address** field, enter the IP address or DNS name of the TFTP server.

3 In the **Server File Name** field, type the name in the format required by the operating system of the server.

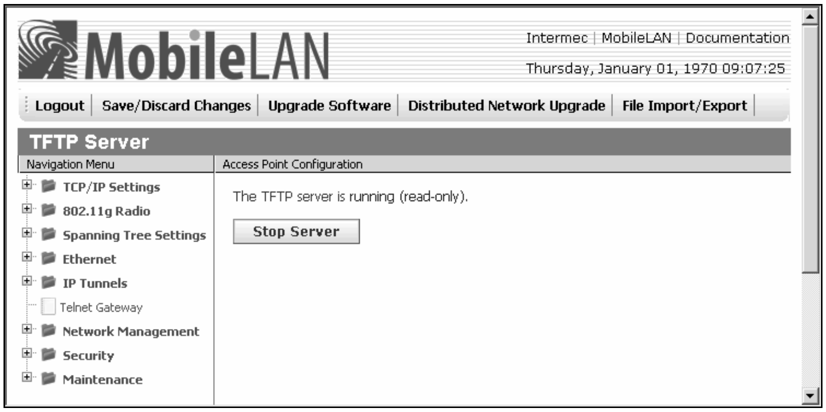
4 In the **Local File Name** field, type the file name for the file on the device. Access point filenames use this format: *segment*:*filename*, where *segment* is 1 for memory or app for the memory card.

When performing TFTP GET commands, this field need only contain the segment identifier (1 or app) because the file name is determined by the header of the downloaded file.

5 Click **Get** or **Put**.

To start or stop the TFTP server

1 Click **Start or stop the TFTP server**. The TFTP Server screen appears.


MobileLAN
Intermec | MobileLAN | Documentation
Thursday, January 01, 1970 09:07:25
Logout | Save/Discard Changes | Upgrade Software | Distributed Network Upgrade | File Import/Export
TFTP Server
Navigation Menu
Access Point Configuration
TCP/IP Settings
802.11g Radio
Spanning Tree Settings
Ethernet
IP Tunnels
Telnet Gateway
Network Management
Security
Maintenance
Stop Server

The TFTP server is running (read-only).

2 Click **Stop Server** to stop the TFTP server. Or click **Start Server** to start the TFTP server.

You can also use the TFTP SERVER START and STOP commands, described on page 207, to start and stop the TFTP server.

A Specifications

This appendix provides specifications 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 approved in the destination country.

Specifications

WA22G

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)
POE 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	802.11g
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
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x, MobileLAN access
Regulatory Approvals	EN 550022/CISPR 22 Class A; FCC Part 15 & ICES-003 Class A; C tick Marked (AS 3548); CE Market, Compliant with RTT&E, EMC, LVD directives; (See separate radio approvals); UL Listed 1950 & IEC 60529-IP53; CSA Certified, C22.2 #950 & C22.3 #94-ENC 3.5; TUV Licensed, EN 60950 & EN 60529-IP53; NYCE Certified, NOM 19, plenum-rated

WA21G

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
POE electrical rating	⎓ 48V, 315 mA
Operating temperature Standard Heater (optional), AC only Heater/insulated bag (optional), AC only	 -25°C to +70°C (-13°F to +158°F) -30°C to +70°C (-22°F to +158°F) -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	IP54 (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	802.11g
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
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x, MobileLAN access
Regulatory Approvals	EN 55022 / CISPR 22 ClassA; FCC Part 15 & ICES-003 Class A; C tick Marked (AS 3548); CE Market, compliant with RTT&E, EMC, LVD Directives (see separate radio approvals); UL listed UL 1950/C22.2 #950 IEC; 60529-IP53 and C22.2 #94-ENC 3.5; TUV Licensed, EN 60950 & EN 60539-IP53; NYCE Certified; NOM 19, plenum-rated.

802.11g Radio Specifications (Actiontec P/N 0832-0040-000)

Frequency band	2.4 to 2.5 GHz worldwide
Type	Direct sequence, spread spectrum
Modulation	Direct sequence, spread spectrum (CCK, DQPSK, DBPSK)
Power output	63 mW (18 dBm)
Basic data rate	11, 5.5, 2, and 1 Mbps
Extended data rate	54, 48, 36, 24, 18, 12, 9, and 6 Mbps
Channels	11 (North America), 13 (Europe), 4 (France), 14 (Japan), 1 (Israel)
Range (Maximum power output, 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	802.11 Wired Equivalent Privacy (WEP) standard, WEP 64, WEP 128, Wi-Fi Protected Access (WPA)
*Lowering the power output level reduces the range.	

Antennas and Antenna Accessories

The following tables identify many of the Intermec antennas and antenna accessories for the radios in your access point. Contact your local Intermec representative for detailed information.

2.4 GHz Antennas (For 802.11g Radios)

Part Number	Description
063363	Antenna, 2.4 GHz, 5 dBi, omni
063366	Antenna, 2.4 GHz, 14 dBi, flat panel
063365	Antenna, 2.4 GHz, 15 dBi, Yagi
065349	Antenna, 2.4 GHz, 9 dBi, omni
066147	Antenna, 2.4 GHz, omni
067261	Antenna, 2.4 GHz, 3 dBi, mini omni
067262	Antenna, 2.4 GHz, 5 dBi, dual flat
067263	Antenna, 2.4 GHz, 9 dBi, flat panel
071121	Antenna, 2.4 GHz, 3 dBi, diversity
071122	Antenna, 2.4 GHz, corner reflector
073304	Antenna, 2.4 GHz, diversity, 3 dbi, omni, tnc
073373	Antenna, 2.4 GHz, omni, 3dbi, tnc
073374	Antenna, 2.4 GHz, dual flat, 5 dbi, TNC
073984	Antenna, 2.4 GHz, corner reflector, 14 dbi

Antenna Accessories

Part Number	Description
061475	Cable connector, Type N polarized
063146	Cable connector, Type N
063245	Cable, Plug/N Plug, 1.5 m (5 ft)
063246	Cable, Plug/N Plug, 6.1 m (20 ft)
064616	Cable, TNC Plug/N Plug, 7.6 m (2.5 ft)
073446	Cable, TNC Plug/N Plug, LRM400, 1.85 m (6 ft)
071178	Cable, TNC Plug/N Plug, LRM400, 3.7 m (12 ft)
071179	Cable, N Plug/N Plug, LMR600, 9.1 m (30 ft)
064432	LMR400 cable, 30.5 m (100 ft)
589377	LMR400 cable prep tool
067265	Adapter cable (to cable), TNC, Plug/N Recept, LMR200, 0.3 m (1 ft)
067266	Adapter cable (to antenna), TNC, Plug/N Plug, LMR400, 0.61 m (2 ft)

Antenna Accessories (continued)

Part Number	Description
061868	Lightning suppressor and bracket
063198	Splitter, 2.4 GHz only
063153	Shrink tubing kit
073518	Lightning protector, 2.3 GHz to 5.9 GHz

Antenna Accessories for Plenum Rating

Part Number	Description
072821	Adapter cable (to cable), TNC Plug/N Recept, LMR200, 0.3 m (1 ft)
072822	Adapter cable (to antenna), TNC Plug/N Plug, LMR400, 0.61 m (2 ft)
072823	Cable, TNC Plug/N Plug, LRM400, 3.7 m (12 ft)
073447	Cable, TNC Plug/N Plug, LRM400, 1.85 m (6 ft), plenum-rated
072824	Cable, TNC Plug/N Plug, 7.6 m (2.5 ft)
072825	Cable, Plug/N Plug, 1.5 m (5 ft)
072826	Cable, Plug/N Plug, 6.1 m (20 ft)
072827	Cable, N Plug/N Plug, LMR600, 9.1 m (30 ft)

B Default Settings

This appendix provides factory defaults for reference purposes only.

Default Settings

This section lists the factory default settings. 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 or DNS name	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	
DNS Address 1	4 nodes, 0 to 255	0.0.0.0	
DNS Address 2	4 nodes, 0 to 255	0.0.0.0	
DNS Suffix 1	0 to 31 characters	(blank)	
DNS Suffix 2	0 to 31 characters	(blank)	
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)	
DHCP User Class	DHCP user class identifier, as defined in RFC 3004	(blank)	
DHCP Vendor Class	DHCP vendor class identifier, as defined in RFC 2132	(blank)	
DHCP for Access Point Network	Use Any Available DHCP Server, Only Use Access Point DHCP Server	Use Any Available DHCP Server	
Auto ARP Minutes	0 to 120	5	
SNTP Server Name	4 nodes, 0 to 255 or DNS name		
Time Zone	4 to 7 characters		

IPv6 Configuration Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable IPv6	Check/Clear	Clear	
Enable Autoconfiguration	Check/Clear	Check	
IPv6 Address	32 hex digits grouped into sets of four separated by colons		
IPv6 Subnet Mask	32 hex digits grouped into sets of four separated by colons	64	
IPv6 Router	32 hex digits grouped into sets of four separated by colons		

DHCP Server Setup Menu Defaults

Parameter Name	Range	Default	Your Site?
Low Address	4 nodes, 0 to 255	10.10.10.100	
High Address	4 nodes, 0 to 255	10.10.10.199	
Lease Time	days:hours:minutes	0:00:20	
Permanently Save IP Address Mappings	Check/Clear	Clear	
IP Subnet Mask	4 nodes, 0 to 255	255.255.255.0	

802.11g Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Frequency	Channel 1 to 11, 2412 to 2462 MHz	Channel 03, 2422 MHz	
Node Type	Master, Station, Disabled	Master	
SSID (Network Name)	0 to 32 characters	INTERMEC	
Member Limit	128 or 100	128 for Primary, 100 for Secondary	

802.11g Radio Menu Defaults (continued)

Parameter Name	Range	Default	Your Site?
Advanced Configuration parameters			
Client Type/Performance	11b/11g with range reliability (Not Wi-Fi), 11b/11g with Wi-Fi compatible rates (Wi-Fi), 11g only for better throughput (Wi-Fi), 11b/11g using 11b supported rates (Wi-Fi)	11b/11g with range reliability (Not Wi-Fi)	
Power Output Level	Maximum, Medium, Low, Minimum	Maximum	
Enable Medium Reservation	Check/Clear	Clear	
Reservation Threshold (Appears if Enable Medium Reservation is enabled)	1 to 65535	500	
Fragmentation Threshold	256 to 1600	1600	
Antenna Control	Two Antennas, One Antenna	Two Antennas	
Mixed Mode Performance	Optimize Mixed (802.11b and 802.11g), Optimize for 802.11g clients, Optimize for 802.11b clients	Optimize Mixed (802.11b and 802.11g)	
Enable Data Rate Fallback	Check/Clear	Check	
Disallow Network Name of ‘ANY’	Check/Clear	Clear	
DTIM Period	1 to 65535	1	
Inbound Filters (Primary Only)			
Allow IAPP	Check/Clear	Check	
Allow Wireless Transport Protocol (WTP)	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	

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 GVRP for VLAN	Check/Clear	Clear	
Rightmost LED Behavior	Ready-to-Work Indicator/Spanning Tree Root Indicator	Ready-to-Work Indicator	
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 Flooding	Universal, Hierarchical, Disabled	Hierarchical	
Multicast Outbound to Secondary LANs	Enabled globally, Set locally	Set locally	
Allow Multicast Outbound to Terminals	Check/Clear	Check	
Unicast Flooding	Universal, Hierarchical, Disabled	Disabled	

Global Flooding Menu Defaults (continued)

Parameter Name	Range	Default	Your Site?
If **Unicast Flooding** is **Universal** or **Hierarchical**:			
Unicast Outbound to Secondary LANs	Enabled globally Set locally	Set locally	
Allow Unicast Outbound to Terminals	Check/Clear	Clear	
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 hex pairs 00 through FF	80 F3	
2	Two sets of hex pairs 00 through FF	81 37	
3 through 20	Two sets of hex pairs 00 through FF	00 00	

Telnet Gateway Configuration Menu Defaults

Parameter Name	Range	Default	Your Site?
Host Name	IP address or DNS name	(blank)	
Host Port	23	23	
Term Port	Off, 23, 5000, 5001, 5002, 5003, 5004, 5005, 5006. 5007, 5008, 5009	Off	
Idle Time	1 to 255	0 (disabled)	
Lost Time	1 to 255	0 (disabled)	

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	

Ethernet Received Filters Menu Defaults

Parameter Name	Range	Default	Your Site?
Static Address Table			
1 through 20	Six sets of hex pairs 00 through FF	00 00 00 00 00 00	
Received Frame Type Filters			
Allow/Pass	Check/Clear	Check	
Scope	Unlisted/All	Unlisted	
Predefined Received Subtype Filters			
Allow/Pass	Check/Clear	Check	

Ethernet Received Filters Menu Defaults (continued)

Parameter Name	Range	Default	Your Site?
Customizable Received 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 hex pairs 00 through FF	00 00	
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 (Appears if Mode is Listen)	Check/Clear	Clear	
Allow IP Multicast (Appears if Mode is Originate if Root)	Check/Clear	Clear	
Multicast Address	4 nodes, 0 to 255	224.0.1.65	
IP Addresses			
1 through 8	4 nodes, 0 to 255 or DNS name up to 31 characters	(blank)	

IP Tunnel Transmit Filters Menu Defaults

Parameter Name	Range	Default	Your Site?
Transmit Frame Type Filters			
Allow/Pass	Check/Clear	Clear	
Scope	Unlisted/All	Unlisted	
Predefined Transmit Subtype Filters			
Allow/Pass	Check/Clear	Clear (except Check for NNL)	
Customizable Transmit 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 hex pairs 00 through FF	00 00	

Network Management Menu Defaults

Parameter Name	Range	Default	Your Site?
Allow Avalanche Access	Check/Clear	Check	
Avalanche Agent Name	IP address or DNS name	(blank)	
Enable SNMPv3	Check/Clear	Check	
Enable SNMPv1/ SNMPv2c	Check/Clear	Check	
SNMP Ready Community	1 to 15 characters	public	
SNMP Write Community	1 to 15 characters	CR52401	
SNMP Secret Community	1 to 15 characters	Secret	
Target Status	Disabled, Deleted, Enabled, Enabled (Reliable)	Disabled	
Target Name	1 to 15 characters	traptarget*x*	
Target IP Address	IPv4 address	0.0.0.0	
Address Table	Check/Clear	Clear	
Bridge State Table	Check/Clear	Clear	
Route Table	Check/Clear	Clear	
Event Tables	Check/Clear	Clear	

Instant On Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable Instant On Server	Check/Clear	Clear	

SNMPv3 Menu Defaults

Parameter Name	Range	Default	Your Site?
Username	1 to 15 characters	INTERMEC	
Password	1 to 15 characters	INTERMEC	
Authentication Protocol	None, MD5, SHA1	SHA1	
Data Privacy Protocol	None, DES, AES (128 Bit)	AES (128 Bit)	

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 TFTP Access (Read-Only)	Check/Clear	Check	
Allow ICMP Configuration	Check/Clear	Check	
Reject Expired Certificates	Check/Clear	Clear	

Passwords Menu Defaults

Parameter Name	Range	Default	Your Site?
Use RADIUS for Login Authorization	Check/Clear	Clear	
User Name	1 to 32 characters (Not case sensitive)	Intermec	
Password	1 to 32 characters (Not case sensitive)	Intermec	
Read Only Password	1 to 32 characters (Not case sensitive)	Intermecread	
Allow Service Password	Check/Clear	Check	

802.11g Radio Security Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable ACL Client Authorization	Check/Clear	Clear	
Enable Alternative Method ACL	Check/Clear	Clear	
ACL RADIUS Client Password (Appears if Enable ACL Client Authorization is enabled)	1 to 32 characters Must match the password configured in the external RADIUS server	wireless	
VLAN	0 to 4093	0 (Disabled)	
Security Level	None, Static WEP, Dynamic WEP/802.1x, WPA/PSK, WPA + 802.1x	None	

802.11g Radio Security Menu Defaults (continued)

Parameter Name	Range	Default	Your Site?
If **Security Level** is **Static WEP**:			
WEP Transmit Key	1, 2, 3, or 4	1	
WEP Key 1 through 4	5 ASCII characters (or hex pairs) to 16 ASCII characters (or hex pairs)	80211	
If **Security Level** is **Dynamic WEP/802.1x**:			
Key Rotation Period	Any number	5	
If **Security Level** is **WPA/PSK**:			
Multicast Encryption Type	TKIP	TKIP	
Pre-shared Key	256 (32 byte) hex value or a 63 ASCII character passphrase	(blank)	
Key Rotation Period	Any number	5	
If **Security Level** is **WPA + 802.1x**:			
Multicast Encryption Type	WEP, TKIP	TKIP	
Key Rotation Period	Any number	5	

RADIUS Server List Menu Defaults

Parameter Name	Range	Default	Your Site?
IP Address/DNS Name	4 nodes, 0 to 255 or DNS name	0.0.0.0	
Secret Key	16 to 32 bytes	(factory default)	
Port	1-65535 Recommended range is 49152-65535	1812	
802.1x	Check/Clear	Clear except Servers 5 and 6	
ACL	Check/Clear	Clear except on Servers 3 and 4	
Login	Check/Clear	Clear except on Servers 1 and 2	

Spanning Tree Security Menu Defaults

Parameter Name	Range	Default	Your Site?
Secure IAPP	Check/Clear	Clear	
If **802.1x security** or **Secure IAPP** is enabled:			
IAPP Secret Key	16 to 32 bytes	(factory default)	
Allow SWAP	Check/Clear	Check	
Allow TLS	Check/Clear	Clear	
Allow TTLS	Check/Clear	Check	
Preferred Protocol	SWAP/TLS/TTLS	TTLS	
User Name	1 to 31 characters	anonymous	
Password	1 to 31 characters	anonymous	
Verify CA Certificate	Check/Clear	Clear	

Embedded Authentication Server Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable Server	Check/Clear	Clear	
If **Enable Server** is enabled:			
Default Secret Key	16 to 32 bytes	(factory default)	
UDP Port	49152-65535	1812	
Authorization Time	hh:dd:mm	0:01:00	

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 gain 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 addresses

An address assigned to hosts using TCP/IP. An IPv4 address belongs to one of five classes (A, B, C, D, E) and is written as *x.x.x.x*, where *x* is a number from 0 to 255. An IPv6 address is 128 bits long and is represented by up to 32 hex digits. The digits are grouped into sets of four, separated by colons. For example, fec0:0000:0000:0000:0210:40ff:fe12:12a6.

In IPv6, leading zeroes in a group can be dropped. Also, if you have one or more groups that are all zeroes, you can replace the zeroes with two colons. You can only do this once. Using the above example, you can shorten it to fec0::210:40ff:fe12:12a6.

However, if the IP address is fec0:0000:0000:1234:0000:4321:abcd:0076, it can only be shortened to fec0::1234:0000:4321:abcd:76 because you can only use the two colons once.

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.

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.

service set

A logical (not physical) radio. You can create up to four service sets for each physical 802.11g radio in an access point. Each service set shares the same physical radio configuration (including the parameters set for Advanced Configuration and Inbound Filters). Each service set has a unique SSID (network name), and you may customize its security configuration and member limit. Multiple service sets are used primarily to allow one radio to support multiple VLANs.

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 WA21G and WA22G 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.

Telnet Gateway

A software feature in Release 2.1 that allows the access point to keep telnet sessions alive even when the wireless client is idle or disconnected for any reason (because the client has roamed out of range, been powered off, lost battery power, etc.).

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.

VLAN (virtual LAN)

A network of wireless end devices that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a local area network. You can group all wireless users on a particular VLAN in order to manage the IP address space differently. Or you can use VLANs to separate secure and non-secure traffic.

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 802.11g radio that allows data encryption for wireless communications. 802.1x security uses WEP encryption.

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.

WPA (Wi-Fi Protected Access)

A feature that can be implemented in the 802.11g, 802.11b, and 802.11a radios for security in a wireless environment. WPA is a strongly enhanced, interoperable Wi-Fi security protocol that addresses many of the vulnerabilities of WEP.

I Index

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 WA2XG System Manual

P/N 074921-002