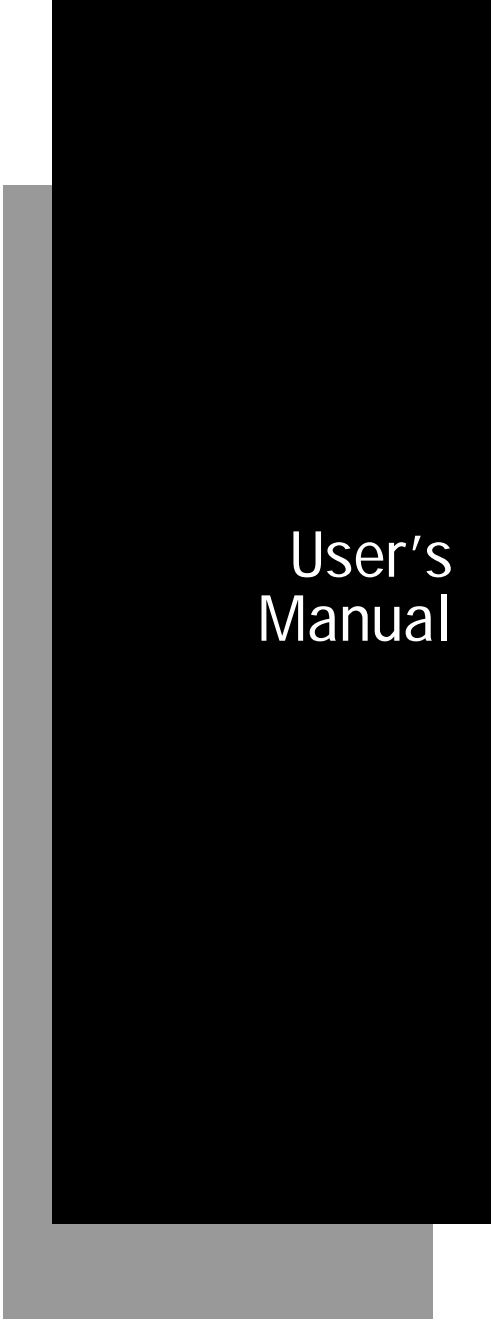


**Intermec**



User's  
Manual



0110/0111/0115  
Access Point

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

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

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

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

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

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

© 1997 by Intermec Technologies Corporation  
All Rights Reserved

The word Intermec, the Intermec logo, JANUS, IRL, TRAKKER, Antares, Adara, Duratherm, EZBuilder, Precision Print, PrintSet, Virtual Wedge, and CrossBar are either trademarks or registered trademarks of Intermec Technologies Corporation.

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.

### *Manual Change Record*

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

Version	Date	Description of Change
002	11/97	Added information about the 0111 Ethernet Access Point and the 0115 Token Ring Access Point to the 0110 Ethernet Access Point User's Manual. Other minor changes were made to reflect the latest firmware.



# Contents

<b>Before You Begin</b>	<b>xii</b>
Warranty Information	xii
Safety Summary	xii
Cautions and Notes	xiii
About This Manual	xiii
Other Related Manuals	xvii

## 1

---

### **Learning About the Access Points**

<b>About the Intermec 0110/0111/0115 Access Points</b>	<b>1-3</b>
<b>Understanding Intermec 2.4 GHz RF Networks</b>	<b>1-5</b>
Using an Access Point in a Simple Wireless Network	1-5
Using Access Points in a Roaming Network	1-8
Token Ring Roaming Scenarios	1-11
Using the Repeating Feature	1-13

## 2

---

### **Installing the Access Point**

<b>Unpacking the Access Point</b>	<b>2-3</b>
<b>System Requirements</b>	<b>2-4</b>
<b>Description</b>	<b>2-5</b>
Understanding the Front Panel LEDs	2-5
Understanding the 0110/0111 Side Panel	2-6
Understanding the 0115 Side Panel	2-7
<b>Understanding the Main Menu</b>	<b>2-8</b>
<b>Performing a Quick Installation</b>	<b>2-9</b>
<b>Performing a Standard Installation</b>	<b>2-10</b>
Deciding How You Will Configure the Access Point	2-10
Attaching an Antenna	2-11
Mounting the Access Point	2-12
Connecting to the Wired Network	2-12
Ethernet	2-12
Token Ring	2-13
Plugging in the Power Supply	2-13
Configuring the Access Point	2-14

*Guidelines for Configuring Intermec 2.4 GHz RF Devices 2-14*  
*Configuring the Access Point Locally (Out-of-Band) 2-15*  
*Configuring the Access Point Remotely (In-Band) Through a Telnet Session 2-15*  
*Configuring the Access Point Remotely Using Modems 2-16*  
*Configuring the Access Point Remotely Using an SNMP Manager 2-17*  
*Configuring the Access Point Remotely Using a Web Browser 2-17*

*Dumping the Configuration to Screen 2-18*

*Resetting the Access Point 2-19*

*Restoring the Access Point to the Default Settings 2-19*

## 3

---

### *Configuring the 0110/0111 Access Point*

*Using the Configuration Menu 3-3*

*Configuring the Access Point 3-4*

*Using the TCP/IP Configuration Menu 3-5*

*Example - Setting the IP Address 3-7*

*Using the Filter Configuration Menu 3-8*

*Using the Bridge Configuration Menu 3-11*

*Using the Radio Configuration Menu 3-12*

*Using the Ethernet Configuration Menu 3-16*

*Setting Security on Access Points 3-17*

*Setting the Security ID 3-17*

*Using the Authorization Table 3-17*

## 4

---

### *Configuring the 0115 Access Point*

*Using the Configuration Menu 4-3*

*Configuring the Access Point 4-4*

*Using the TCP/IP Configuration Menu 4-5*

*Example - Setting the IP Address 4-7*

*Using the Filter Configuration Menu 4-8*

- Using the Bridge Configuration Menu 4-11**
  - About Bridging Modes 4-12
    - Multi-Ring SR/TB Mode 4-12
    - Single-Ring SR/TB Mode 4-13
    - TB Mode 4-14
  - Hardware Filtering Configuration Menu 4-15
  - Frame Mapping Configuration Menu 4-15
- Using the Radio Configuration Menu 4-16**
- Using the Token Ring Configuration Menu 4-20**
- Setting Security on Access Points 4-22**
  - Setting the Security ID 4-22
  - Using the Authorization Table 4-22

## 5

---

### **Using an SNMP Manager or a Web Browser**

- Configuring the Access Point Using an SNMP Manager 5-3**
  - Using the SNMP Configuration Menu 5-3
  - SNMP Supported Traps 5-8
    - MIB II Traps 5-8
    - Enterprise Specific Traps 5-8
- Configuring the Access Point Using a Web Browser 5-9**
  - Understanding the Main Screen 5-9
  - Understanding the Network Management Options 5-10
  - Understanding the Device Management Options 5-10

## 6

---

### **Maintaining and Troubleshooting the Access Point**

- Viewing the Access Point Statistics 6-3**
  - Radio Statistics (Ethernet and Token Ring) 6-6
  - Bridge Statistics (Ethernet and Token Ring) 6-6
  - Filter Statistics (Ethernet and Token Ring) 6-6
  - Reset Statistics (Ethernet and Token Ring) 6-6
  - TCP/IP Statistics (Ethernet) 6-6
  - Ethernet Statistics 6-6
  - Token Ring Statistics 6-6
  - Source Route Statistics Menu (Token Ring) 6-7
- Viewing the Access Point Parameters 6-7**
  - Radio Status Menu (Ethernet and Token Ring) 6-9
  - Bridge Status Menu (Ethernet and Token Ring) 6-9

*Forwarding Database Table (Ethernet and Token Ring) 6-10*

*Token Ring Status Menu 6-10*

*TCP/IP Status Menu (Token Ring) 6-10*

*Source Route Table (Token Ring) 6-11*

***Increasing Wireless Network Performance 6-11***

*Microwave Ovens 6-11*

*Transmission Range 6-11*

***How to Obtain Help With Your Installation 6-12***

*Diagnostics Menu 6-12*

*Commonly Asked Technical Support Questions 6-14*

---

**A**

***Specifications***

*General Specifications A-3*

*Physical Specifications A-3*

*Other Specifications A-4*

---

**B**

***Using the Site Survey Tools and the Antenna Pointing Tool***

*Using the Radio Diagnostics Menu B-3*

*Running a Broadcast Site Survey B-3*

*Link Quality B-4*

*RSSI B-4*

*Running a Directed Site Survey B-4*

*Using the Antenna Pointing Tool B-6*

---

**C**

***Upgrading the Access Points***

*Using the Download Menu C-3*

*Upgrading One Access Point C-4*

*Upgrading Multiple Access Points C-4*

*Disallowing an Access Point From Receiving an Image C-5*

*Viewing the Download Status of the Access Points C-6*



**G**

---

*Glossary*

**I**

---

*Index*





## Before You Begin

---

This section introduces you to standard warranty provisions, safety precautions, cautions, document formatting conventions, and sources of additional product information. A documentation roadmap is also provided to guide you in finding the appropriate information.

---

### *Warranty Information*

To receive a copy of the standard warranty provision for this product, contact your local Intermec support services organization. In the U.S. call 1-800-755-5505, and in Canada call 1-800-688-7043. Otherwise, refer to the Worldwide Sales & Service list that ships with this manual for the address and telephone number of your Intermec sales organization.

---

### *Safety Summary*

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

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

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

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

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

---

## Cautions and Notes

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



### Caution

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

### Conseil

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

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

---

## About This Manual

This manual provides you with information on the features of this product, how to install it, how to configure it, and how to troubleshoot it. You must be familiar with your host PC, your other Intermec equipment, and your network.

### What You Will Find in This Manual

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

For Information On	Refer To
Understanding the access point	Chapter 1, "Learning About the Access Point." Explains how the access point works in an RF network and the access point features. This chapter also provides system requirements.
Installing the access point	Chapter 2, "Installing the Access Point." Explains the quick path and standard path for installing the access point. Also, this chapter summarizes the different ways you can configure the access point.
Configuring the Ethernet access point using the menus	Chapter 3, "Configuring the 0110/0111 Access Point." Explains the parameters you need to configure on the access point and how to use the Configuration Menu options.



**For Information On**

Configuring the token ring access point using the menus

Configuring the access point using an SNMP management package

Configuring the access point using a web browser

Maintaining and troubleshooting the access point

Specifications

Performing Site Surveys

Upgrading access points

**Refer To**

Chapter 4, “Configuring the 0115 Access Point.” Explains the parameters you need to configure on the access point and how to use the Configuration Menu options.

Chapter 5, “Using an SNMP Manager or a Web Browser.” Explains how to configure the parameters using an SNMP management package.

Chapter 5, “Using an SNMP Manager or a Web Browser.” Explains how to configure the parameters using a web browser.

Chapter 6, “Maintaining and Troubleshooting the Access Point.” Explains how to use the Status Menu and Statistics Menu options. Also provides suggestions on improving wireless network performance. Contains answers to frequently asked questions.

Appendix A, “Specifications.” Provides specifications for the access point.

Appendix B, “Using the Site Survey Tools and the Antenna Pointing Tool.” Explains how to use the access point to monitor RF integrity on your network.

Appendix C, “Upgrading the Access Points.” Explains how to upgrade one or more access points.

In addition, this manual contains a glossary and an index.

### *Terminology*

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

Term	Description
access point	Refers to an 0110, 0111, or 0115 Access Point
JANUS device	Refers to a JANUS 2010 hand-held computer, a JANUS 2020 hand-held computer, or a JANUS 2050 vehicle-mount computer that runs in the Intermec 2.4 GHz RF network.
TRAKKER Antares terminal	Refers to any terminal in the TRAKKER Antares family of terminals that runs in the Intermec 2.4 GHz RF network.
data collection device or station	Refers to any of the JANUS or TRAKKER Antares family of products that run in the Intermec 2.4 GHz RF network.
wired network	Refers to the Ethernet or token ring network.

### *Format Conventions for Input From a Keyboard or Keypad*

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

Convention	How to Interpret the Convention
Special text	Shows the command as you should enter it into the device. See "Format Conventions for Commands" later in this section.
<i>Italic text</i>	Indicates that you must replace the parameter with a value. See "Format Conventions for Commands" later in this section.
<b>Bold text</b>	Indicates the keys you must press on a PC keyboard. For example, "press <b>Enter</b> " means you press the key labeled "Enter" on the PC keyboard.

### *Format Conventions for Commands*

This manual includes sample commands that are shown exactly as you should type them on your device. The manual also describes the syntax for many commands, defining each parameter in the command. This example illustrates the format conventions used for commands:




When you use the LOADADD command, follow this syntax:

```
loadadd [path\]filename [path\filename path\filename...]
```

where:

*path* is the drive and directory of the file(s) to include in the image file. If you do not include a *path*, the current directory is used.

*filename* is the name of the file or files to include in the image file and load to the device.

You can include multiple *path\filename* and *path\\*.\** parameters in the command. The *path\\*.\** parameter loads all the files in a directory. For example, type this command at the DOS prompt and press :

```
loadadd c:\janus\config.sys c:\atadriv\*. * c:\data\*. *
```

This table defines the conventions used in the example:

Convention	Description
Special font	Commands appear in this font. You enter the command exactly as it is shown.
<i>Italic text</i>	Italics indicate a variable, which you must replace with a real value, such as a number, filename, or keyword.
[ ]	Brackets enclose a parameter that you may omit from the command. Do not include the brackets in the command.
Required parameters	If a parameter is not enclosed in brackets [ ], the parameter is required. You must include the parameter in the command; otherwise, the command will not execute correctly.
where	This word introduces a list of the command's parameters and explains the values you can specify for them.

---

## *Other Related Manuals*

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

<b>Intermec Manuals</b>	<b>Intermec Part No.</b>
<i>Model 200 Controller System Manual</i>	063439
<i>Model 200 Controller Technical Reference Manual</i>	064398
<i>TRAKKER® Antares™ 2420 and 2425 Hand-Held Terminal User's Manual</i>	064024
<i>JANUS™ 2010 Hand-Held Computer User's Manual (4MB)</i>	065714
<i>JANUS™ 2020 Hand-Held Computer User's Manual (4MB)</i>	065715
<i>JANUS™ 2050 Vehicle-Mount Computer User's Manual (4MB)</i>	065716
<i>2070 and 2075 Pen-Based Computer User's Manual</i>	065144
<i>JANUS™ 2.4 GHz Install Kit (4MB)</i>	064672
<b>Other Manuals</b>	
<i>NetWare Administrator's Guide</i>	



# 1

## *Learning About the Access Point*



*This chapter explains the features of the access points and some basic concepts about your wireless network.*

## *About the Intermec 0110/0111/0115 Access Points*

---

The Intermec access points are long-range, high-performance local area network (LAN) products that bridge Intermec's 2.4 GHz radio frequency (RF) network and your wired (Ethernet or token ring) network. The access points operate at the Data Link level (layer 2) of the OSI model, providing protocol-independent access for other Intermec 2.4 GHz RF devices, such as TRAKKER® Antares™ RF terminals, into your existing wired network.

The access points are designed to be a “plug-and-play” product. In many cases, you will not need to run any software to configure it. If you need to configure the access point, you will find the software easy to use.

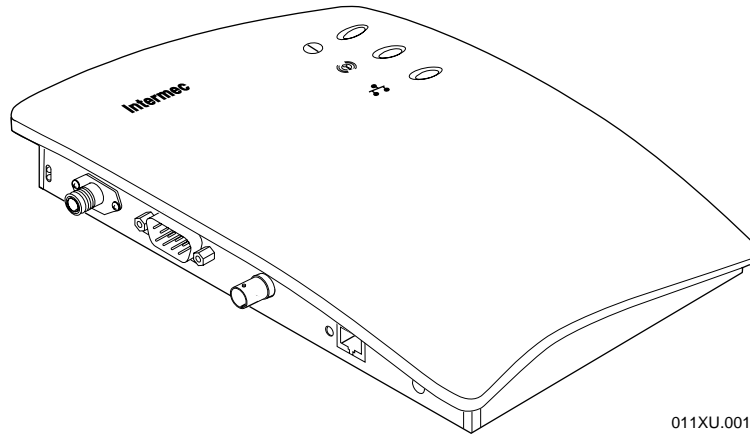
The access points are:

- small, lightweight, mountable
- capable of filtering packets at full Ethernet or token ring speeds
- configurable locally and remotely
- SNMP manageable
- Web browser manageable
- a site survey tool
- capable of locating other access points
- capable of downloading new firmware (images) to other access points.

The 0110/0111 Access Points connect to an Ethernet network. The 0110 contains a WLI Forum OpenAir™ 2.4 GHz FHSS radio that has a power output of 100mW. The 0111 contains the same type of radio, but it has a power output of 500mW.

---

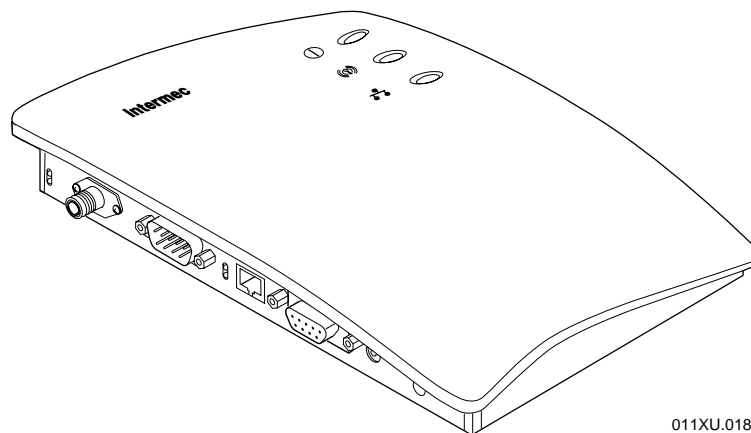
**0110/0111 Access Point**



The 0115 Access Point connects to a token ring network. The 0115 contains a WLI Forum OpenAir 2.4 GHz FHSS radio that has a power output of 100mW or 500mW, depending on the specific country RF regulations.

---

**0115 Access Point**



## *Understanding Intermec 2.4 GHz RF Networks*

---

This section explains how your 0110/0111/0115 Access Point connects your wired network with Intermec's 2.4 GHz RF network. Since the wireless devices operate similar to wired products, all of your existing applications that operate over Ethernet or token ring will work with the wireless network without any special wireless networking software.

---

### *Using an Access Point in a Simple Wireless Network*

With wireless networks, data collection devices easily communicate when they are in range of each other. JANUS devices can dynamically connect and reconnect with each other using off-the-shelf peer-to-peer network operating systems.

**JANUS TCP/IP devices** Use Intermec's JANUS 2.4 GHz Install Utility if you want these JANUS devices to communicate with a host using a standard TCP/IP application; using Intermec TNVT, ANSI, TN3270, or TN5250 terminal emulation; or using Novell TNVT or ANSI terminal emulation.

**TRAKKER Antares TCP/IP terminals** These terminals can communicate to a host using a standard TCP/IP application or Intermec TNVT or ANSI terminal emulation.

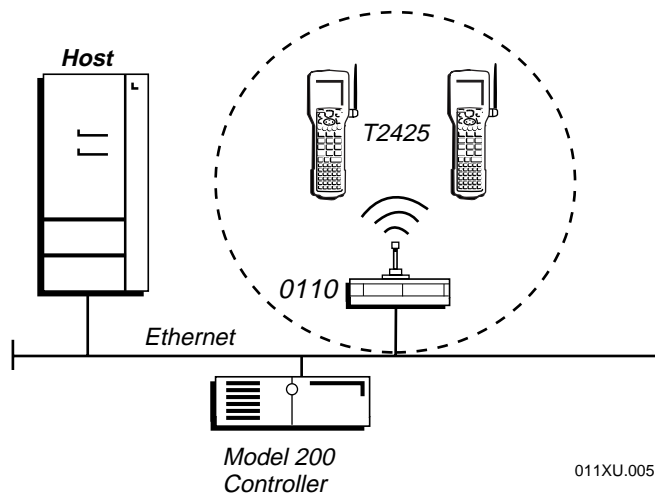
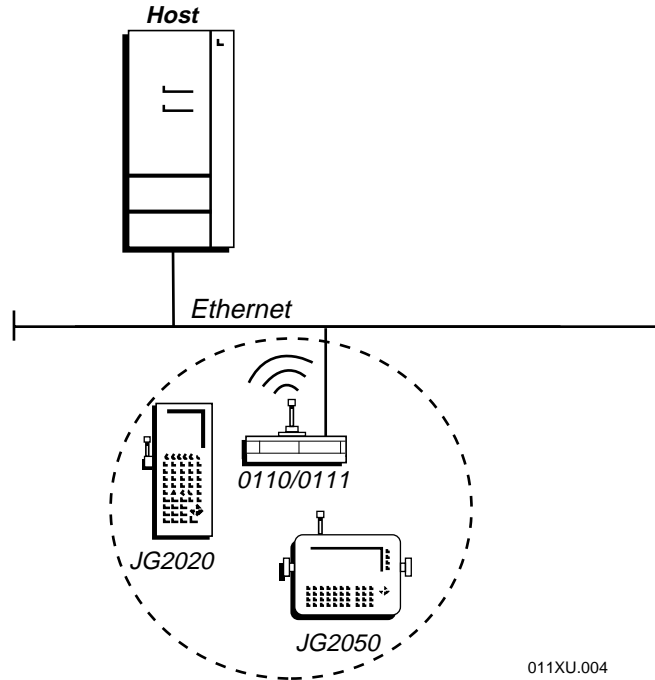
**JANUS UDP Plus devices** Use Intermec's JANUS 2.4 GHz Install Utility if you want these JANUS devices to communicate to a host using standard VT, ANSI, 3270, or 5250 terminal emulation or screen mapping. The access point routes packets from the terminal to the Model 200 Controller, which routes the packets on to the host.

**TRAKKER Antares UDP Plus terminals** These terminals can communicate with the host using standard VT, ANSI, 3270, or 5250 terminal emulation or screen mapping. The access point routes packets from the terminal to the Model 200 Controller, which routes the packets on to the host.

Many companies have an existing Ethernet or another wired network and want to be able to extend that capability to wireless nodes. Use the 0110/0111 Access Point to connect your Ethernet network to an Intermec 2.4 GHz RF network.

---

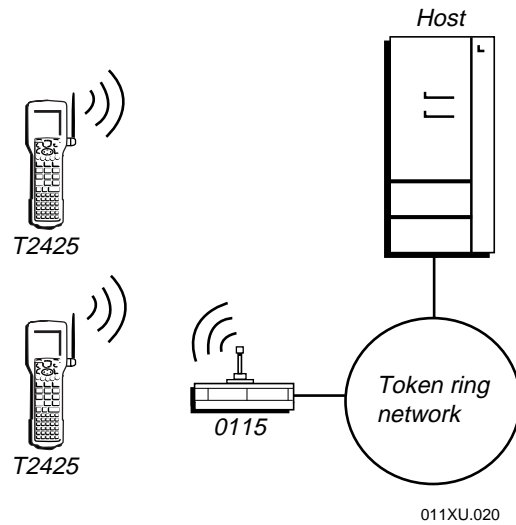
*Two Simple Wireless Networks Connecting to an Ethernet Network*



Many companies have an existing token ring or wired LAN infrastructure and want to be able to extend that capability to wireless nodes. Use the 0115 Access Point to connect your token ring network to an Intermec 2.4 GHz RF network. In the following illustration, the token ring network is autonomous. All systems are connected to this ring.

---

### *A Simple Wireless Network Connected to a Token Ring Network*



---

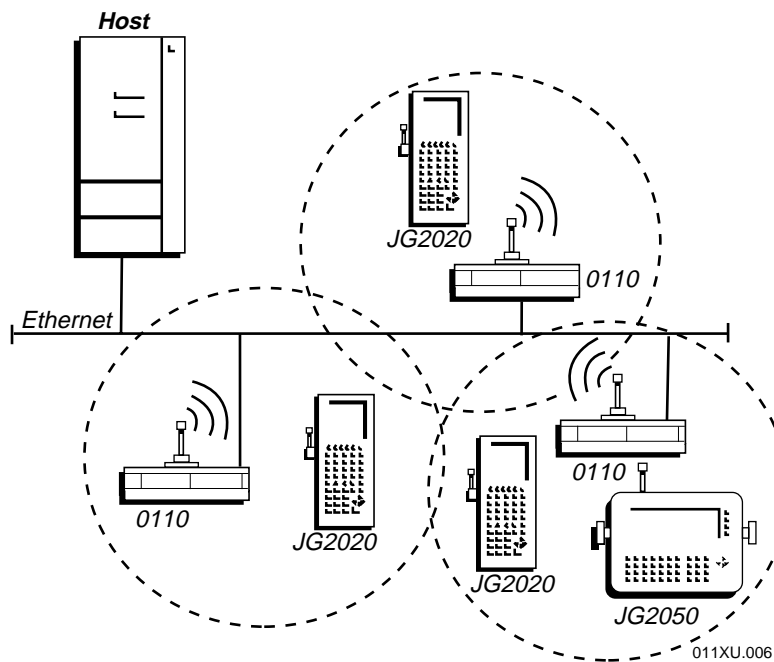
## Using Access Points in a Roaming Network

For larger or more complex environments, you install access points so that data collection devices can roam from one access point to another while maintaining the same network connection. Access points establish coverage areas or cells similar in concept to those of a cellular phone network. Intermec data collection devices can connect with any access point that is within range.

Each access point within a roaming network must be configured as a master with a unique channel/subchannel pair, but all access points must have the same domain and security ID. The roaming clients also must be configured to use the same domain and security ID. As the roaming client *seamlessly* switches from cell to cell, its network connectivity is preserved. When the roaming client leaves the transmission range of one access point, the software automatically polls the other access points in the same domain to continue the network connection.

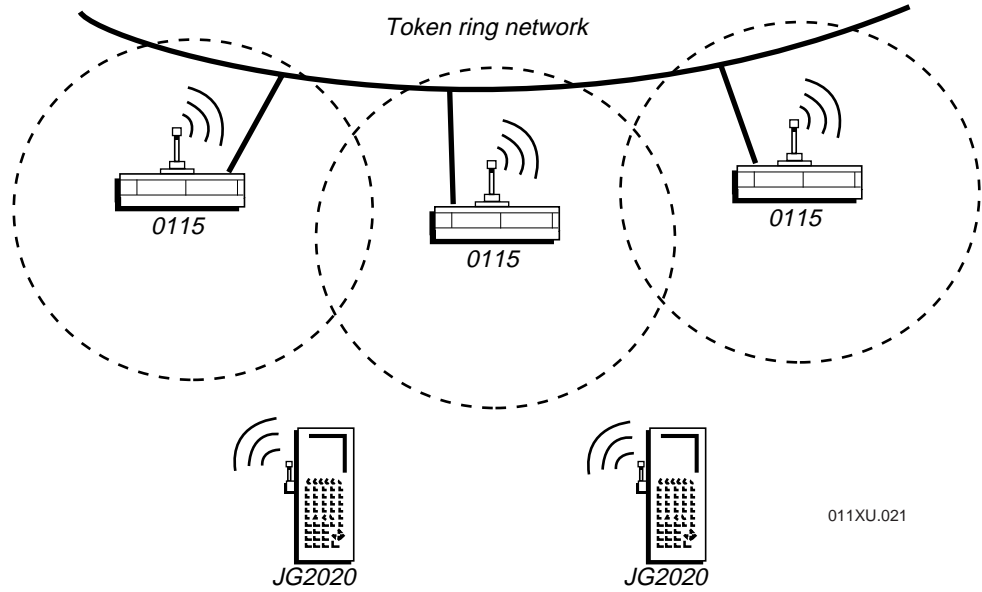
---

### A More Complex Wireless Network Connected to an Ethernet Network





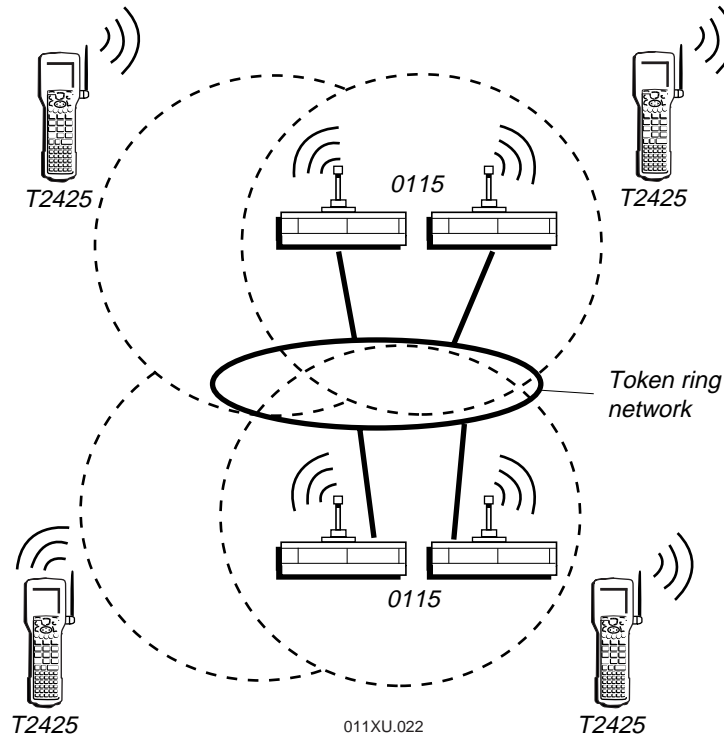
A More Complex Wireless Network Connected to a Token Ring Network



With the access points' multichannel architecture, you can have more than one access point in the same cell area to increase the aggregate throughput supported by the network. In addition, the overlapping cells offer redundancy of coverage that you may require in networks where downtime is not tolerated.

---

**An Overlapping Wireless Network Connected to a Token Ring Network**



---

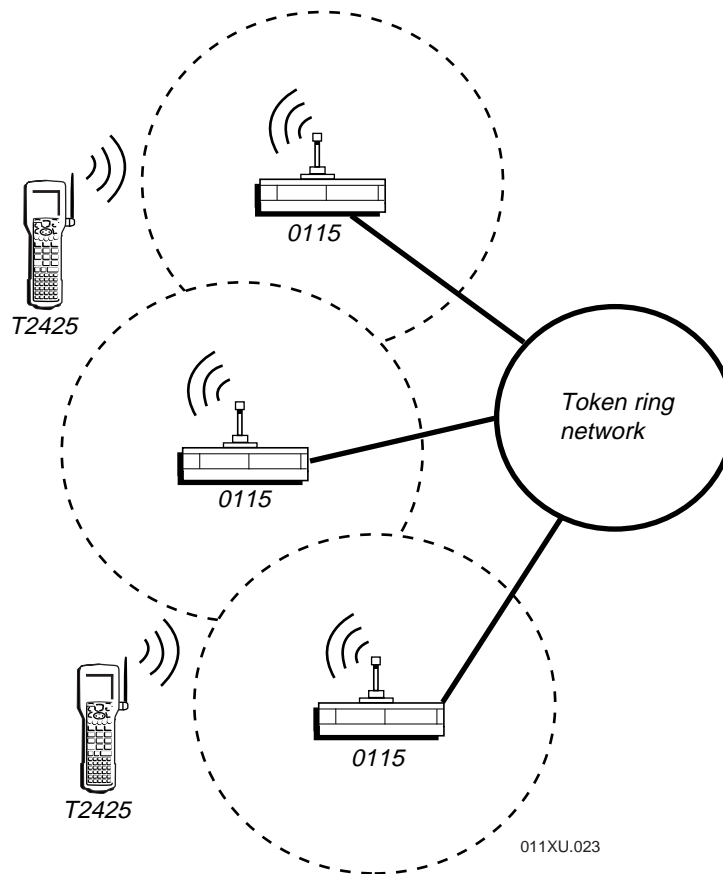
## Token Ring Roaming Scenarios

These roaming scenarios are supported by the 0115 Access Point:

- Roaming among access points located on the same ring.
- Roaming among access points located on different rings, separated by Source-Route Bridges or Transparent Bridges.

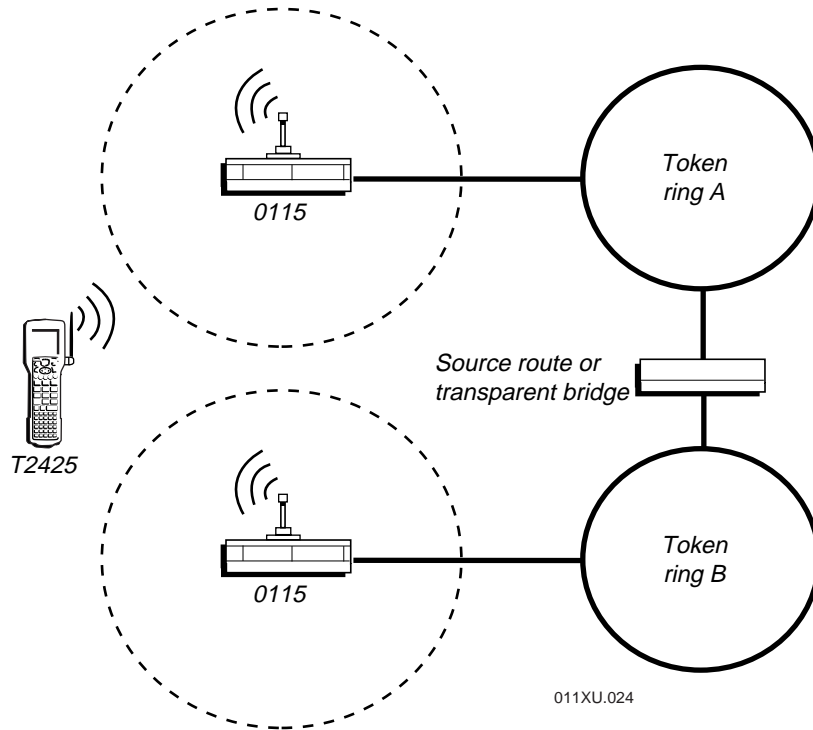
---

### Roaming Among Access Points on the Same Ring



---

Roaming Among Access Points on Different Rings



**Note:** If you want to roam among access points that are separated by IP or IPX routers, you need to use a roaming protocol, such as Mobile IP or Mobile IPX.

**Note:** You cannot roam between 0115 Access Points and 0110/0111 Access Points.

---

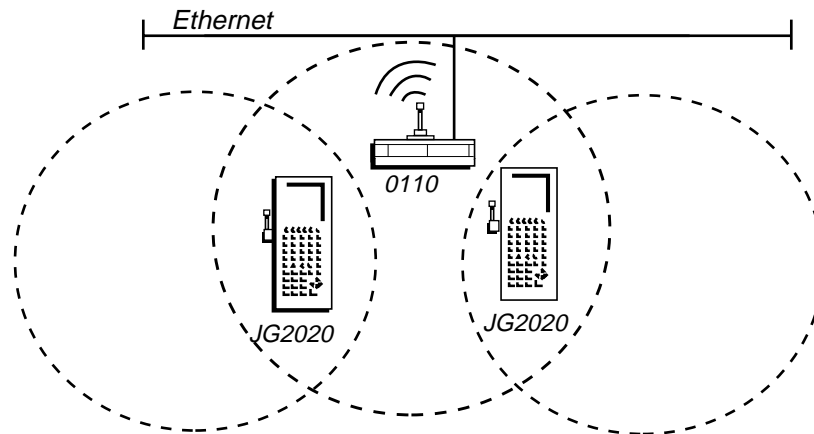
## Using the Repeating Feature

**Note:** Currently, you cannot use the access point as a wireless repeater. That is, the access point must always be connected to the wired network.

You can enable or disable the repeating feature on 0110/0111/0115 Access Points. If you enable this feature, the access point can forward (repeat) packets that are sent to it from a data collection device to another device when the data collection devices are not within range of each other, thereby doubling the effective range of your wireless network. However, the disadvantage of this feature is that network throughput can drop by as much as half.

The repeating feature differs from two data collection devices communicating in a peer-to-peer network. When two devices communicate peer-to-peer, they both have a peer-to-peer protocol loaded and they establish a connection with each other.

If you disable the repeating feature, the access point will not forward packets to data collection devices unless the devices are communicating peer-to-peer. By default, repeating is disabled.



011XU.010



# 2

## *Installing the Access Point*





*This chapter describes the access point and explains how to install the access point using a quick path and the standard path.*

## *Unpacking the Access Point*

---

When you receive your Intermec 0110/0111/0115 Access Point, you need to verify the contents of the package. Each package comes with:

- 0110 Access Point, 0111 Access Point, or 0115 Access Point
- antenna
- (0110/0111) Ethernet “T” connector
- *0110/0111/0115 Access Point Manual Supplement*

If any of these items are missing or damaged, please contact your local Intermec representative. You may need to take the following steps to correct the problem.

- Take photographs, if necessary.
- Contact the transport carrier.

**Note:** *You are responsible for all damage claims against the carrier. See the “Intermec Terms of Sale” printed on your sales invoice.*

## System Requirements

---

Before you can install and configure your 0110/0111/0115 Access Point, you need the following minimum system requirements:

- (0110/0111) An Ethernet cable drop (10BaseT or 10Base2) with the appropriate Ethernet cable  
(0115) A token ring cable drop (UTP or STP) with the appropriate token ring cable
- A terminal or a PC that is running a terminal emulation program, an empty serial port on the terminal or PC, and a null modem cable  
Or, a PC that is running a Telnet (TCP/IP) client on the wired network
- (Optional) To ensure that you have a wireless connection, you need at least one other Intermec data collection device installed on the Intermec 2.4 GHz RF network.

For your access point, you may need:

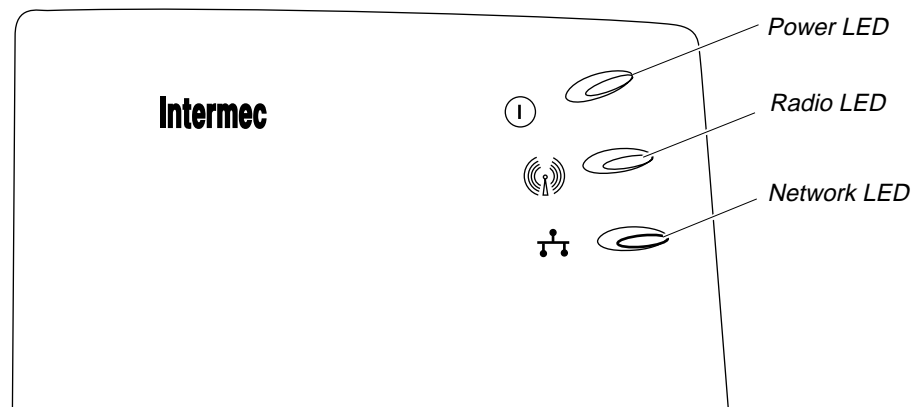
- Mounting options  
Environmental box for an external antenna (P/N 065089)  
Environmental box for the standard antenna (P/N 065096)  
Cubical-mount bracket (P/N 065235)  
Wall-mount bracket (P/N 065236)
- Special power cord - Intermec sells many international power cords. If you need a special power cord for your access point, contact your local Intermec representative.
- Special antennas - Intermec sells many antenna options. If you need a special antenna for your wireless network, contact your local Intermec representative.
- Other accessories - Intermec sells other accessories such as lightning arresters and amplifiers. If you would like to know more about these accessories, contact your local Intermec representative.

## Description

The 0110/111/0115 Access Point has three front panel LEDs and some side panel connectors and LEDs. This section describes these LEDs and connectors.

### Understanding the Front Panel LEDs

There are three LEDs on the front of the access point.

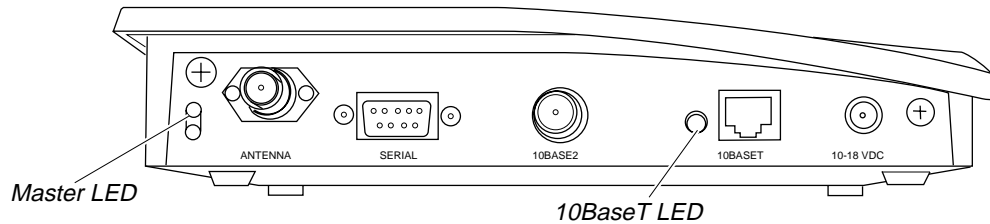


011XU.007

LED	Color	State	Description
Power LED	Tricolor	Orange	Running power-on diagnostics
		Green	OK, ready to transmit
		Red	Diagnostics failed, hardware problem
Radio LED	Orange	Flashing	Transmitting over RF network
Network LED	Green	Flashing	Transmitting over wired network

## Understanding the 0110/0111 Side Panel

The side panel of the access point contains several connectors and LEDs.

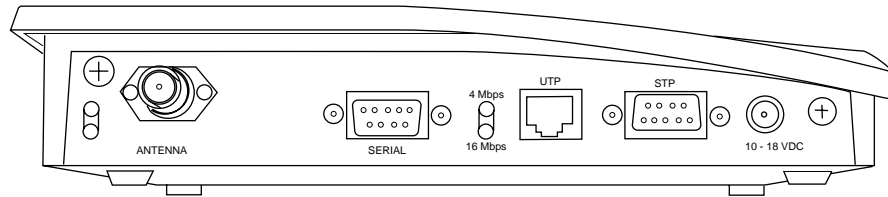


011XU.008

LED	Color	State	Description
Master LED	Green	Steady on	Access point is configured as a master.
		Off	Access point is not configured as a master. It may be configured as a station.
Other LED	Green	Off	Reserved for future functionality.
10BaseT LED	Green	Steady on	Access point has a 10BaseT cable plugged into its connector.
		Off	Access point does not have a 10BaseT cable plugged in or is connected to a 10Base2 cable.

## Understanding the 0115 Side Panel

The side panel of the 0115 Access Point contains several connectors and LEDs.



011XU.014

LED	Color	State	Description
Master LED	Green	Steady on	Access point is configured as a master.
		Off	Access point is not configured as a master. It may be configured as a station.
Other LED	Green	Off	Reserved for future functionality.
4 Mbps LED	Green	Steady on	Access point ring speed is 4 Mbps.
16 Mbps LED	Yellow	Steady on	Access point ring speed is 16 Mbps.

## Understanding the Main Menu

---

If you choose to configure the 0110/0111/0115 Access Point locally, remotely using a Telnet session, or remotely using modems, you will see the Main Menu.

```
                                Main Menu
Selection      Description
-----
1              Configuration Menu
2              Statistics Menu
3              Status Menu
4              Download Menu
5              Diagnostics Menu
6              Reset Ethernet Access Point

Enter a selection number or <ESC> for previous menu -> 1
```

**Note:** Depending on the model of the access point, the descriptions in this menu may be slightly different.

**Note:** Depending on the current settings of the access point, the descriptions in the menus may be slightly different.

Menu	Where to Find an Explanation
Configuration Menu (Ethernet)	See Chapter 3, "Configuring the 0110/0111 Access Point."
Configuration Menu (token ring)	See Chapter 4, "Configuring the 0115 Access Point."
Statistics Menu	See Chapter 6, "Maintaining and Troubleshooting the Access Point."
Status Menu	See Chapter 6, "Maintaining and Troubleshooting the Access Point."
Download Menu	See Appendix C, "Upgrading the Access Points."
Diagnostics Menu	See Chapter 6, "Maintaining and Troubleshooting the Access Point."
Reset Access Point	See "Resetting the Access Point" later in this chapter.

## Performing a Quick Installation

---

You may follow the quick installation procedure to install your 0110/0111/0115 Access Point if ALL of the following conditions are true:

- There will only be one access point on this network.
- You will use all the default values.
- You will not be managing the access point remotely through a Telnet session and therefore, you do not need to assign it an IP address.
- You will not be setting a security ID on your wireless network.
- (0115) Your token ring network operates at 16 Mbps.
- (0115) Your token ring network uses transparent bridging.

If any of the above conditions are not true, see “Performing a Standard Installation” later in this chapter.



### Caution

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

### Conseil

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



### Caution

***Make sure all components with antennas are at least 10 feet (3 meters) apart when power is applied. Failure to comply could result in equipment damage.***

### Conseil

***Assurez-vous que la distance entre tous les éléments avec antennes soit d'au moins dix pieds (3 mètres) avant de faire la connexion avec l'alimentation électrique, faute de quoi vous risquez d'endommager votre installation.***

To use the quick installation procedure

1. Using a clockwise motion, firmly screw the antenna onto the antenna connector on the side panel of the access point.
2. Mount the access point using an environmental box or mounting bracket.
3. (0110/0111) Attach an Ethernet cable to the appropriate Ethernet port (10Base2 or 10BaseT) on the side panel of the access point.  
(0115) Attach a token ring cable to the appropriate token ring port (STP or UTP) on the side panel of the access point.
4. Plug one end of the power supply cable into the 10-18 VDC port on the side panel of the access point and the other end into an AC power outlet. Since there is no On/Off switch, the access point turns on as soon as power is applied.

You are ready to begin using your access point to send packets from the Intermec 2.4 GHz RF network to your wired network.

## *Performing a Standard Installation*

---

1. Decide how you will configure the access point.
2. Attach the antenna.
3. Mount the access point.
4. Connect the access point to the wired network.
5. Plug in the power supply.
6. Configure the access point.

---

### *Deciding How You Will Configure the Access Point*

There are five methods you can use to configure the access point. You can configure the access point:

- Locally using a null modem cable that connects the access point to a terminal or a PC that is running a terminal emulation program.
- Remotely using a PC that is running a Telnet (TCP/IP) client on the wired network.
- Remotely using modems.
- Remotely using an SNMP manager.
- Remotely using a Web browser



If you decide to configure the access point locally, you will need to configure it before you mount it.

If you decide to configure the access point remotely using a Telnet session, first you will need to set the IP address locally. Or, you can enable the access point to request its IP address from a BOOTP server and supply the address of the server. Then, you can mount the access point and configure it.

---

## Attaching an Antenna

The 0110/0111/0115 Access Point is shipped with a standard directly-connected antenna. Intermec sells several different antennas, including higher gain and directional antennas. Each of these antennas ships with installation and mounting instructions. For information on additional antenna options, contact your local Intermec representative.



### Caution

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

### Conseil

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



### Caution

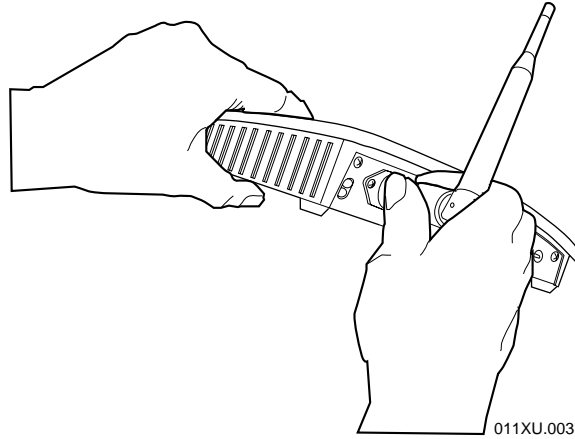
***Make sure all components with antennas are at least 10 feet (3 meters) apart when power is applied. Failure to comply could result in equipment damage.***

### Conseil

***Assurez-vous que la distance entre tous les éléments avec antennes soit d'au moins dix pieds (3 mètres) avant de faire la connexion avec l'alimentation électrique, faute de quoi vous risquez d'endommager votre installation.***

**To install the antenna**

- Using a clockwise motion, firmly screw the antenna onto the antenna connector on the side panel of the access point.



---

## *Mounting the Access Point*

The 0110/0111/0115 Access Point was designed to sit on a flat surface. Intermec offers accessories that let you place the access point in an environmental box, mount the access point to a cubicle, or mount it to a wall.

For more information, see the instruction sheet that came with your box or bracket.

---

## *Connecting to the Wired Network*

You connect your 0110/0111 Access Point to the Ethernet network and you connect the 0115 Access Point to the token ring network.

### *Ethernet*

The 0110/0111 Access Point is connected to the Ethernet network using 10BaseT cabling or 10Base2 cabling.

### *Using 10BaseT Cabling*

The 10BaseT cable typically connects the access point to a 10BaseT hub or wiring rack. Use the same cable that would otherwise be plugged into a 10BaseT workstation on the Ethernet network. If you are using a good cable, on the side panel the green LED nearest the connector will light.

Standard 10BaseT specifications apply to the 10BaseT interface of the access point. No segment can exceed 328 feet (100 meters).

### *Using 10Base2 Cabling*

When using 10Base2 cabling with the access point, you must properly terminate the cable on each end.

Standard 10Base2 specifications apply to the 10Base2 interface of the access point. Each coaxial cable segment can support up to 30 devices and the cable itself cannot exceed 607 feet (185 meters).

### *Token Ring*

The 0115 Access Point is connected to the token ring network using an STP cable or a UTP cable.

**Note:** *If the adapter cable does not connect the access point to the token ring network when the access point is powered on, you will need to perform an Open Token Ring Adapter from the Token Ring Configuration Menu. Otherwise, the access point will not work.*

### *Unshielded Twisted Pair (UTP) Cabling*

The UTP cable is typically connected between the access point and a MAU. If you are using a good cable and the access point is in the ring, one of the LEDs (4 Mbps/16 Mbps) nearest the connector will light.

### *Shielded Twisted Pair (STP) Cabling*

The STP cable is typically connected between the access point and a MAU. If you are using a good cable and the access point is in the ring, the one of the LEDs (4 Mbps/16 Mbps) nearest the connector will light.

---

## *Plugging in the Power Supply*

Attach the power supply in the cable into the 10-18 VDC port on the side panel of the access point and the other end into an AC power outlet. Since there is no On/Off switch, the access point turns on as soon as power is applied. The Power LED on the front panel lights.

---

## *Configuring the Access Point*

This section provides guidelines on setting up the 0110 Access Point so that you can configure it. For help on the configuration parameters, see Chapter 3, "Configuring the 0110/0111 Access Point" or Chapter 4, "Configuring the 0115 Access Point" or Chapter 5, "Using an SNMP Manager or a Web Browser."

### *Guidelines for Configuring Intermec 2.4 GHz RF Devices*

- All access points are masters.
- All data collection devices that communicate with the access points are stations.
- Each access point must have a unique channel/subchannel pair. If possible, each access point should have a unique channel. Use the subchannel parameter only when you have more than 15 access points (you have used all 15 channels) in the same coverage area.
- All access points and data collection devices in the same roaming network must have the same domain and security ID. Security ID is an optional parameter.
- For roaming networks, overlap the transmission ranges of the access points.

*Note: You can set up another roaming network in the same area by configuring another set of access points and data collection devices with a new domain and security ID.*

- To get roaming to occur across routers, use a roaming protocol like Mobile IP or Mobile IPX.
- Roaming will not occur between 0115 Access Points and 0110/0111 Access Points.

### *Configuring the Access Point Locally (Out-of-Band)*

To configure the access point locally, you need to use a null modem cable to connect the access point to an empty serial port on your terminal or PC. This RS-232 cable must have a 9-pin socket connector to connect to the DB-9 serial port on the access point on one side and whatever your terminal or PC requires on the other side. Intermec offers a 9F to 25M null modem 3-wire RS232 cable (P/N 047569).

If you choose to configure the access point using a PC, the PC must have a terminal emulation program running.

**Note:** *If you use a terminal emulation program that has the option to check for the CD signal before establishing a connection, configure the program to ignore CD. Or, verify that your null modem cable is a full handshake cable and pulls CD high. Intermec offers a JANUS Interlnk/Intrsvr cable (P/N 059167).*

#### To locally configure your access point

1. Unplug the access point. The Power LED is not lit.
2. Use the null modem cable to connect the serial port on the side panel of the access point to an empty serial port on your terminal or your PC.
3. Configure the terminal or terminal emulation program for a baud rate of 9600 bps, no parity, 8 data bits, and 1 stop bit.

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

4. Plug in the access point. The Power LED lights. While the access point is booting, messages appear on the your terminal or your PC screen. When the access point is done booting, an “Initialization Complete” message appears.
5. On the terminal or PC, press **Enter**.

You will enter the Main Menu. For help, see Chapter 3, “Configuring the 0110/0111 Access Point” or Chapter 4, “Configuring the 0115 Access Point.”

### *Configuring the Access Point Remotely (In-Band) Through a Telnet Session*

To configure the access point remotely through a Telnet session across the wired network, you must first set the access point IP address locally. Or, you can enable the access point to request its IP address from a BOOTP server and supply the address of the server. To set the IP address locally, see the previous procedure, “Configuring the Access Point Locally (Out-of-Band).” The access point does not ship with a default IP address.

**To configure the access point remotely through a Telnet session**

1. From a terminal or a PC that is running a Telnet (TCP/IP) client on the wired network, open a Telnet session on the access point.
2. If you enabled the feature that limits Telnet access by using a password (in the TCP/IP Configuration Menu), you are prompted for a password. Enter the password.

You will enter the Main Menu. For help, see Chapter 3, "Configuring the 0110/0111 Access Point" or Chapter 4, "Configuring the 0115 Access Point."

*Configuring the Access Point Remotely Using Modems*

To configure your access point using modems, you need to connect one modem to your terminal or your PC and you need to use a straight-through cable to connect another modem to the access point.

**To configure the access point using modems**

1. Attach a modem to your terminal or your PC.
2. Using the terminal or terminal emulation program, configure the modem to communicate at a baud rate of 9600 bps.
3. From the terminal or terminal emulation program, send these commands to the modem:  

```
ATS0=1      (Auto-answer after 1 ring)
AT&D0       (Ignore DTR)
ATE0        (No local echo)
ATQ1        (Suppress result codes)
AT&W0       (Store configuration in non-volatile memory)
```
4. Attach a modem using a straight-through cable to your access point.
5. From the modem connected to your terminal or PC, dial the phone number of the modem connected to the access point.
6. After the access point's modem has answered, press **Enter**.

You will see the Main Menu. For help, see Chapter 3, "Configuring the 0110/0111 Access Point" or Chapter 4, "Configuring the 0115 Access Point."

*Configuring the Access Point Remotely Using an SNMP Manager*

1. From an SNMP manager on your wired network, open an SNMP session on the access point.
2. Modify the access point parameters.

For help, see Chapter 5, “Using an SNMP Manager or a Web Browser.”

*Configuring the Access Point Remotely Using a Web Browser*

1. Start a supported web browser on your PC. This PC must be connected to the network either using a wired or wireless connection.
2. Replace the URL path with the IP address of the access point. The browser displays the Intermecc screen for the Access Point Web Manager.
3. If you set a browser user name and a browser user password in the TCP/IP Configuration Menu, you need to enter them before you can enter the Web Manager.
4. Modify the access point parameters.

For help, see Chapter 5, “Using an SNMP Manager or a Web Browser.”

## Dumping the Configuration to Screen

---

When you are finished configuring the 0110/0111/0115 Access Point, you may want to see all of your current parameter settings on the same screen. Also, if you are having problems with your access point, Intermec Technical Support may ask you to use a screen capture program to create a snapshot of this screen and print it out for troubleshooting purposes.

To dump the configuration to screen

1. From the Main Menu, at the prompt type **1** to enter the Configuration Menu and press **Enter**.
2. From the Configuration Menu, type **9** to dump the configuration to screen and press **Enter**.

```
Configuration
TCP/IP Configuration
IP Address                192.9.175.181
Subnet Mask                255.255.255.0
Default Gateway Address    192.9.175.1
Send BOOTP at Boot Time   true
BOOTP Server (0.0.0.0 for Broadcast) 0.0.0.0
Telnet Access              enabled
Filter Configuration
Filter Fixed nodes         filtering
Filter IP Packets          not filtering
Filter IPX Packets         not filtering
Filter NetBEUI Packets    not filtering
Filter AppleTalk Packets  filtering
Filter DECNet Packets     not filtering
Filter Other Packets      not filtering
Filter IPX RIP Broadcast Packets not filtering
Filter IPX SAP Broadcast Packets not filtering
Filter IPX LSP Broadcast Packets not filtering
Filter ARP Broadcast Packets not filtering
ARP Filter Network Address 0.0.0.0
ARP Filter Subnet Mask    0.0.0.0
Broadcast Bandwidth Allocation % 7
Hit any key to continue ...
```

The configuration parameters appear on the screen. The information may be presented page by page. Press any key to continue scrolling through the information.



## Resetting the Access Point

---

This section explains how to reset the 0110/0111/0115 Access Point. Certain parameters, such as TCP/IP parameters, do not take effect until you reset the access point.

To reset the access point

1. From the Main Menu, type **6** and press **Enter**.
2. Type **1** to confirm that you want to reset the access point and press **Enter**.

If you are communicating with the access point through a Telnet session, your connection is terminated and the access point is reset.

**Note:** You can also reset the radio on the access point without resetting the entire unit. For help, see “Using the Radio Configuration Menu” in Chapter 3.

## Restoring the Access Point to the Default Settings

---

**Note:** You can only restore the factory default settings if your access point is connected locally using a null modem cable to a terminal or a PC.

To restore the access point to factory defaults

1. Connect the access point to your terminal or PC using a null modem cable and start the Main Menu. For help see “Configuring the Access Point Locally (Out-of-Band)” earlier in this chapter.
2. From the Main Menu, type **1** and press **Enter**.
3. From the Configuration Menu, type **8** to restore the access point to factory default settings and press **Enter**.
4. Reset the access point for the parameters to take effect. For help, see “Resetting the Access Point” in the previous section.



## *Configuring the 0110/0111 Access Point*



*This chapter explains how to configure the access point using the Configuration Menu.*

## Using the Configuration Menu

---

The Configuration Menu lets you set all the parameters that allow the 0110/0111 Access Point to communicate with your network.

To access the Configuration Menu

- From the Main Menu, type **1** and press **Enter**. The Configuration Menu appears.

Configuration Menu	
Selection	Description
-----	-----
1	TCP/IP Configuration Menu
2	Filter Configuration Menu
3	Bridge Configuration Menu
4	Radio Configuration Menu
5	Ethernet Configuration Menu
6	Authorization Table Configuration Menu
7	SNMP Configuration Menu
8	Reset Access Point to Factory Defaults
9	Dump Configuration To Screen
Enter a selection number or <ESC> for previous menu ->	

From the Configuration Menu, there are several menu options. To access any other menu or to access a parameter in a menu, type the number in the Selection column that corresponds to the menu or parameter you want and press **Enter**.

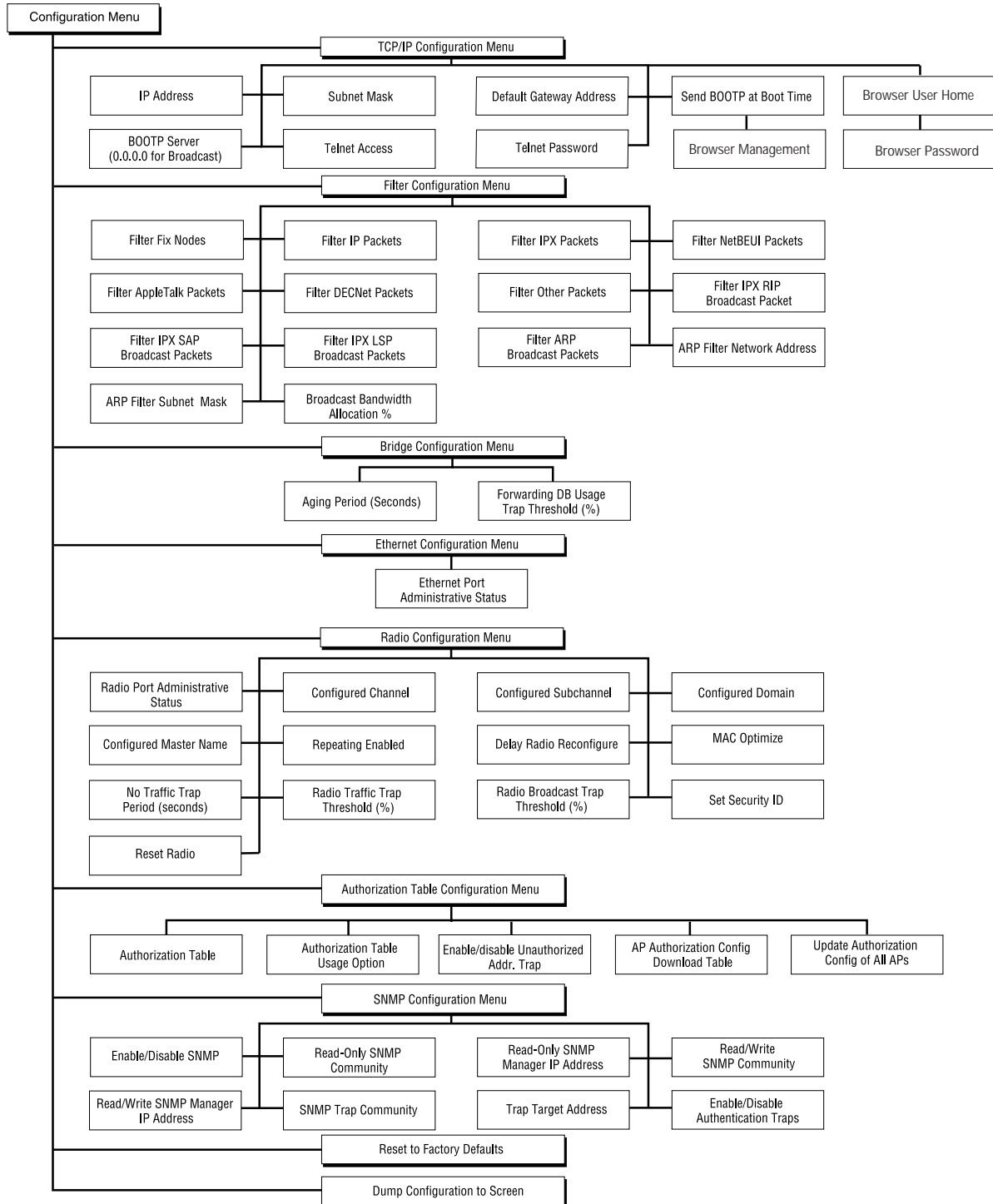
**Note:** *Reset Access Point to Factory Defaults option is only available if you are configuring the access point locally.*

To return to a previous menu

- Press **Esc**.

# Configuring the Access Point

This chart shows all the parameters available in the Configuration Menu.



## Using the TCP/IP Configuration Menu

The TCP/IP Configuration Menu lets you change the TCP/IP parameters of the 0110/0111 Access Point.

To access the TCP/IP Configuration Menu

- From the Configuration Menu, type **1** and press **Enter**. The TCP/IP Configuration Menu appears.

TCP/IP Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	IP Address	0.0.0.0
2	Subnet Mask	0.0.0.0
3	Default Gateway Address	0.0.0.0
4	Send BOOTP at Boot Time	true
5	BOOTP Server (0.0.0.0 for Broadcast)	0.0.0.0
6	Telnet Access	enabled
7	Telnet Password	
8	Browser Management	enabled
9	Browser User Name	
10	Browser Password	

Enter a selection number or <ESC> for previous menu ->

Parameter	Description	Default	Reset Access Point?
IP address	Assign each access point a unique valid IP v4 address.  Or, set the Send BOOTP at boot time parameter to True. This parameter lets the access point to request an IP address from a BOOTP server each time it boots.	0.0.0.0	Yes
Subnet mask	Determines what network the access point is on.	0.0.0.0	Yes

---

**TCP/IP Configuration Parameters**

Parameter	Description	Default	Reset Access Point?
Default gateway address	Set this parameter if you want to route packets to an IP host or node on another IP subnet.  Since access points and devices cannot communicate across subnets, you must provide the IP address of a default gateway. This gateway will route the packets to the proper destination.	0.0.0.0	Yes
Send BOOTP at boot time	Set this parameter if you do not want to assign the access point an IP address. The access point can request an IP address from a BOOTP server each time it boots.  <i>Note: If you are requesting an IP address from a BOOTP server, the MAC address for the access point is on the bottom panel.</i>	True	No
BOOTP server address	If you set the Send BOOTP at boot time parameter to True, you must provide the IP address of that server.	0.0.0.0 (sends a broadcast)	No
Telnet access	Enable this feature if you want a remote user to be able to open a Telnet session to the access point.	Enabled	No
Telnet password	If you set the Telnet access parameter to Enabled, you can provide a password to control access to this feature.	None	No
Browser management	Enable this feature if you want a remote user to be able to use a Web browser to manage the access point.	Enabled	No
Browser user name	If you set the Browser management parameter to Enabled, you can provide a user name and password to control access to this feature.	None	No
Browser password			



### Example - Setting the IP Address

To set an IP address for the access point, you need to connect the access point to your terminal or PC and configure it locally. Or, you can enable the access point to request its IP address from a BOOTP server and supply the address of the server.

#### To set the IP address

1. From the Main Menu, type **1** and press **Enter**. The Configuration Menu appears.
2. From the Configuration Menu type **1** and press **Enter**. The TCP/IP Configuration Menu appears.
3. At the “Enter a selection number or <ESC> for previous menu” prompt, type **1** and press **Enter**. The current IP address parameter is displayed on your screen and its current value next to it.

```
IP Address [0.0.0.0]
Enter a new value ->
```

4. Enter a valid IP v4 address and press **Enter**.

```
IP Address [0.0.0.0]
Enter a new value -> 100.9.8.7
```

The TCP/IP Configuration Menu appears with the new value for the IP address in the Current Value column.

TCP/IP Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	IP Address	100.9.8.7
2	Subnet Mask	0.0.0.0
3	Default Gateway Address	0.0.0.0
4	Send BOOTP at Boot Time	true
5	BOOTP Server (0.0.0.0 for Broadcast)	0.0.0.0
6	Telnet Access	enabled
7	Telnet Password	
8	Browser Management	enabled
9	Browser User Name	
10	Browser Password	

Enter a selection number or <ESC> for previous menu ->

## Using the Filter Configuration Menu

---

The Filter Configuration Menu lets you customize the type of traffic that is forwarded from the Ethernet network to the wireless network. None of these filters affects traffic flow. However, the more filters you turn on, the more bandwidth you save. For most situations, the default filters work.

### To access the Filter Configuration Menu

- From the Configuration Menu, type **2** and press **Enter**. The Filter Configuration Menu appears.

Filter Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Filter Fixed Nodes	filtering
2	Filter Bridge Packets	filtering
3	Filter LAN Manager Packets	filtering
4	Filter IP Packets	not filtering
5	Filter IPX Packets	not filtering
6	Filter NetBEUI Packets	not filtering
7	Filter AppleTalk Packets	filtering
8	Filter Other Packets	not filtering
9	Filter IPX RIP Broadcast Packets	filtering
10	Filter IPX SAP Broadcast Packets	filtering
11	Filter IPX LSP Broadcast Packets	filtering
12	Filter ARP Broadcast Packets	not filtering
13	ARP Filter Network Address	0.0.0.0
14	ARP Filter Subnet Mask	0.0.0.0
15	Broadcast Bandwidth Allocation	% 80

Enter a selection number or <ESC> for previous menu ->

---

**Filter Configuration Parameters**

Parameter	Description	Default
<b>Filter Fixed Nodes</b>	Determines if packets that are destined for a non-broadcast, non-multicast, non-bridge address are forwarded to the wireless network.  Do not enable this filter when using the node address overwrite feature.	Filtering
<b>Filter Bridge Packets</b>	Determines if the access point will forward packets that are sent between access points (bridges) to the wireless network. Bridges periodically exchange packets to discover each other.	Filtering
<b>Filter LAN Manager Packets</b>	Determines if the access point will forward LAN Manager Packets to the wireless network. These packets are destined for LAN Manager stations.	Filtering
<b>Protocol Type Filters</b>	Determines if the access point will forward packets of a particular protocol type to the wireless network.  If you enable Filter other packets, only the protocol types that are listed are forwarded. All other protocol types are filtered.  Do not filter protocol types that your wireless network must receive. For example, if you use TCP/IP on your wireless network, do not filter IP traffic.	
	Filter IP packets	Not filtering
	Filter IPX packets	Not filtering
	Filter NetBEUI packets	Not filtering
	Filter AppleTalk packets	Filtering
	Filter DECNet packets	Not filtering
	Filter other packets	Not filtering

---

**Filter Configuration Parameters**

Parameter	Description	Default
<b>IPX Broadcast Filters</b>	Determines if the access point will forward various IPX packets from the wired network to the wireless network.  You can usually filter all the IPX packets since these packets are of interest to routers and not data collection devices.	
	Filter IPX RIP broadcast packets	Filtering
	Filter IPX SAP broadcast packets	Filtering
	Filter IPX LSP broadcast packets	Filtering
<b>ARP Broadcast Filter</b>	Determines if the access point enables IP ARP broadcast filtering. ARP packets will be forwarded from the wired network to the wireless network only if the destination IP address is on the IP network defined by the ARP filter network address and ARP filter subnet mask.	
	Filter ARP broadcast packets	Not filtering
	ARP filter network address	0.0.0.0
	ARP filter subnet mask	0.0.0.0
<b>Broadcast Bandwidth Allocation (%)</b>	Determines the maximum percentage of the RF bandwidth that may be allocated for broadcast traffic. This feature lets you limit broadcast traffic.  For example, to prioritize directed packets, you may want to reserve radio bandwidth for directed packets by setting this limit to less than 100%.	80

## Using the Bridge Configuration Menu

The Bridge Configuration Menu lets you set parameters for the learned database.

To access the Bridge Configuration Menu

- From the Configuration Menu, type **3** and press **Enter**. The Bridge Configuration Menu appears.

Bridge Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Aging Period (seconds)	300
2	Forwarding DB Usage Trap Threshold (%)	100
Enter a selection number or <ESC> for previous menu ->		

Parameter	Description	Default
Aging period (seconds)	Specifies the amount of time in seconds (10 to 1,000,000) that the learned physical address of the network node is stored in the Forwarding Database (DB). When the aging period expires, this learned physical address is discarded. This data is dynamically acquired by the access point so that it can forward packets properly.	300
Forwarding DB usage trap threshold (%)	Specifies the percentage (0 to 100) of learned database entries after which an SNMP trap will be sent. The Forwarding Database can hold up to 2048 entries.	100

## Using the Radio Configuration Menu

---

The Radio Configuration Menu lets you set the radio parameters for your 0110/0111 Access Point parameters.

To access the Radio Configuration Menu

- From the Configuration Menu, type **4** and press **Enter**. The Radio Configuration Menu appears.

Radio Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Radio Port Administrative Status	enabled
2	Configured Domain	0
3	Configured Channel	1
4	Configured Subchannel	1
5	Configured Station Type	master
6	Configured Master Name	MASTER
7	Repeating Enabled	false
8	Delay Radio Reconfigure	false
9	MAC Optimize	auto
10	No Traffic Trap Period (seconds)	0
11	Radio Traffic Trap Threshold (%)	100
12	Radio Broadcast Trap Threshold (%)	100
13	Set Security ID	
14	Reset Radio	

Enter a selection number or <ESC> for previous menu ->

Parameter	Description	Default
Radio port administrative status (SNMP)	Determines if you can use an SNMP manager to change the radio parameters. You may need to enable this parameter if the wireless interface is disabled by an SNMP manager.	Enabled

---

**Radio Configuration Parameters**

Parameter	Description	Default
Configured domain	<p>Specifies the domain (0 to 16) that all masters and stations in the same roaming subnetwork will use to communicate with each other. The domain is a software filter and does not affect the actual radio frequency or the frequency hop sequence.</p> <p>You can use different domains to establish different roaming subnetworks within your building.</p>	0
Configured channel	<p>Specifies the channel (1 to 15) that each master will use to communicate with its stations. Each channel defines a unique frequency hopping sequence. To communicate, all radios must be on the same channel and there must be one (and only one) master that provides the timing for that channel.</p> <p>For networks with multiple masters (such as in roaming subnetworks), set each master to a different channel. Stations determine their channel by the master to which they are synchronized.</p> <p>Channels allow multiple subnetworks with higher data rate transmission capability in the same air space.</p>	1
Configured subchannel (1 to 15)	<p>Specifies a subchannel to use if you need more than 15 masters in the same coverage area, and therefore you have used all the channels. The subchannel is a software code that is appended to each radio packet and does not affect the frequency hop sequence.</p> <p>For example, use channel 1, subchannel 1 for Master A and channel 1, subchannel 2 for Master B. The two masters will not communicate with each other. However, they are still sharing the 1.6 Mbps pipe since they are both sharing the same channel.</p>	1

---

**Radio Configuration Parameters**

Parameter	Description	Default
Configured station type	Determines if the access point is acting as a station or a master.	Master
Configured master name (Optional)	Specifies a unique name (1 to 11 alphanumeric characters) for each master.	MASTER
Repeating enabled	Determines if the access point is to repeat signals coming from one data collection device that are destined for another data collection device. These two devices must be out of range of one another, but both devices must be within range of the access point.	False
Delay radio reconfigure	<p>Lets you delay radio parameter changes from taking effect. Set this parameter to True if:</p> <ul style="list-style-type: none"> <li>• you are configuring the access point and data collection devices are still sending packets through the access point to the host. You do not want them to lose communication when the parameters change.</li> <li>• you are using a wireless device to configure the access point and you cannot afford to lose communication when the parameters change.</li> </ul> <p>For the radio parameters to take effect, you will need to reset the radio or reset the access point.</p>	False
MAC optimize	<p>Specifies what type of MAC optimization to use. If you leave the parameter at Auto, the access point determines the number of data collection devices that are synchronized to it and adjusts this parameter accordingly.</p> <p>You may want to set this parameter to improve the throughput for smaller networks. If you have 0 to 1 devices, set this parameter to Light. If you have 2 to 7 devices, set it to Very Light. If you have more than 7 devices, set it to Normal.</p>	Auto



---

**Radio Configuration Parameters**

Parameter	Description	Default
No traffic trap period (SNMP)	Specifies the number of seconds (0 to 10,000,000) after which the SNMP manager sends a No-Traffic trap.	0
Radio traffic trap threshold (SNMP)	Specifies a percentage (10 to 100) of radio traffic after which the SNMP manager sends a Radio High Usage trap.	100*
Radio broadcast trap threshold (SNMP)	Specifies a percentage (10 to 100) of radio broadcast traffic after which the SNMP manager sends a Radio High Usage trap.	100*
Set security ID	Specifies a security ID for every access point and data collection device in the wireless network. This ID is encrypted and stored in the access point itself; it is not stored in software.  The security ID is case-sensitive and can be from 1 to 20 alphanumeric characters.	None
Reset radio	Lets you reset the radio in the access point without resetting the entire unit. If you set the Delay Radio Reconfigure parameter to true, this feature will cause any changes to the radio parameters that have not taken effect to take effect.	None

\*If you set this parameter to 100, you will disable this trap.

## Using the Ethernet Configuration Menu

---

The Ethernet Configuration Menu lets you enable or disable the Ethernet port administrative status.

To access the Ethernet Configuration Menu

- From the Configuration Menu, type **5** and press **Enter**. The Ethernet Configuration Menu appears.

Ethernet Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Ethernet Port Administrative Status	enabled
Enter a selection number or <ESC> for previous menu ->		

Parameter	Description	Default
Ethernet port administrative status (SNMP)	Use this parameter to enable the Ethernet port administrative status if the Ethernet interface is disabled by an SNMP manager. This parameter corresponds to the SNMP MIB-II Administrative status parameter.	Enabled

## Setting Security on Access Points

---

This section explains how to use security IDs and the authorization table for added security on your wireless network.

---

### *Setting the Security ID*

For added security, you can set a security ID on access points and data collection devices. The security ID must be the same for all devices that are communicating in the same wireless network. This ID is encrypted and stored in the access point itself; it is not stored in the software.

The security ID is case-sensitive and it can be up to 20 alphanumeric characters. By default, no security ID is set.

To set the security ID

1. From the Configuration Menu, type **4** to access the Radio Configuration Menu and press **Enter**.
2. From the Radio Configuration Menu, type **13** to set the Security ID and press **Enter**.
3. Enter a new Security ID and press **Enter**.

---

### *Using the Authorization Table*

In addition to setting the security IDs, you can use the authorization table to record the MAC addresses of the data collection devices that are allowed or disallowed to connect to the Ethernet network through the access point.

To access the Authorization Table Configuration Menu

1. From the Main Menu, type **1** to access the Configuration Menu and press **Enter**.
2. From the Configuration Menu, type **6** to access the Authorization Table Configuration Menu and press **Enter**.

Authorization Table Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Authorization Table	
2	Authorization Table Usage Option	disabled
3	Enable/Disable Unauthorized Address Trap	
4	AP Authorization Configuration Download Table	
5	Update Authorization Configuration of All APs	
Enter a selection number or <ESC> for previous menu ->		

Parameter	Description	Default
Authorization table	Lists the MAC addresses that can communicate through the access point. This table can hold a maximum of 256 MAC addresses, which you need to manually add or delete.	
Authorization table usage option	Determines if this authorization table will include or exclude wireless devices and if the table will be used at all. If you have not recently updated the table, you may want to disable usage until you can add all the proper addresses.	Disabled
Enable/disable unauthorized address trap (SNMP)	Determine if an SNMP trap will tell the SNMP manager that an unauthorized user has tried to send packets through the access point.	
AP authorization configuration download table	Lets you watch the progress of the distribution. This table lists the MAC address, IP address, version, and download status of the access points. The distribution usually happens so quickly that you only see the final status.	
Update authorization configuration of all APs	Distributes the authorization table from this access point to all other access points on the network. You do not have to set up a new authorization table on each access point in the same network.	

# 4

## *Configuring the 0115 Access Point*



*This chapter explains how to configure the access point using the Configuration Menu.*

## *Using the Configuration Menu*

---

The Configuration Menu lets you set all the parameters that allow the 0115 Access Point to communicate with your network.

### To access the Configuration Menu

- From the Main Menu, type **1** and press **Enter**. The Configuration Menu appears.

Configuration Menu	
Selection	Description
-----	-----
1	TCP/IP Configuration Menu
2	Filter Configuration Menu
3	Bridge Configuration Menu
4	Radio Configuration Menu
5	Token Ring Configuration Menu
6	Authorization Table Configuration Menu
7	SNMP Configuration Menu
8	Reset Token Ring Access Point to Factory Defaults
9	Dump Configuration To Screen
Enter a selection number or <ESC> for previous menu ->	

From the Configuration Menu, there are several options. To access another menu or to access a parameter in a menu, type the number in the Selection column that corresponds to the menu or parameter you want and press **Enter**.

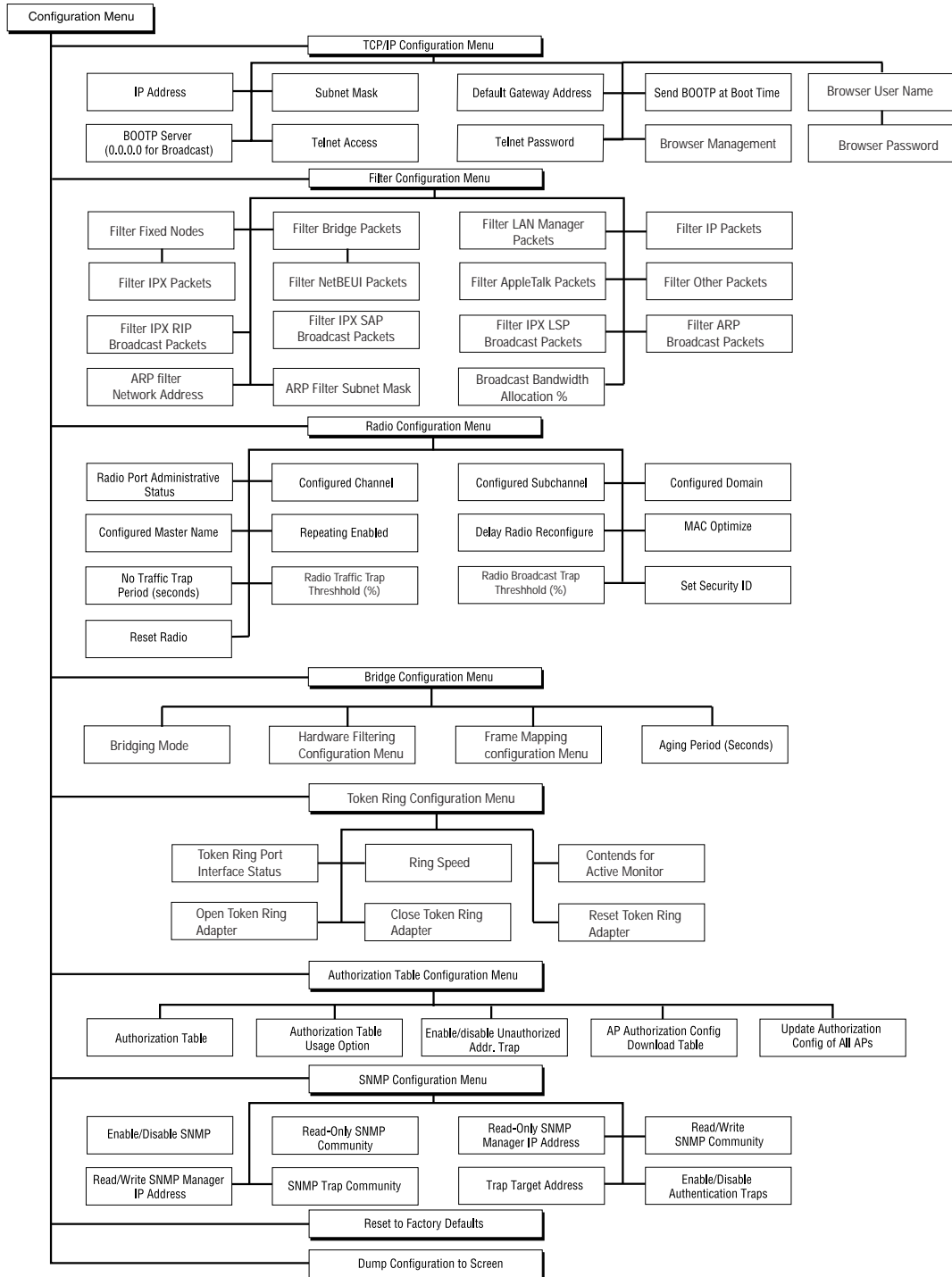
***Note:** Reset Token Ring Access Point to Factory Defaults option is only available if you are configuring the access point locally.*

### To return to a previous menu

- Press **Esc**.

# Configuring the Access Point

This chart shows all the parameters available in the Configuration Menu.





## Using the TCP/IP Configuration Menu

The TCP/IP Configuration Menu lets you change the TCP/IP parameters of the 0115 Access Point.

To access the TCP/IP Configuration Menu

- From the Configuration Menu, type **1** and press **Enter**. The TCP/IP Configuration Menu appears.

TCP/IP Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	IP Address	0.0.0.0
2	Subnet Mask	0.0.0.0
3	Default Gateway Address	0.0.0.0
4	Send BOOTP at Boot Time	true
5	BOOTP Server (0.0.0.0 for Broadcast)	0.0.0.0
6	Telnet Access	enabled
7	Telnet Password	
8	Browser Management	enabled
9	Browser User Name	
10	Browser Password	

Enter a selection number or <ESC> for previous menu ->

Parameter	Description	Default	Reset Access Point?
IP address	Assign each access point a unique valid IP v4 address.  Or, set the Send BOOTP at boot time parameter to True. This parameter lets the access point request an IP address from a BOOTP server each time it boots.	0.0.0.0	Yes
Subnet mask	Determines what network the access point is on.	0.0.0.0	Yes

---

**TCP/IP Configuration Parameters**

Parameter	Description	Default	Reset Access Point?
Default gateway address	Set this parameter if you want to route packets to an IP host or node on another IP subnet.  Since access points and devices cannot communicate across subnets, you must provide the IP address of a default gateway. This gateway will route the packets to the proper destination.	0.0.0.0	Yes
Send BOOTP at boot time	Set this parameter if you do not want to assign the access point an IP address. The access point can request an IP address from a BOOTP server each time it boots.  <i>Note: If you are requesting an IP address from a BOOTP server, the MAC address for the access point is on the bottom panel.</i>	True	No
BOOTP server address	If you set the Send BOOTP at boot time parameter to True, you must provide the IP address of that server.	0.0.0.0 (sends a broadcast)	No
Telnet access	Enable this feature if you want a remote user to be able to open a Telnet session to the access point.	Enabled	No
Telnet password	If you set the Telnet access parameter to Enabled, you can provide a password to control access to this feature.	None	No
Browser management	Enable this feature if you want a remote user to be able to use a Web browser to manage the access point.	Enabled	No
Browser user name	If you set the Browser management parameter to Enabled, you can provide a user name and password to control access to this feature.	None	No
Browser password			

### Example - Setting the IP Address

To set an IP address for the access point, you need to connect the access point to your terminal or PC and configure it locally. Or, you can enable the access point to request its IP address from a BOOTP server and supply the address of the server.

To set the IP address

1. From the Main Menu, type **1** and press **Enter**. The Configuration Menu appears.
2. From the Configuration Menu type **1** and press **Enter**. The TCP/IP Configuration Menu appears.
3. At the “Enter a selection number or <ESC> for previous menu” prompt, type **1** and press **Enter**. The current IP address parameter is displayed on your screen and its current value next to it.

```
IP Address [0.0.0.0]
Enter a new value ->
```

4. Enter a valid IP v4 address and press **Enter**.

```
IP Address [0.0.0.0]
Enter a new value -> 100.9.8.7
```

The TCP/IP Configuration Menu appears with the new value for the IP address in the Current Value column.

TCP/IP Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	IP Address	100.9.8.7
2	Subnet Mask	0.0.0.0
3	Default Gateway Address	0.0.0.0
4	Send BOOTP at Boot Time	true
5	BOOTP Server (0.0.0.0 for Broadcast)	0.0.0.0
6	Telnet Access	enabled
7	Telnet Password	
8	Browser Management	enabled
9	Browser User Name	
10	Browser Password	
Enter a selection number or <ESC> for previous menu ->		

## Using the Filter Configuration Menu

---

The Filter Configuration Menu lets you customize the type of traffic that is forwarded from the token ring network to the wireless network. None of these filters affects traffic flow. However, the more filters you turn on, the more bandwidth you save. For most situations, the default filters work.

### To access the Filter Configuration Menu

- From the Configuration Menu, type **2** and press **Enter**. The Filter Configuration Menu appears.

Filter Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Filter Fixed Nodes	filtering
2	Filter Bridge Packets	filtering
3	Filter LAN Manager Packets	filtering
4	Filter IP Packets	not filtering
5	Filter IPX Packets	not filtering
6	Filter NetBEUI Packets	not filtering
7	Filter AppleTalk Packets	filtering
8	Filter Other Packets	not filtering
9	Filter IPX RIP Broadcast Packets	filtering
10	Filter IPX SAP Broadcast Packets	filtering
11	Filter IPX LSP Broadcast Packets	filtering
12	Filter ARP Broadcast Packets	not filtering
13	ARP Filter Network Address	0.0.0.0
14	ARP Filter Subnet Mask	0.0.0.0
15	Broadcast Bandwidth Allocation	% 80

Enter a selection number or <ESC> for previous menu ->

---

**Filter Configuration Parameters**

Parameter	Description	Default
<b>Filter Fixed Nodes</b> (Multi-Ring mode)	Determines if packets that are destined for a non-broadcast, non-multicast, non-bridge address are forwarded to the wireless network.  Do not enable this filter when using the node address overwrite feature.	Filtering
<b>Filter Bridge Packets</b>	Determines if the access point will forward packets that are sent between access points (bridges) to the wireless network. Bridges periodically exchange packets to discover each other.	Filtering
<b>Filter LAN Manager Packets</b>	Determines if the access point will forward LAN Manager Packets to the wireless network. These packets are destined for LAN Manager stations.	Filtering
<b>Protocol Type Filters</b>	Determines if the access point will forward packets of a particular protocol type to the wireless network.  If you enable Filter other packets, only the protocol types that are listed are forwarded. All other protocol types are filtered.  Do not filter protocol types that your wireless network must receive. For example, if you use TCP/IP on your wireless network, do not filter IP traffic.	
	Filter IP packets	Not filtering
	Filter IPX packets	Not filtering
	Filter NetBEUI packets	Not filtering
	Filter AppleTalk packets	Filtering
	Filter DECNet packets	Not filtering
	Filter other packets	Not filtering

---

**Filter Configuration Parameters**

Parameter	Description	Default
<b>IPX Broadcast Filters</b>	Determines if the access point will forward various IPX packets from the wired network to the wireless network.  You can usually filter all the IPX packets since these packets are of interest to routers and not data collection devices.	
	Filter IPX RIP broadcast packets	Filtering
	Filter IPX SAP broadcast packets	Filtering
	Filter IPX LSP broadcast packets	Filtering
<b>ARP Broadcast Filter</b>	Determines if the access point enables IP ARP broadcast filtering. ARP packets will be forwarded from the wired network to the wireless network only if the destination IP address is on the IP network defined by the ARP filter network address and ARP filter subnet mask.	
	Filter ARP broadcast packets	Not filtering
	ARP filter network address	0.0.0.0
	ARP filter subnet mask	0.0.0.0
<b>Broadcast Bandwidth Allocation (%)</b>	Determines the maximum percentage of the RF bandwidth that may be allocated for broadcast traffic. This feature lets you limit broadcast traffic.  For example, to prioritize directed packets, you may want to reserve radio bandwidth for directed packets by setting this limit to less than 100%.	80

## Using the Bridge Configuration Menu

The Bridge Configuration Menu lets you set parameters for the learned database.

To access the Bridge Configuration Menu

- From the Configuration Menu, type **3** and press **Enter**. The Bridge Configuration Menu appears.

Bridge Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Bridging Mode	TB
2	Hardware Filtering Configuration Menu	
3	Frame Mapping Configuration Menu	
4	Aging Period (seconds)	300
Enter a selection number or <ESC> for previous menu ->		

Parameter	Description	Default
Bridging mode	Specifies the Bridging mode (Multi-Ring SR/TB, Single-Ring SR/TB, TB) in which the access point will operate.	TB
Bridge parameters menu (Multi-Ring mode, Single-Ring mode)	Lets you configure these bridge parameters, depending on the bridging mode: Bridge number, Radio ring number, and Token ring number.	
Hardware filtering configuration menu (Single-Ring mode, TB mode)	Lets you filter packets based on their destination MAC addresses.	None

---

**Bridge Configuration Parameters**

Parameter	Description	Default
Frame mapping configuration menu	Lets you configure how wireless node's packet frame types are to be converted.	None
Aging period (seconds)	Specifies the amount of time in seconds (10 to 1,000,000) that the learned physical address of the network node is stored in the Forwarding Database (DB). When the aging period expires, this learned physical address is discarded. This data is dynamically acquired by the access point so that it can forward packets properly.	300

---

**About Bridging Modes**

Originally developed by IBM, source routing is typically used in token ring environments. The source routing (SR) standard requires that the source station on a multi-ring LAN specify the route to reach the destination. In transparent bridging (TB), bridges dynamically learn the topology of a network. Bridges use this information to make forwarding decisions as opposed to requiring data collection devices to specify routes.

The 0115 Access Point operates in three different bridging modes:

- Multi-Ring SR/TB
- Single-Ring SR/TB
- TB

**Multi-Ring SR/TB Mode**

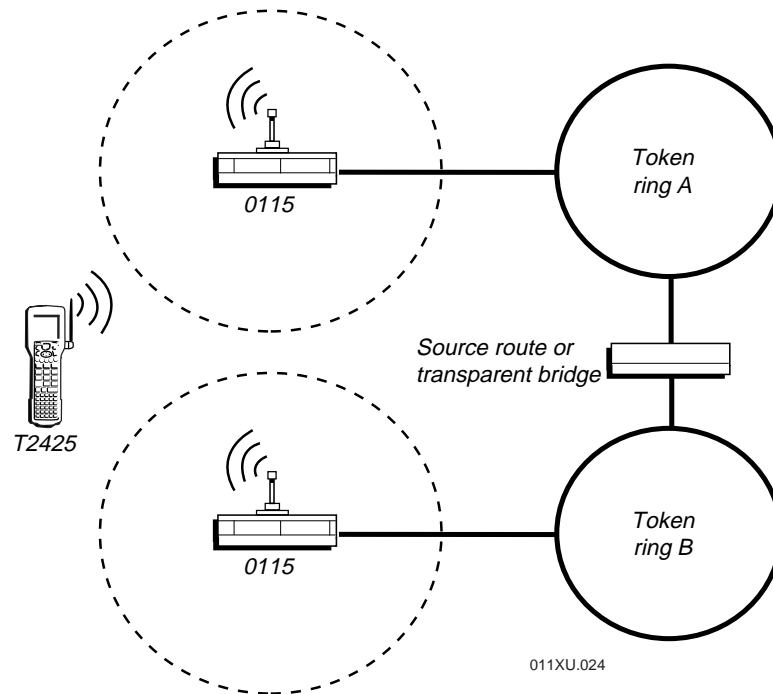
In Multi-Ring SR/TB mode, you must configure these parameters:

**Bridge Number** This parameter uniquely identifies the access point on a given token ring. This number must be different from all other bridge numbers on the ring.

**Radio Ring Number** This parameter is a virtual ring number that is associated with the wireless network. On the token ring, data collection devices appear to hosts to be part of a different ring.

**Token Ring Number** This parameter is the number of the token ring to which the access point is attached.



*Multi-Ring SR/TB Mode*

The access point looks at the Route Information Field (RIF) in each packet coming from the token ring network. From the RIF, the access point determines if the packet should be accepted and forwarded to the wireless network. Packets coming from the wireless network are forwarded to the token ring network if the destination node's physical address has not been learned to be in the wireless network.

The Multi-Ring SR/TB mode provides optimum performance when token ring network use is high. The access point is not required to do any learning or address lookups on the token ring side. Also, this mode will provide optimum performance if you are using locally administered MAC addresses and therefore, the wired and wireless nodes have similar prefixes.

*Single-Ring SR/TB Mode*

In Single-Ring SR/TB mode, you must configure this parameter:

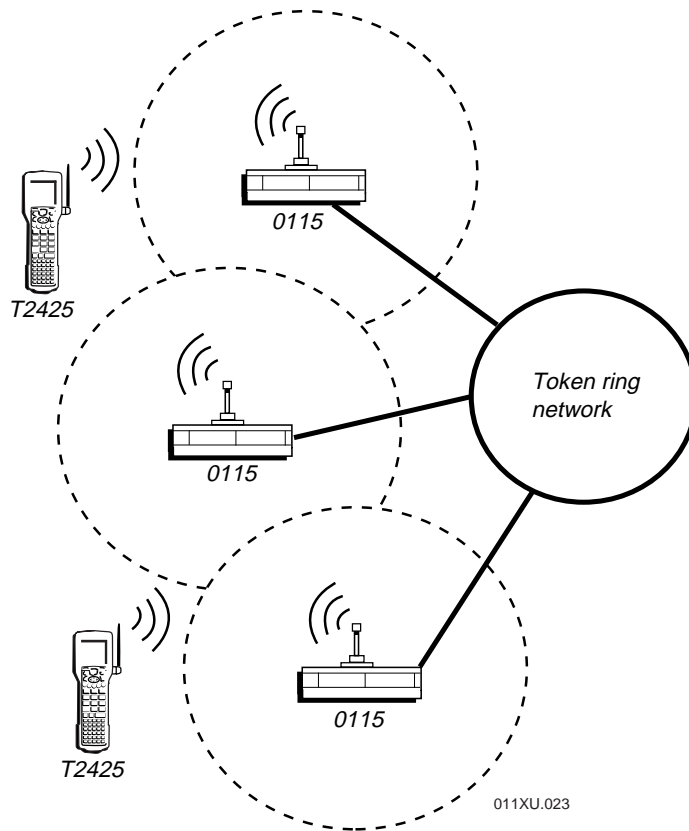
**Token Ring Number** This parameter is the number of the token ring to which the access point is attached.

Data collection devices appear to be on the token ring to which the access point is attached. Because data collection devices appear on the main ring, filtering based on the source route cannot be done. Learning occurs as it does in the Transparent Bridging mode and, therefore, performance in this mode is similar to the access point when it is in Transparent Bridging mode.

### TB Mode

In TB mode, you do not need to configure any other parameters. The TB mode makes the access point act like a transparent bridge. That is, the access point listens to all packets on both of its ports, wired and wireless, and learns which physical addresses are on each side. It uses this information to limit the forwarding of packets from the token ring network to the wireless network and vice versa.

Because the access point must learn physical addresses and perform lookups for each packet on the token ring, its filtering performance on a heavily used token ring will be less than when operating in Multi-Ring SR/TB mode. You should only use this mode if the data collection devices on the token ring do not support source routing.



## Hardware Filtering Configuration Menu

The Hardware Filtering Configuration Menu lets you filter packets based on their destination MAC addresses. These packets will not be sent from the token ring network to the wireless network.

RL2 Packet Forwarding assumes the MAC addresses are to be filtered if they have MAC addresses beginning with 00-20-a6. You can enable up to three additional MAC address prefixes by using the MAC Prefix(n) to set the MAC address bytes and the Forward Packets with MAC Prefix(n) to enable the filter.

Hardware Filtering Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	RL2 Packet Forwarding	enabled
2	MAC Prefix1	00 00 00
3	Forward Packets with MAC Prefix1 disabled	
4	MAC Prefix2	00 00 00
5	Forward Packets with MAC Prefix2 disabled	
6	MAC Prefix3	00 00 00
7	Forward Packets with MAC Prefix3 disabled	

Enter a selection number or <ESC> for previous menu ->

## Frame Mapping Configuration Menu

The Frame Mapping Configuration Menu contains parameters that let you configure how wireless stations' packet frame types will be converted. Data collection devices send Ethernet packet frames to the access point, which converts them into token ring packet frames.

When the Auto Detect Wireless Frame Types parameter is enabled, the access point learns the frame types as the data collection devices are communicating. If you set this parameter to disabled, you can specify the frame type to be used in the Map Token Ring Frame Type To and Map Token Ring SNAP Frame Type To parameters.

**Note:** On some OS/2 stations, you may need to set the Automatic Mapping From LLC2 to EII parameter to enabled.

Frame Mapping Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Auto Detect Wireless Frame Types	enabled
2	Map Token Ring Frame Type to	Ethernet 802.2
3	Map Token Ring SNAP Frame Type to	Ethernet II
4	Automatic Mapping From LLC2 to EII	enabled

Enter a selection number or <ESC> for previous menu ->

## Using the Radio Configuration Menu

---

The Radio Configuration Menu lets you set the radio parameters for your 0115 Access Point parameters.

To access the Radio Configuration Menu

- From the Configuration Menu, type **4** and press **Enter**. The Radio Configuration Menu appears.

Radio Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Radio Port Administrative Status	enabled
2	Configured Domain	0
3	Configured Channel	1
4	Configured Subchannel	1
5	Configured Master Name	MASTER
6	Repeating Enabled	false
7	Delay Radio Reconfigure	false
8	MAC Optimize	auto
9	No Traffic Trap Period (seconds)	0
10	Radio Traffic Trap Threshold (%)	100
11	Radio Broadcast Trap Threshold (%)	100
12	Set Security ID	
13	Reset Radio	

Enter a selection number or <ESC> for previous menu ->

---

**Radio Configuration Parameters**

Parameter	Description	Default
Radio port administrative status (SNMP)	Determines if you can use an SNMP manager to change the radio parameters. You may need to enable this parameter if the wireless interface is disabled by an SNMP manager.	Enabled
Configured domain	Specifies the domain (0 to 16) that all masters and stations in the same roaming subnetwork will use to communicate with each other. The domain is a software filter and does not affect the actual radio frequency or the frequency hop sequence.  You can use different domains to establish different roaming subnetworks within your building.	0
Configured channel	Specifies the channel (1 to 15) that each master will use to communicate with its stations. Each channel defines a unique frequency hopping sequence. To communicate, all radios must be on the same channel and there must be one (and only one) master that provides the timing for that channel.  For networks with multiple masters (such as in roaming subnetworks), set each master to a different channel. Stations determine their channel by the master to which they are synchronized.  Channels allow multiple subnetworks with higher data rate transmission capability in the same air space.	1
Configured subchannel (1 to 15)	Specifies a subchannel to use if you need more than 15 masters in the same coverage area and therefore, you have used all the channels. The subchannel is a software code that is appended to each radio packet and does not affect the frequency hop sequence.	1

---

**Radio Configuration Parameters**

Parameter	Description	Default
Configured subchannel ( <i>continued</i> )	For example, use channel 1, subchannel 1 for Master A and channel 1, subchannel 2 for Master B. The two masters will not communicate with each another. However, they are still sharing the 1.6 Mbps pipe since they are both sharing the same channel.	
Configured master name (Optional)	Specifies a unique name (1 to 11 alphanumeric characters) for each master.	MASTER
Repeating enabled	Determines if the access point is to repeat signals coming from one data collection device that are destined for another data collection device. These two devices must be out of range of one another, but both devices must be within range of the access point.	False
Delay radio reconfigure	Lets you delay radio parameter changes from taking effect. Set this parameter to True if: <ul style="list-style-type: none"> <li>• you are configuring the access point and data collection devices are still sending packets through the access point to the host. You do not want them to lose communication when the parameters change.</li> <li>• you are using a wireless device to configure the access point and you cannot afford to lose communication when the parameters change.</li> </ul> <p>For the radio parameters to take effect, you will need to reset the radio or reset the access point.</p>	False
MAC optimize	Specifies what type of MAC optimization to use. If you leave the parameter at Auto, the access point determines the number of data collection devices that are synchronized to it and adjusts this parameter accordingly.	Auto

---

**Radio Configuration Parameters**

Parameter	Description	Default
MAC optimize ( <i>continued</i> )	You may want to set this parameter to improve the throughput for smaller networks. If you have 0 to 1 devices, set this parameter to Light. If you have 2 to 7 devices, set it to Very Light. If you have more than 7 devices, set it to Normal.	
No traffic trap period (SNMP)	Specifies the number of seconds (0 to 10,000,000) after which the SNMP manager sends a No-Traffic trap.	0
Radio traffic trap threshold (SNMP)	Specifies a percentage (10 to 100) of radio traffic after which the SNMP manager sends a Radio High Usage trap.	100*
Radio broadcast trap threshold (SNMP)	Specifies a percentage (10 to 100) of radio broadcast traffic after which the SNMP manager sends a Radio High Usage trap.	100*
Set security ID	Specifies a security ID for every access point and data collection device in the wireless network. This ID is encrypted and stored in the access point itself; it is not stored in software.  The security ID is case-sensitive and can be from 1 to 20 alphanumeric characters.	None
Reset radio	Lets you reset the radio in the access point without resetting the entire unit. If you set the Delay Radio Reconfigure parameter to true, this feature will cause any changes to the radio parameters that have not taken effect to take effect.	None

\*If you set this parameter to 100, you will disable this trap.

## Using the Token Ring Configuration Menu

---

The Token Ring Configuration Menu lets you set the radio parameters for your 0115 Access Point parameters.

To access the Token Ring Configuration Menu

- From the Configuration Menu, type **5** and press **Enter**. The Token Ring Configuration Menu appears.

Token Ring Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Token Ring Port Interface Status	enabled
2	Ring Speed	16 Mbps
3	Contends for Active Monitor	no
4	Open Token Ring Adapter	
5	Close Token Ring Adapter	
6	Reset Token Ring Adapter	
Enter a selection number or <ESC> for previous menu ->		

Parameter	Description	Default
Token ring port interface status (SNMP)	Use this parameter to enable the token ring interface if it has been disabled by an SNMP manager.	Enabled
Ring speed	Specifies the speed (4 Mbps, 16 Mbps) at which the access point communicates to the token ring network. This parameter must match the speed of the token ring network.	16 Mbps



---

**Token Ring Configuration Parameters**

Parameter	Description	Default
Contends for active monitor	<p>Specifies whether the access point participates in the process to select the active monitor of the ring.</p> <p>If you set this parameter to No, the access point will never become the active monitor of the ring, unless it is the only station in the ring.</p> <p>Each ring needs one active monitor to make sure the ring operates normally. The active monitor looks for token errors and begins the ring recovery process, when required. All other stations in the ring act as standby monitors and monitor the ring to make sure the active monitor is doing its job. If the stations detect that the active monitor is not doing its job, they will restart the contention process and select a new active monitor.</p>	No
Open token ring adapter	<p>Inserts the access point into the ring. The access point automatically attempts to open the adapter when it boots. If it fails, send this command after resolving the problem that caused the failure.</p> <p>Before the access point can send or receive data, you must test the cable connection, physically connect the receive and transmit pairs into the ring, discover its neighbors, and notify them that the ring configuration has changed.</p>	None
Close token ring adapter	<p>Removes the access point from the ring. You may be able to use this feature to resolve some token ring errors.</p>	None
Reset token ring adapter	<p>Resets the access point's token ring adapter. You may be able to use this feature to resolve some token ring errors.</p>	None

## *Setting Security on Access Points*

---

This section explains how to use security IDs and the authorization table for added security on your wireless network.

---

### *Setting the Security ID*

For added security, you can set a security ID on 0115 Access Points and data collection devices. The security ID must be the same for all devices that are communicating in the same network. This ID is encrypted and stored in the access point itself; it is not stored in the software.

The security ID is case-sensitive and it can be up to 20 alphanumeric characters. By default, no security ID is set.

To set the security ID

1. From the Configuration Menu, type **4** to access the Radio Configuration Menu and press **Enter**.
2. From the Radio Configuration Menu, type **12** to set the Security ID and press **Enter**.
3. Enter a new Security ID and press **Enter**.

---

### *Using the Authorization Table*

In addition to setting the security IDs, you can use the authorization table to record MAC addresses of the data collection devices that are allowed or disallowed to connect to the token ring network through the 0115 Access Point.

To access the Authorization Table Configuration Menu

1. From the Main Menu, type **1** to access the Configuration Menu and press **Enter**.
2. From the Configuration Menu, type **6** to access the Authorization Table Configuration Menu and press **Enter**.

```

                                Authorization Table Configuration Menu
Selection      Description                      Current Value
-----
1              Authorization Table
2              Authorization Table Usage Option      disabled
3              Enable/Disable Unauthorized Address
              Trap
4              AP Authorization Configuration
              Download Table
5              Update Authorization Configuration of
              All APs

Enter a selection number or <ESC> for previous menu ->
    
```

Parameter	Description	Default
Authorization table	Lists the MAC addresses that can communicate through the access point. This table can hold a maximum of 256 MAC addresses, which you need to manually add or delete.	
Authorization table usage option	Determines if this authorization table will include or exclude wireless devices and if the table will be used at all. If you have not recently updated the table, you may want to disable usage until you can add all the proper addresses.	Disabled
Enable/disable unauthorized address trap (SNMP)	Determine if an SNMP trap will tell the SNMP manager that an unauthorized user has tried to send packets through the access point.	
AP authorization configuration download table	Lets you watch the progress of the distribution. This table lists the MAC address, IP address, version, and download status of the access points. The distribution usually happens so quickly that you only see the final status.	
Update authorization configuration of all APs	Distributes the authorization table from this access point to all other access points on the network. You do not have to set up a new authorization table on each access point in the same network.	



# 5

## *Using an SNMP Manager or a Web Browser*



*This chapter explains how to use an SNMP manager or a web browser to configure and monitor your access point.*

## *Configuring the Access Point Using an SNMP Manager*

---

You can configure and monitor your 0110/0111/0115 Access Point using an SNMP management package. The access point supports these MIBs:

- MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Source route bridge MIB (RFC 1525)
- (0110/0111) Extended Ethernet MIB (RFC 1643)
- (0115) Token Ring 802.5 MIB (RFC 1231)

Before you use an SNMP manager with your access point, you need to set certain parameters in the SNMP Configuration Menu either locally using a null modem cable or remotely through a Telnet session or modems.

***Note:** If you decide to configure the access point remotely using an SNMP manager, first you will need to set the IP address locally. Or, you can enable the access point to request its IP address from a BOOTP server and supply the address of the server.*

---

### *Using the SNMP Configuration Menu*

You may want to configure your 0110/0111/0115 Access Point through the SNMP Configuration Menu (in-band or out-of-band) to set SNMP parameters before using an SNMP manager.

To access the SNMP Configuration Menu

- From the Configuration Menu, type **7** to access the SNMP Configuration Menu and press **Enter**.

SNMP Configuration Menu		
Selection	Description	Current Value
-----	-----	-----
1	Enable/Disable SNMP	enabled
2	Read-Only SNMP Community	public
3	Read-Only SNMP Manager IP Address	0.0.0.0
4	Read/Write SNMP Community	private
5	Read/Write SNMP Manager IP Address	0.0.0.0
6	SNMP Trap Community	AccessPointTrap
7	Trap Target Address	0.0.0.0
8	Enable/Disable Authentication Traps	enabled

Enter a selection number or <ESC> for previous menu ->

Parameter	Description	Default
Enable/disable SNMP	Lets you use an SNMP manager with the access point.	Enabled
Read-only SNMP community	Specifies the community that is supported by the access point. Actions permitted by this community are read-only (GET and GET-NEXT).  SET attempts using this community will be rejected. A general error response and an authentication trap (if enabled) will be generated.	Public
Read-only SNMP manager IP address	Specifies the IP address of the SNMP manager that is permitted to use the read-only SNMP community. An address of 0.0.0.0 indicates any manager may use this community.	
Read/write SNMP community	Specifies the community that is supported by the access point. Actions permitted by this community are read/write (GET, GET-NEXT, and SET).	
Read/write SNMP manager IP address	Specifies the IP address of the SNMP manager that is permitted to use the read/write SNMP community. An address of 0.0.0.0 indicates any manager may use the community.	

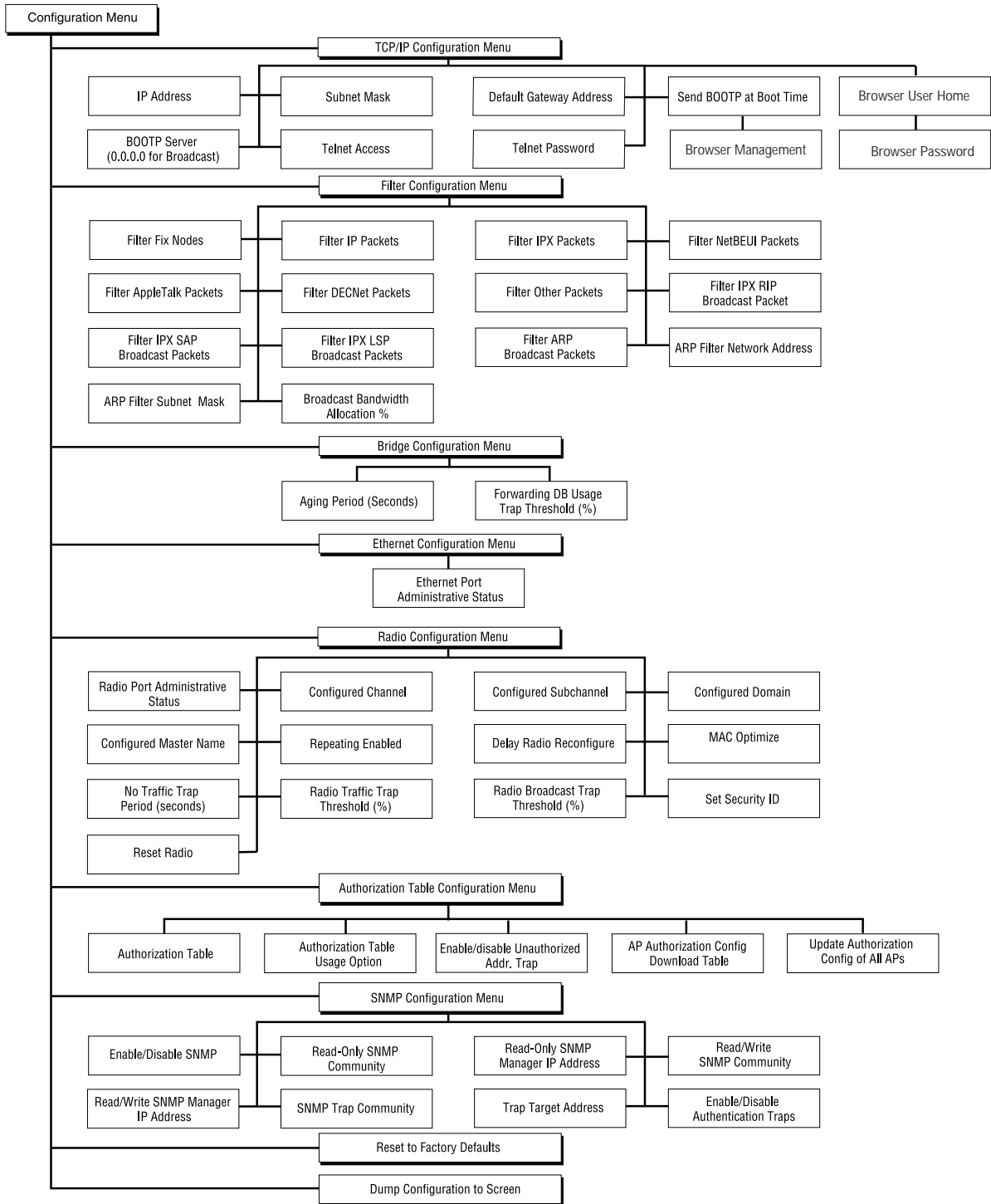


---

*SNMP Configuration Menu Parameters*

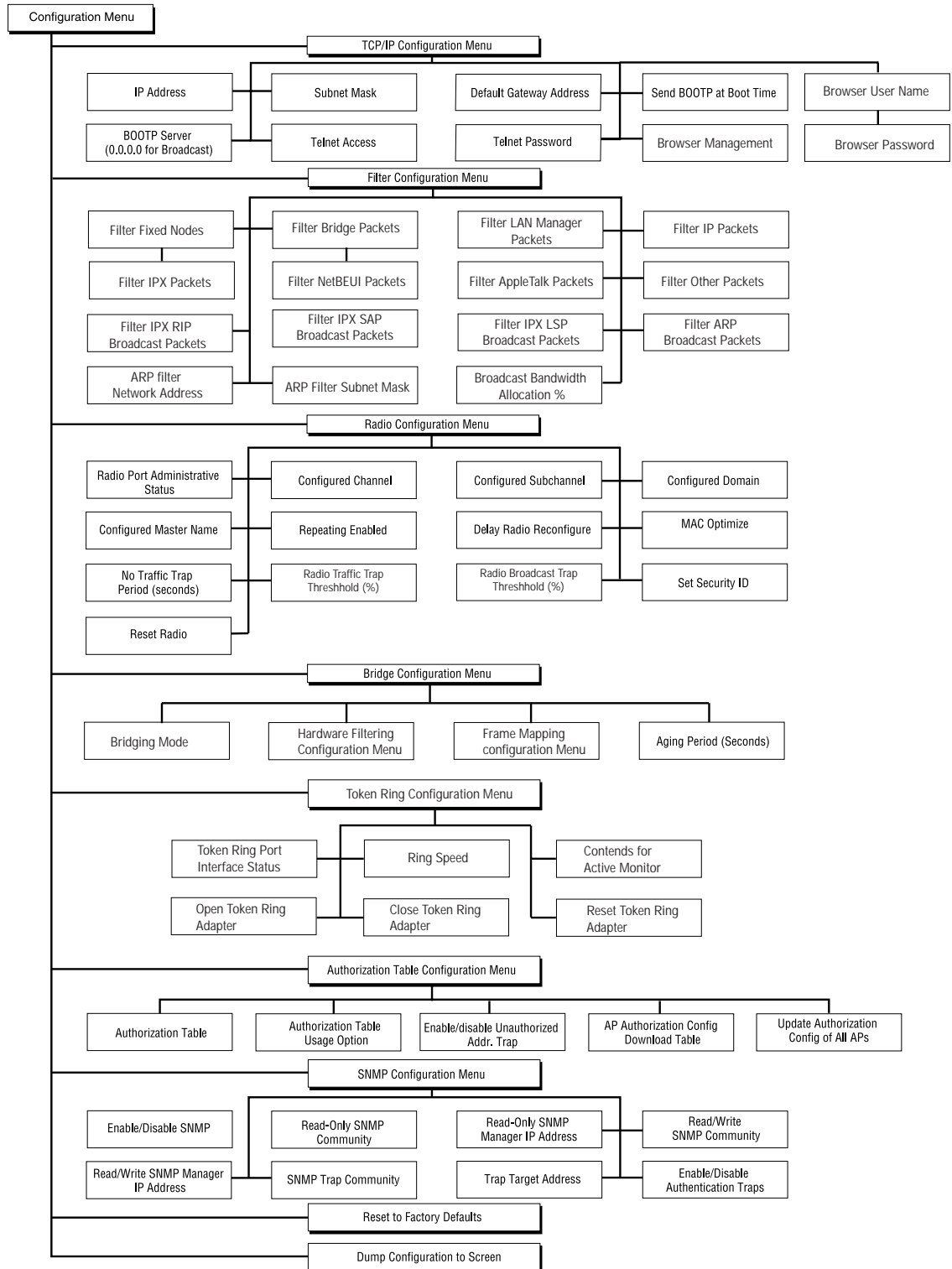
Parameter	Description	Default
SNMP trap community	Specifies the community that the access point will use when generating TRAP PDUs to remote managers.	
Trap target address	Specifies the IP address of the device that is receiving generated TRAP PDUs. A value of 0.0.0.0 disables trap generation.	
Enable/disable authentication traps	Determines if these traps are sent to the trap target address whenever anyone attempts to use an SNMP manager on the access point with an invalid community or from an invalid community.	

Ethernet Configuration Menu Parameters



011XU.011

### Token Ring Configuration Parameters



---

## *SNMP Supported Traps*

The 0110/0111/0115 Access Point supports the following authentication traps. When they occur, these traps are sent to the SNMP manager defined by the trap target address.

### *MIB II Traps*

Trap	Description
Cold start	Sent when the access point turns on or reboots.
Link up	Sent by each interface at startup or after coming back up.
Link down	Sent when the access point software cannot initialize or communicate with either interface.
Authorization	Sent to the network manager when someone tries to manage an access point with an invalid community.

### *Enterprise Specific Traps*

Trap	Description
No traffic	Sent when set to a non-zero value and when the access point does not receive any traffic from other radios for the configured period of time. You can configure the No-Traffic Trap Period parameter in the Radio Configuration Menu.
Broadcast threshold	Sent if the radio broadcast traffic exceeds the limit set by the Radio Broadcast Trap Threshold parameter in the Radio Configuration Menu.
Radio high usage	Sent if the radio traffic has crossed the limit set by the Radio Traffic Threshold parameter in the Radio Configuration Menu.
Serial port down	Sent when the serial port of the access point is not working. The status of this port is checked only when the access point boots.
Unauthorized usage trap	Sent when an unauthorized data collection device tries to connect to the network through the access point.

## *Configuring the Access Point Using a Web Browser*

---

You can configure and monitor your 0110/0111/0115 Access Point using a web browser. The access point supports these browsers:

- Netscape Navigator 3.01 or above for Win95/WinNT
- Netscape Navigator 3.01 or above for Macintosh
- Netscape Navigator 3.01 or above for SUN
- Microsoft Internet Explorer 3.01 or above for Win95/WinNT

To connect to the access point

1. Start a supported web browser on your PC. This PC must be connected to the network either using a wired or wireless connection.
2. Replace the URL path with the IP address of the access point. The browser displays the Intermec screen for the Access Point Web Manager.

For example, the starting URL is `www.intermec.com`. Replace this URL with `http://100.25.200.1`, which is the access point IP address.

3. If you set a browser user name and a browser user password in the TCP/IP Configuration Menu, you need to enter them before you can enter the Web Manager.

---

### *Understanding the Main Screen*

The main screen is divided into a left menu side and a right graphical side. The first half of the menu side details the network management options. The second half lists the device management options that are the same options as those available through the other configuration methods (Telnet, SNMP, etc.).

Next to each menu item is either a + (plus) or a - (minus). A plus indicates that there are submenu items that are not being displayed. To display these hidden submenu items, click once on the plus.

A minus indicates that all the submenu items are being displayed. To hide these submenu items, click once on the minus.

---

## *Understanding the Network Management Options*

The web manager offers three network management options: Discover APs, Network Map, and Traffic Monitor.

**Discover APs** This screen displays all of the access points that are detected on the wired network. It also tells you their MAC address, the IP address, the domain, the channel, the subchannel, and the master name.

When you position the mouse over the picture of the access point, the IP address appears on the status line. You can click on the picture to configure the access point.

**Network Map** This screen displays all of the access points and the wireless devices that are communicating with them. Under each access point is a list of the MAC addresses of the wireless devices that are currently synchronized to it.

When you position the mouse over the picture of the access point, the IP address appears on the status line. You can click on the picture to configure the access point.

**Traffic Monitor** This screen displays a real-time graph of the traffic that each access point is processing. Each access point is shown with its master name and MAC address. Each access point also has a graph that shows the volume of traffic and the:

- transmitted unicast packets
- transmitted broadcast packets
- received unicast packets
- received broadcast packets

Unicast packets are transmissions where the destination is a single, known node that is specified in the packet.

Broadcast packets also include multi-cast packets. Both types are packets where the destination is two or more nodes.

---

## *Understanding the Device Management Options*

The web manager offers five device management options: Configuration, Statistics, Status, Download Image, and Update Other APs.

For help on the Configuration Menu, see Chapter 3, "Configuring the 0110/0111 Access Point" and Chapter 4, "Configuring the 0115 Access Point."

For help on the Statistics Menu or the Status Menu, see Chapter 6, "Maintaining and Troubleshooting the Access Point."

For help on the Download Image Menu or Update Other APs Menu, see Appendix C, "Upgrading the Access Points."

# 6

## *Maintaining and Troubleshooting the Access Point*





*This chapter provides information that helps you diagnose and solve any problems you may encounter when installing and configuring the access point. If you cannot resolve the problem, contact Intermec Technical Support.*

## *Viewing the Access Point Statistics*

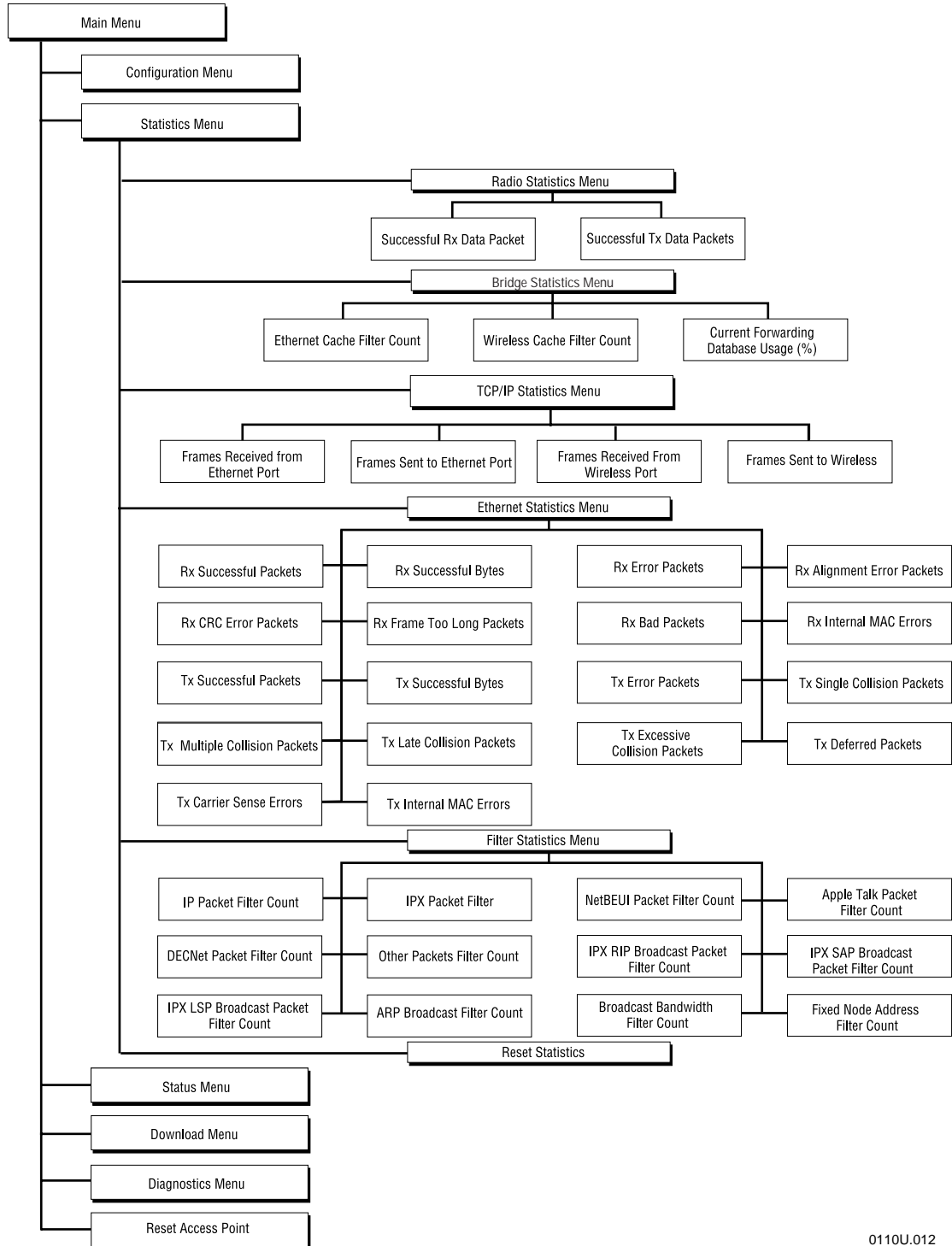
---

This section explains how you can use the Statistics Menu to view statistics on your wired and wireless network.

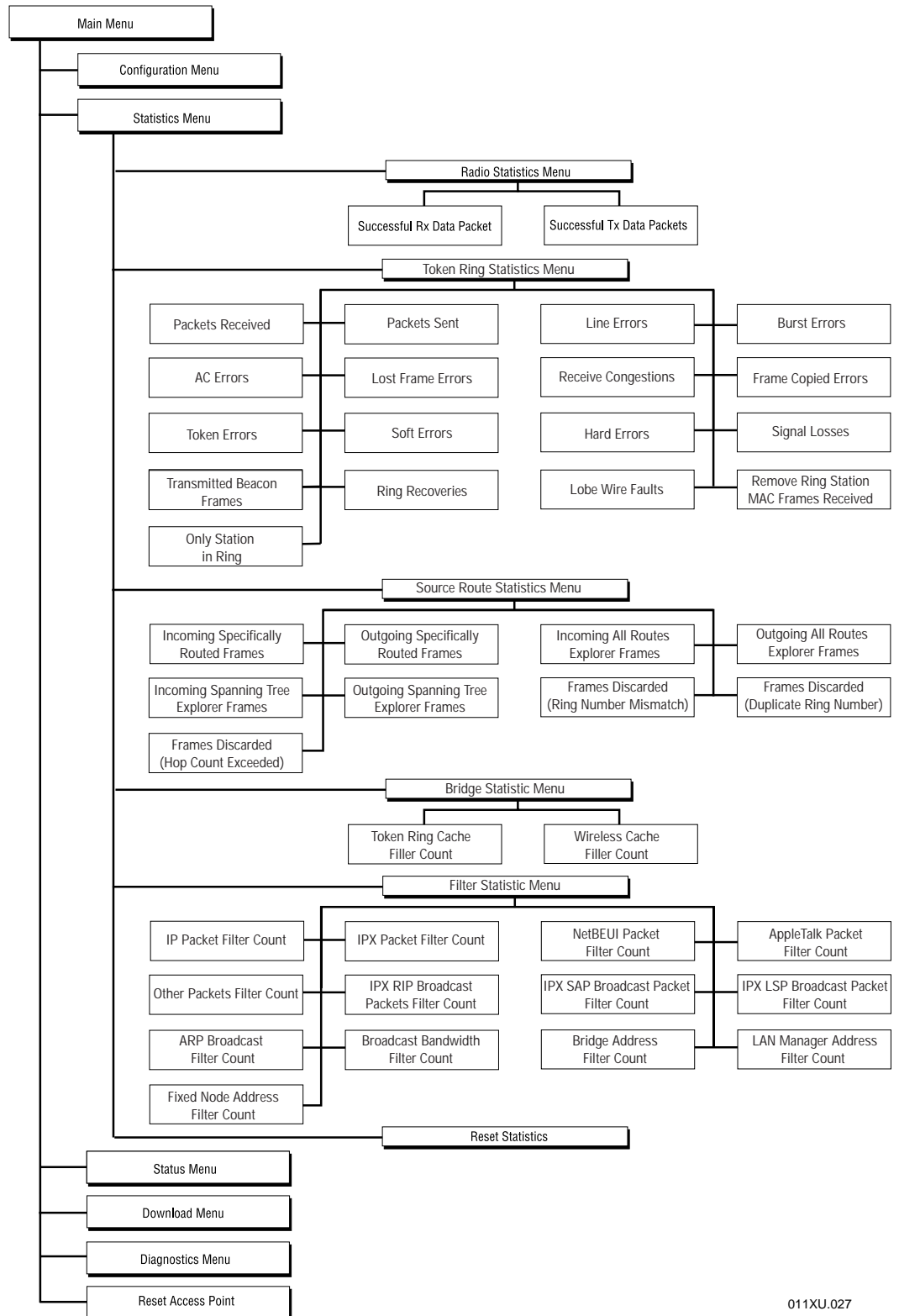
To access the Statistics Menu

- From the Main Menu, type **2** and press **Enter**.

Ethernet Statistics Menu Parameters



Token Ring Statistics Menu Parameters



011XU.027

---

### *Radio Statistics (Ethernet and Token Ring)*

The radio statistics show the number of successfully transmitted and received packets through the radio of the 0110/0111/0115 Access Point.

---

### *Bridge Statistics (Ethernet and Token Ring)*

The bridge statistics show information about packets that were filtered due to the 0110/0111/0115 Access Point learning about the location of nodes. It also shows the percentage of the forwarding database table that is taken up by learned node addresses. You can also view this table through the Status Menu, discussed later in this chapter.

---

### *Filter Statistics (Ethernet and Token Ring)*

The filter statistics show the number of packets that the 0110/0111/0115 Access Point filtered out because of the various filter options you chose.

---

### *Reset Statistics (Ethernet and Token Ring)*

You can reset the existing 0110/0111/0115 Access Point statistics and start gathering new statistics.

To reset statistics

1. From the Statistics Menu, type **6** and press **Enter**.
2. Type **1** to confirm that you want to reset the statistics and press **Enter**.

---

### *TCP/IP Statistics (Ethernet)*

The TCP/IP statistics show the number of frames (packets) that were sent to and received from the wired and wireless sides of the 0110/0111 Access Point. This count does not include traffic forwarded by the access point. However, it does include Telnet and SNMP packets, such as ping, that are processed by the access point's local stack.

---

### *Ethernet Statistics*

The Ethernet statistics display various information about Ethernet traffic to and from the 0110/0111 Access Point.

---

### *Token Ring Statistics*

The token ring statistics display various information about token ring traffic to and from the 0115 Access Point.

## Source Route Statistics Menu (Token Ring)

The source route statistics show the number of incoming, outgoing, and discarded frames processed by the 0115 Access Point.

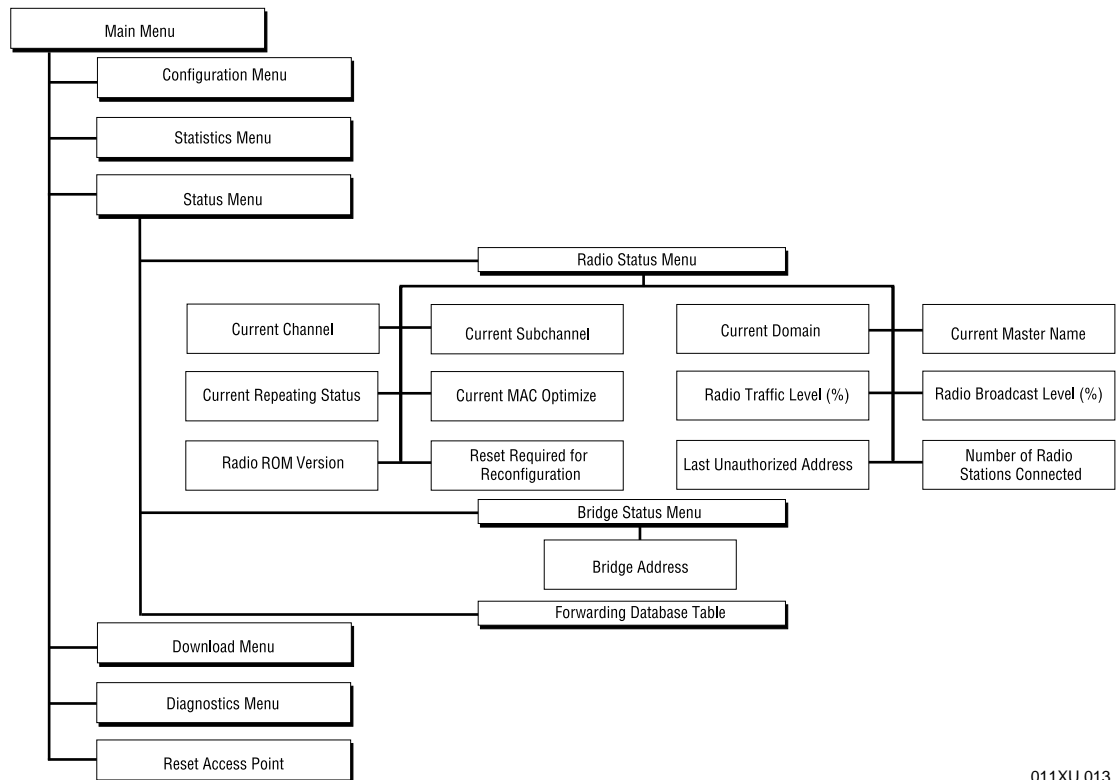
## Viewing the Access Point Parameters

This section explains how to use the Status Menu to view the current 0110/0111/0115 Access Point parameters.

To access the Status Menu

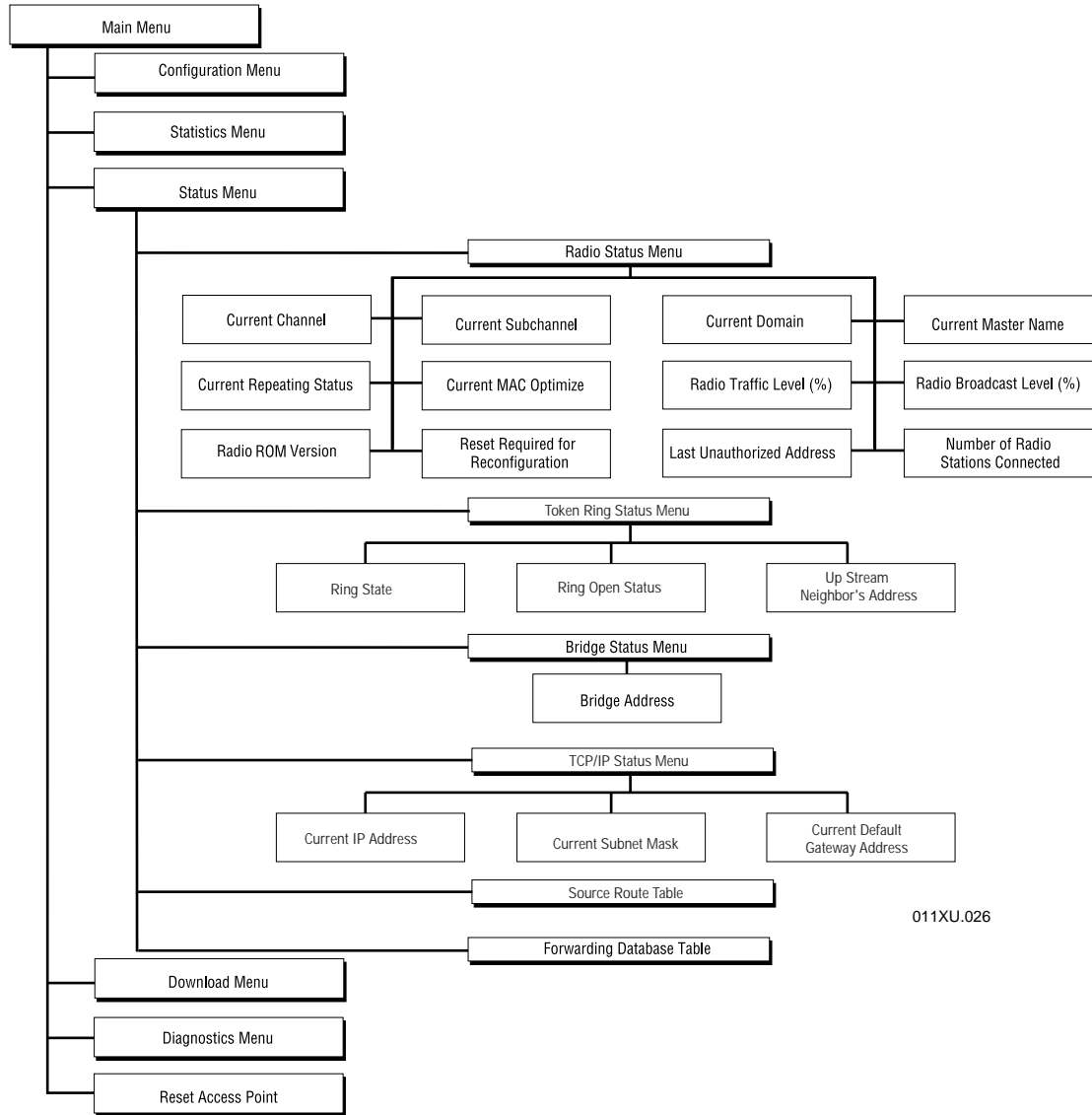
- From the Main Menu, type **3** and press **Enter**.

### Ethernet Status Menu Parameters



011XU.013

Token Ring Status Menu Parameters



011XU.026

---

### *Radio Status Menu (Ethernet and Token Ring)*

The current 0110/0111/0115 Access Point radio parameters appear in the Radio Status Menu.

Parameter Name	Description
Current Channel	The channel the access point is using to communicate with its data collection devices.
Current Subchannel	The subchannel the access point is using to communicate with its data collection devices.
Current Domain	The domain all access points and data collection devices are using to communicate.
Current Master Name	A meaningful name for the access point.
Radio traffic level	This value may cause an SNMP trap.
Radio broadcast level	This value may cause an SNMP trap.
Last unauthorized address	Shows the MAC address of the last data collection device that tried to attach to the Ethernet network through this access point, but was prevented because of the authorization table.
Radio ROM version	The radio ROM version of this access point.
Reset required for reconfiguration	Set to true if there is a parameter pending that will not take effect until the access point or radio is reset.
Number of radio stations connected	The number of the current data collection devices configured as stations that are synchronized to this access point and have communicated within a specified time period (Aging Period parameter).
Aging period	This parameter is used with the Number of Radio Stations Connected parameter.

---

### *Bridge Status Menu (Ethernet and Token Ring)*

The MAC address of the 0110/0111/0115 Access Point is the bridge address in the Bridge Status Menu.

---

## Forwarding Database Table (Ethernet and Token Ring)

The 0110/0111/0115 Access Point is a learning bridge. After watching the packets on the network, the access point builds a database table of nodes located on either side (wired or wireless) of it. Use this menu option to view the forwarding database table. This table can hold a maximum of 2048 entries.

If the Fixed Nodes filter is turned on, this table will only contain MAC addresses of data collection devices, which will change as those nodes roam.

---

### Example

Forwarding Database Table		
Physical Address	Port	Status
-----	----	-----
00:00:a2:00:49:c5	ethernet	learned
00:20:a6:31:04:fd	internal	self
Hit any key to continue ...		

---

## Token Ring Status Menu

The current 0115 Access Point token ring parameters appear in the Token Ring Status Menu.

---

## TCP/IP Status Menu (Token Ring)

The current 0115 Access Point TCP/IP parameters appear in the TCP/IP Status Menu.

Parameter Name	Description
Current IP Address	The IP address of the access point.
Current Subnet Mask	The subnet mask of the token ring network that the access point is connected to.
Current Default Gateway Address	The IP address of the gateway that will route the packets to the proper destination if you are sending packets to an IP host or node on another IP subnet.



---

### *Source Route Table (Token Ring)*

When the 0115 Access Point is configured for Multi-Ring SR/TB mode or Single-Ring SR/TB mode, this table shows the source routes that it has learned from each token ring station. In Multi-Ring SR/TB mode, the source route includes the radio ring number and the bridge number as part of the RIF.

---

## *Increasing Wireless Network Performance*

---

This section provides you with ideas on how to increase performance and network satisfaction on a wireless network.

---

### *Microwave Ovens*

Microwave ovens operate in the same frequency band as the access point. Therefore, if you use a microwave within range of your Intermec 2.4 GHz RF network, you may notice network performance degradation. However, both your microwave and your 2.4 GHz RF network will continue to function.

---

### *Transmission Range*

Every environment is unique with different obstacles, barriers, materials, etc. Therefore, it is difficult to determine the exact range that will be achieved with testing. Intermec highly recommends that you allow an Intermec-certified RF specialist to perform a site survey before you install a wireless network. For more information on site surveys, contact your local Intermec representative.

There are tools on the access point that were developed to aid in the site survey process, but they are not adequate enough to perform a complete site survey. For help using these tools, see Appendix B, “Using the Site Survey Tools and the Antenna Pointing Tool.”

Radio signals may reflect off of some obstacles or be absorbed by others, depending on their construction. For example, with two radios you may achieve up to 1000 feet (305 meters) in open space outdoors if the two antennas are line of sight, meaning there are no obstacles between them. However, the same two units may only achieve up to 500 feet (152 meters) of range when the RF signal has to travel through items, such as cubicles. If there are office walls to penetrate, the signal range may decrease to 300 feet (91 meters).

If you are interested in antenna options, contact your Intermec representative about antenna kits.

Proper antenna placement can help improve range. Here are some guidelines:

- Place the antenna in a vertical position. It can be mounted upside down from the ceiling or a beam.
- Place the antenna as high as possible. In an office environment, try to place it above cubicle walls.
- Do not place a sheet of metal (like a filing cabinet) between two antennas.
- Two antennas that are communicating should be in the same plane. For example, do not place one antenna on its side and place the other one standing upright.

## *How to Obtain Help With Your Installation*

---

The 0110/0111/0115 Access Point is designed to be very easy to install and operate. If you are having trouble with your installation, make sure you can answer these questions, before calling Intermec Technical Support:

- 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 version of the access point firmware are you using?

## *Diagnostics Menu*

---

There are diagnostic tools built into the 0110/0111/0115 Access Point that will help you or Intermec Technical Support in solving problems. If you call Intermec Technical Support, they may ask you to look at some of the parameters in the Diagnostics Menu.

To access the Diagnostics Menu

- From the Main Menu, type **5** and press **Enter**. The Diagnostics Menu appears.

Diagnostics Menu		
Selection	Description	Current Value
-----	-----	-----
1	Radio Diagnostics Menu	
2	Technical Support Parameters	Enabled
3	Boot ROM Version	
4	Flash Code Version	
5	Ping IP Hosts	
6	Discover APs	
7	Display Wireless Network Tree	

Enter a selection number or <ESC> for previous menu ->

Parameter Name	Description
Radio Diagnostics Menu	You can run the site survey tools, run the antenna pointing tool, and read the ROM version of the radio contained inside the access point. For help, see Appendix B, “Using the Site Survey Tools and the Antenna Pointing Tool.”
Technical support parameters	You can enable or disable this feature.
Boot ROM version	You can use this auto-boot feature to initialize the Ethernet, token ring and radio cards and start the SNMP agent, if you are using one. If the auto-boot is successful, you receive the message, “Initialization Complete.” You can only use this feature if your access point is connected locally using a null modem cable to a terminal or PC.
Flash code version	You can find out the software version of this access point.
Ping IP hosts	You can ping another IP host on the network. This feature may be useful in isolating which side of the access point (wired or wireless) is not working properly. To use this feature, you need to have the host’s IP address.

Parameter Name	Description
Discover APs	You can use this access point to look for all other access points on the network. The access point returns a table containing all the MAC addresses, IP addresses, domains, channels, subchannels, and master names it finds.
Display wireless network tree	<p>You can display the tree of all of the access points that this access point discovers along with their relationship to one another, i.e., who is synchronized to whom.</p> <p>The access point from which the tree is being built is listed with asterisks (***) next to its name.</p>

## Commonly Asked Technical Support Questions

Problem/Symptom/Question	Possible Solution/Answer
Is the access point fully booted? The Power LED is steady red.	<p>The Power LED changes from orange to steady green.</p> <p>You may have a hardware problem with your access point.</p> <ol style="list-style-type: none"><li>1. Unplug the access point and then plug it back in to cycle the power. Verify the Power LED is red.</li><li>2. Call Intermec Technical Support.</li></ol>
I cannot configure the access point locally using the serial port.	<ol style="list-style-type: none"><li>1. Verify you are using a null modem cable to connect the access point to your terminal or PC.</li><li>2. Verify the terminal or PC is set to 9600 N81.</li></ol>
I cannot ping or Telnet to my new access point.	<p>The access point does not come with a default IP address. Before you can remotely connect to the access point, you must locally set an IP address . Or, you can configure the access point to get an IP address from a BOOTP server.</p>

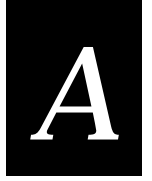
Problem/Symptom/Question	Possible Solution/Answer
(Ethernet) The data collection device (station) cannot connect to the network.	<p>You may not be in range of the access point (master).</p> <ol style="list-style-type: none"> <li>1. Use one of the site survey tools to verify that you have a wireless connection.</li> <li>2. Check the Ethernet Statistics Menu to verify there is Ethernet traffic that the access point can detect.</li> <li>3. If you are using a 10BaseT cable, verify that the 10BaseT LED on the side panel is lit. If it is lit, the cable is functional.</li> <li>4. Verify that the access point is not filtering out the type of traffic you are trying to pass through it.</li> </ol>
(Token ring) The data collection device (station) cannot connect to the network.	<p>You may not be in range of the access point (master).</p> <ol style="list-style-type: none"> <li>1. Use one of the site survey tools to verify that you have a wireless connection.</li> <li>2. Check the Token Ring Statistics Menu to verify there is token ring traffic that the access point can detect.</li> <li>3. If you are using a UTP cable, verify that the LED nearest the connector on the side panel is lit. If it is lit, the cable is functional.</li> <li>4. Verify the access point is not filtering out the type of traffic you are trying to pass through it.</li> </ol>
The data collection device (station) cannot synch to the access point (master).	<p>Verify that the data collection device and access point have the same domain and security ID.</p> <p>Access points must be configured as masters and data collection devices must be configured as stations.</p>
How can I tell which data collection devices are synchronized to my access point?	Use the Status Menu to view the Forwarding Database Table. Data collection devices that are synchronized to the access point are listed.
Are the wrong filters set?	Use the Configuration Menu to turn on one of the filters. Then, check the Filter Statistics Menu. If the count is increasing on the filter you set, that kind of traffic is on the network. If data collection devices cannot attach to the network after setting this filter, turn that filter off.

**Problem/Symptom/Question**

The throughput seems slow.

**Possible Solution/Answer**

1. Verify your antennas are well-placed, not behind metal, and there are not too many obstacles. See "Increasing Wireless Network Performance" earlier in this chapter.
2. If you move the antenna closer to the data collection device and throughput increases, you may want to add a second access point and implement roaming.
3. You may be able to set filters to filter out Ethernet traffic from the wireless side of the network.



# *Specifications*





*This appendix provides technical specifications for reference purposes only. Actual product's performance and compliance with local telecommunications regulations may vary from country to country. Intermec will only ship products that are type approved in the destination country.*

## General Specifications

---

<b>Data rate</b>	1.6 Mbps (Wireless)
<b>Domains</b>	16
<b>Channels</b>	15
<b>Range (std antenna)</b>	Up to 500 ft (150 m) indoors Up to 1000 ft (300 m) outdoors Unlimited with roaming
<b>Frequency band</b>	2.4 to 2.5 GHz world-wide (Varies by country)
<b>Radio type</b>	WLI Forum OpenAir, 2.4 GHz, frequency hopping, spread spectrum
<b>Radio power output</b>	(0110) 100mW (0111) 500mW (0115) 100mW or 500mW, depending on country RF regulations

## Physical Specifications

---

<b>Size</b>	1.66 in (42 mm) H 6.54 in (166 mm) L 8.54 in (217 mm) W
<b>Weight</b>	1.5 lb (0.71 kg)
<b>Temperature range</b>	Not using an environmental box -4°F to 140°F (-20°C to 60°C)  Inside an environmental box -4°F to 122°F (-20°C to 50°C)
<b>Humidity (non-condensing)</b>	10 to 90%
<b>Electrical rating</b>	≡ 10 to 18 V (input voltage), 750 mA

## *Other Specifications*

---

<b>Architecture</b>	Transparent bridge
<b>Ethernet interfaces</b>	10Base2 (thin coaxial BNC) 10BaseT (twisted-pair)
<b>Token ring interfaces</b>	STP/DBP plug UTP/RJ45 plug
<b>Data rate</b>	10 Mbps (Ethernet) 4 Mbps or 16 Mbps (token ring)
<b>Media Access protocol</b>	CSMA/CA
<b>Ethernet compatibility</b>	(0110/0111) Ethernet packet types and Ethernet addressing on the wired and wireless side (0115) IEEE 802.3 on the wireless side
<b>Token ring compatibility</b>	IEEE 802.5 on the wired side
<b>Filtering rate</b>	14,880 packets per second
<b>Filters (protocol)</b>	AppleTalk, NetBEUI, IPX, IP, DECNET, Other
<b>Filters (others)</b>	IP ARP, Novell RIP, SAP, LSP
<b>Serial port max data rate</b>	19,200 bps
<b>Management access (Telnet)</b>	Intermec 2.4 GHz RF, serial, Ethernet or token ring
<b>Software upgrades</b>	Downloadable over the network or serial port
<b>SNMP agent</b>	Version 1 RFC 1213 and 1493
<b>SNMP traps</b>	Cold start, link up, link down, authorization
<b>User authorization table</b>	Allow or disallow specific data collection devices to connect to the access point.
<b>Report management</b>	Remotely manage the access point through a modem attached to the serial port.
<b>Wireless network management</b>	Identify data collection devices synchronized to the access point.
<b>ETSI Testing</b>	For purposes of ETS 300 328 type testing, the access point was tested over a temperature range of -4°F to 131°F (-20°C to 55°C).

**B**

*Using the Site Survey Tools and the  
Antenna Pointing Tool*





*This chapter explains how to use the two mechanisms to determine proper placement of radios and antennas: a site survey tool and an antenna pointing tool. Both of these tools are included with the access point.*

## Using the Radio Diagnostics Menu

---

The Radio Diagnostics menu lets you run the site survey tools and the antenna pointing tool. It also provides the radio ROM version.

To access the Radio Diagnostics Menu

1. From the Main Menu, type **5** and press **Enter**. The Diagnostics Menu appears.
2. From the Diagnostics Menu, type **1** and press **Enter**. The Radio Diagnostics Menu appears.

Radio Diagnostics Menu		
Selection	Description	Current Value
-----	-----	-----
1	Run Broadcast Site Survey	
2	Run Directed Site Survey	
3	Run Antenna Pointing Tool	
4	Radio ROM Version	V1.8EB

Enter a selection number or <ESC> for previous menu ->

---

### Running a Broadcast Site Survey

Site survey tools show you the quality of the wireless link between the access points and the data collection devices. Running site surveys are useful to a network installer who is deciding where to place access points and data collection device antennas. Performing site surveys are also useful to a network administrator when diagnosing user performance problems.

The broadcast site survey is accessible from the Radio Diagnostics Menu. It shows the MAC addresses, Link Quality and Received Signal Strength (RSSI) of each data collection device that the access point can find.

#### To run a broadcast site survey

1. From the Radio Diagnostics Menu, type **1** and press **Enter**.
2. Select a period of time to let the access point sit. During this time the access point will record the MAC addresses found, link quality, and RSSI.
3. Review and evaluate the information in the site survey. The results will show an average value for each parameter.

If you check the data before the survey is complete, you will see average values for the elapsed time.

#### *Link Quality*

The higher the link quality number from a particular node, the better the link. If the link quality number is 0, this number indicates that the node is no longer responding at all. You need to watch this parameter to verify that you will be able to maintain a reliable wireless connection.

***Note:** The link quality number of the Intermec RF devices may be low if those radios are in their Sleep mode when being surveyed. As these adapters wake up, the link quality number may change.*

#### *RSSI*

RSSI indicates how strong a signal was received from a particular node.

---

### *Running a Directed Site Survey*

After running the broadcast site survey, you may want to run the directed site survey to check the packets per second and bytes per second measurements between the access point and a particular data collection device.

#### To run a directed site survey

1. From the Radio Diagnostics Menu, type **1** and press **Enter**.
2. Run the broadcast site survey. For help, see “Running a Broadcast Site Survey” earlier in this chapter.
3. From the Radio Diagnostics Menu, type **2** to run the directed site survey and press **Enter**.



```
Site Survey Table

Index Address Link Quality (1-poor, 5=strong) RSSI
-----
1 00:20:a6:10:2a:f4 5 156
2 00:20:a6:10:10:57 5 130

Index of the Node to Perform a Directed Site Survey on [1]
Enter new value-> 2

Packet Size (Bytes) [1500]
Enter new value->

Performing Site Survey
Hit <ESC> to terminate and any other key for intermediate results
..

Site Survey Completed

Node Address 00:20:a6:10:10:57
Packets Per Second 46
Bytes Per Second 69000
Average RSSI 151
Average Latency (mS) 42
Maximum Latency (mS) 150
Standard Deviation of Latency (mS) 22
```

---

## Using the Antenna Pointing Tool

The antenna pointing tool measures throughput between the access point and a specific data collection device as packets per second and kilobits per second. Running the antenna pointing tool can help a network installer with difficult antenna installations.

### To use the antenna pointing tool

1. From the Radio Diagnostics Menu, type **3** and press **Enter**.
2. Enter the MAC address of any data collection device that is synchronized with the master and press **Enter**.
3. Enter the packet size in bytes and press **Enter**.
4. Enter the sample interval and press **Enter**.

The antenna pointing tool shows you the MAC address, packets per second, kBps, and RSSI. The tool continues to run until you stop it. You can experiment with various placements of the antenna until you determine the optimum location.

```
Target Node Address [00:20:a6:00:1b:d5]
Enter new value->

Packet Size (Bytes) [1500]
Enter new value->

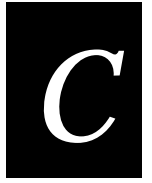
Sample Interval [Once per second]
  1. Twice per second
  2. Once per second
  3. Every five seconds
Enter a selection number or <ESC>-> 2

Press any key to end Antenna Pointing Tool
MAC: 00:20:a6:00:1b:d5    pps: 20    kBps: 30    RSSI: 149

Antenna Pointing Tool complete.

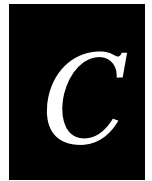
Hit any key to continue..
```





## *Upgrading the Access Points*





*This appendix explains how to use the Download Menu to upgrade one or more access points.*

## *Using the Download Menu*

---

You may need to upgrade the firmware on the 0110/0111/0115 Access Point. From the Download Menu you can download a new image file.

If you are configuring an 0110/0111 Access Point through the serial port, you can download a new image using Xmodem, BOOTP/TFTP, TFTP, or FTP.

If you are configuring an 0115 Access Point through the serial port you can download new image files using Xmodem, TFTP, or FTP.

**Note:** *If you are configuring an access point using Telnet, you will not have the Xmodem option.*

### To access the Download Menu

- From the Main Menu, type **4** and press **Enter**. The Download Menu appears.

```

                                     Download Menu
Selection      Description
-----
1              Download AP Image Using X-Modem
2              Download AP Image Using BOOTP/TFTP
3              Download AP Image Using TFTP
4              Download AP Image Using FTP
5              Accept Downloads From Other APs
6              AP Image Download Table
7              Update Images of All APs
8              Update Images of Selected APs
9              Update Image of a Specific AP

Enter a selection number or <ESC> for previous menu ->

```

**Note:** *The 0115 Access Point does not let you download the AP image using BOOTP/TFTP.*

---

## *Upgrading One Access Point*

1. Choose a method to download the new image.
2. Place the new image file on the hard drive, floppy disk, server, etc.

*Note: When downloading the image using Xmodem, use the Xmodem or Xmodem CRC protocol.*

3. From the Download Menu, select the method you are going to use to download the new image and press **Enter**.
4. Follow the prompts and enter the new image name, server IP address, FTP user name, or FTP password, pressing **Enter** after you fill in each parameter.

The new image is downloaded to the access point. When the download is successful, the access point will automatically reboot and load the new image.

---

## *Upgrading Multiple Access Points*

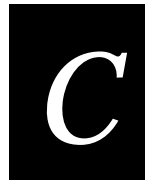
You can use one upgraded 0110/0111/0115 Access Point to upgrade other access points' firmware on the same wired subnetwork. You can choose to update:

- all access points on the segment or ring.
- selected access points on the segment or ring.
- one access point on the segment or ring, if you know its IP address.

To update all access points

1. Download the new image to one access point. For help, see "Upgrading One Access Point" earlier in this chapter.
2. From the Download Menu, select the option to update the images of all access points and press **Enter**.

The access point begins a discovery where it locates all the access points on the segment. It then downloads the new image to all the access points it finds.



**To update selected access points**

1. Download the new image to one access point. For help, see “Upgrading One Access Point” earlier in this chapter.
2. From the Download Menu, select the option to update the images of selected access points and press **Enter**.

The access point begins a discovery where it locates all the access points on the segment. From the access points it finds, you can choose which ones will receive the new image.

**To update one specific access point**

1. Download the new image to one access point. For help, see “Upgrading One Access Point” earlier in this chapter.
2. From the Download Menu, select the option to update the image of a specific access point and press **Enter**.
3. When prompted, enter the IP address of the access point you want to update and press **Enter**.

The access point downloads the new image to the access point.

---

*Disallowing an Access Point From Receiving an Image*

If you do not want an 0110/0111/0115 Access Point to receive any new images, you can set a parameter that allows or disallows it from receiving images sent on the wired network.

**To disallow an access point from receiving an image**

1. From the Download Menu, select the option to accept downloads from other access points and press **Enter**.
2. Type **2** to disable the ability of the access point to accept new images across the wired network.

**To allow an access point to receive an image.**

1. From the Download Menu, select the option to accept downloads from other access points and press **Enter**.
2. Type **1** to enable the access point to accept new images across the wired network.

---

## *Viewing the Download Status of the Access Points*

- From the Download Menu, select the option to view the AP image download table and press **Enter**.

The Access Point Download table appears. This table lists the MAC addresses, IP addresses, version, and download status of all the access points on the segment.



*Glossary*





***10BaseT, 10Base2, or 10Base5***

An implementation of Ethernet IEEE standard to describe the primary characteristics of the cabling system. The 10 signifies 10 Mbit/s. Base indicates that the type of signaling used is baseband. The T at the end means that twisted-pair cable is used. The number (2, 5, or 10) at the end indicates the maximum cable length in hundreds of meters.

***bandwidth***

The size (in Hertz) of the frequency range that a signal transmission occupies. Typical narrow band signals occupy a 25 KHz bandwidth. The 2.4 GHz RF network signal occupies a 1 MHz bandwidth.

***BOOTP (Bootstrap Protocol) server***

A device that contains a table that matches IP addresses to IP nodes. Before an IP node (device) can communicate with the network, it needs an IP address. When, the IP node queries the BOOTP server, it supplies its physical address. The BOOTP server then checks its tables to determine the corresponding IP address. To reassign an IP address, you only need to update the table in the BOOTP server.

***bridge***

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

***broadcast***

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

***channel***

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

***CSMA/CD (Carrier Sense Multiple Access/Collision Detection)***

An Ethernet device using CSMA/CD senses whether or not a channel is in use before attempting to transmit information. If it detects no other carrier, it transmits. If a collision is detected, the device stops transmitting, waits a random length of time, and begins transmitting again.

***data collection device***

An Intermec 2.4 GHz RF device used with a scanner that collects data by scanning bar codes and sending this data to a host computer.

***domain***

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

***download image***

A software file that is used to upgrade the software code running on the access point.

***Ethernet***

A type of LAN that allows the transmission of computer data, audio data, and video data at 10 Mbit/s across a linear bus topology. Ethernet uses the access method known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD). See IEEE 802.3 standard for the specifications.

***frequency hopping***

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

***interference***

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

***IP (Internet Protocol)***

This is the protocol for the network layer in TCP/IP protocol. It acts as a router for frames and is also responsible for frame addressing. It verifies it has all the frames to pass to the TCP layer and that they are in the correct order.

***IP address***

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

***IPX (Internet Packet eXchange)***

This is the protocol for the network layer in SPX/IPX protocol. It provides a way for packets to be exchanged on a network. It acts as a router for messages to other computers, it directs incoming data to the correct local process, and is also in charge of addressing.

***LAN (Local Area Network)***

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

***MAU (Media Access Unit)***

In a token ring network, a device to attach multiple network stations in a star topology, internally wired to connect the stations into a logical ring. The MAU contains relays to short out nonoperating stations. Multiple MAUs can be connected into a larger ring through their Ring In/Ring Out connectors.

***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.

***narrow band***

A channel of about 25 KHz bandwidth in the RF spectrum. The FCC allocates Narrow Band channels and issues a license to the user. Each user of a specific narrow band frequency range must obtain a site license from the FCC.

***network administrator***

The person who is responsible for the installation, management, and control of a network.

***OSI model***

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

***packet***

The unit of information that the network uses to communicate. A packet includes a single network message with its associated header, addressing information, data, and optional trailer. A packet can also be called a frame or datagram.

***peer-to-peer network***

A type of LAN whose workstations are capable of being both clients and servers.

***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 of that traffic.

*serial*

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

*server*

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

*SNMP (Simple Network Management Protocol)*

This protocol was used to manage network activity before the OSI model was approved. This application runs on top of the TCP/IP protocol. It uses management programs called "agents" to monitor network traffic. It stores the information it collects in the Management Information Base (MIB). Your network administrator can use management software interacting with the MIB to obtain information about network activity.

*spread spectrum*

A radio data transmission modulation technique by which the transmitted signal is spread over a bandwidth wider than the information bandwidth. Spread Spectrum bands are designated by the FCC and require no user license.

*SPX (Sequenced Packet eXchange)*

This is the protocol for the transport layer in the SPX/IPX protocol. It provides a method for reliable data transfer. SPX makes sure that packets from higher layers are received in order and without error before sending them to IPX for transmission.

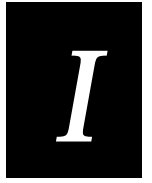
*subnet mask*

An internal TCP/IP protocol stack variable. This mask is used in the IP protocol to separate the subnet address from the local IP address. The IP protocol performs a bit-wise AND on the IP address and the subnet mask. Each address segment represents one byte, where 255 converts to FF hex.

For example, if the IP address is 192.009.150.184 and the subnet mask is for a Class C network (255.255.255.0), the subnet address is 192.009.150.

*TCP (Transmission Control Protocol)*

This is the protocol for the transport layer in the TCP/IP protocol. It provides a method for reliable, error-free, full-duplex communications between sender and receiver nodes. TCP takes long messages from higher layers and breaks them up before passing them to IP for transmission. It makes sure that the messages are in sequence when it receives them and it retries failed transmissions.



*Index*



## Numbers

- 10Base2 cabling, 2-4, 2-13
- 10BaseT cabling, 2-4, 2-12
- 10BaseT LED, 2-6
- 10BaseT, 10Base2, or 10Base5, definition, G-3
- 16 Mbps LED, 2-7
- 2.4 GHz RF networks, understanding, 1-5
- 4 Mbps LED, 2-7

## A

- access point
  - configuring, 2-10, 2-14, 3-4, 4-4
  - description, 1-3, 2-5
  - features, 1-3
  - fitting in your 2.4 GHz RF network, 1-5
  - installing, 2-9, 2-10
  - mounting, 2-10, 2-12
  - package contents, 2-3
  - resetting, 2-19
  - specifications, A-3
  - system requirements, 2-4
  - transmission range, 6-11
  - upgrading more than one, C-4
  - upgrading one, C-3, C-4
  - using in a more complex network, 1-8
  - using in a peer-to-peer network, 1-13
  - using in a roaming network, 1-8
  - using in a simple network, 1-5
  - using with JANUS devices, 1-5, 1-8, 1-9
  - using with TRAKKER Antares terminals, 1-5
- Access Point Download table, C-6
- aging period, 3-11, 4-12
- antenna
  - installing, 2-10, 2-11
  - options, 2-4
  - placement, 6-11
- antenna pointing tool, using, B-3, B-6
- AP authorization configuration download table, 3-18, 4-23
- architecture, A-4
- ARP broadcast filter, 3-10, 4-10
- attaching an antenna, 2-10, 2-11
- authentication traps, 5-5
  - enterprise specific, 5-8
  - MIB II, 5-8
  - supported by the access point, 5-8
- authorization table, 3-17, 3-18, 4-22, 4-23
- Authorization Table Configuration Menu, 3-17, 4-22
  - AP authorization configuration download table, 3-18, 4-23
  - authorization table, 3-18, 4-23
  - authorization table usage option, 3-18, 4-23
  - unauthorized address trap, 3-18, 4-23

- update authorization configuration of all APs, 3-18, 4-23

- authorization table usage option, 3-18, 4-23
- authorization trap, 5-8
- auto detect wireless frame types, 4-15
- automatic mapping from LLC2 to EII, 4-15

## B

- bandwidth, definition, G-3
- boot ROM version, 6-13
- BOOTP server
  - definition, G-3
  - using to set an IP address, 2-11, 2-15, 3-7, 4-7, 5-3
- BOOTP server address, 3-6, 4-6
- BOOTP/TFTP, using to download new firmware, C-3
- bootstrap protocol server, *See* BOOTP server
- bridge
  - definition, G-3
  - description, 1-3
- Bridge Configuration Menu, 3-11, 4-11
  - aging period, 3-11, 4-12
  - Bridge Parameters Menu, 4-11
  - Bridging mode, 4-11
  - forwarding DB usage trap threshold, 3-11
  - Frame Mapping Configuration Menu, 4-12, 4-15
  - Hardware Filtering Configuration Menu, 4-11, 4-15
- bridge number, 4-12
- Bridge Parameters Menu, 4-11
- bridge statistics, 6-6
- Bridge Status Menu, 6-9
- Bridging mode, 4-11, 4-12
  - bridge number, 4-12
  - Multi-Ring SR/TB mode, 4-12
  - radio ring number, 4-12
  - Single-Ring SR/TB mode, 4-13
  - TB mode, 4-14
  - token ring number, 4-12, 4-13
- broadcast bandwidth allocation, 3-10, 4-10
- broadcast site survey, B-3
  - link quality, B-4
  - RSSI, B-4
- broadcast threshold trap, 5-8
- broadcast, definition, G-3
- browser management, 3-6, 4-6
- browser password, 3-6, 4-6
- browser user name, 3-6, 4-6

## C

- cabling
  - STP, 2-13
  - using 10Base2, 2-13
  - using 10BaseT, 2-12
  - UTP, 2-13
- carrier sense multiple access/collision detection, *See* CSMA/CD

- cautions, explanation of, xii
- channel, 3-13, 4-17, A-3
  - definition, G-3
- close token ring adapter, 4-21
- cold start trap, 5-8
- command format conventions, xiv
- Configuration Menu, 2-8
  - accessing, 3-3, 4-3
  - Authorization Table Configuration Menu, 3-17, 4-22
  - Bridge Configuration Menu, 3-11, 4-11
  - dumping the configuration to screen, 2-18
  - Ethernet Configuration Menu, 3-16
  - Filter Configuration Menu, 3-8, 4-8
  - Radio Configuration Menu, 3-12, 4-16, 4-20
  - SNMP Configuration Menu, 5-3
  - TCP/IP Configuration Menu, 3-5, 4-5
- configuration, viewing on screen, 2-18
- configuring the 2.4 GHz RF network, guidelines, 2-14
- configuring the access point, 2-14
  - deciding on a method, 2-10
  - locally, 2-10, 2-15
  - using a PC with Telnet software, 2-10, 2-15
  - using a Web browser, 2-10, 5-9
  - using an SNMP manager, 2-10, 2-17, 5-3
  - using modems, 2-10, 2-16
  - using the Configuration menu, 3-3, 4-3
- connecting the power supply, 2-10
- connecting to the Ethernet network, 2-10, 2-12
- connecting to the token ring network, 2-10, 2-13
- connectors, side panel, 2-6, 2-7
- contents for active monitor, 4-21
- conventions used in this manual, xiv
- copyright information, ii
- CSMA/CD, definition, G-3
- cubicle-mount bracket, 2-4

## D

- data collection device, definition, G-3
- data rate, A-3, A-4
- default gateway address, 3-6, 4-6
- delay radio reconfigure, 3-14, 4-18
- diagnostic tools, using, 6-12
- Diagnostics Menu, 2-8
  - boot ROM version, 6-13
  - discover APs, 6-14
  - display wireless network tree, 6-14
  - flash code version, 6-13
  - ping IP hosts, 6-13
  - Radio Diagnostics Menu, 6-13
  - technical support parameters, 6-13
- directed site survey, B-4
- discover APs, 5-10, 6-14
- display wireless network tree, 6-14
- domain, 3-13, 4-17, A-3
  - definition, G-4

- download image, definition, G-4
- Download Menu, 2-8, C-3
- download status, viewing, C-6
- downloading new image files, C-3
- dumping the configuration to screen, 2-18

## E

- electrical rating, A-3
- enable/disable SNMP, 5-4
- enterprise specific traps, 5-8
  - broadcast threshold, 5-8
  - no traffic, 5-8
  - radio high usage, 5-8
  - serial port down, 5-8
  - unauthorized usage, 5-8
- environmental box, 2-4
- Ethernet compatibility, A-4
- Ethernet Configuration Menu, 3-16
  - chart, 5-6
  - Ethernet port administrative status, 3-16
- Ethernet interfaces, A-4
- Ethernet network, 1-4, 1-6
  - connecting, 2-10
  - connecting the access point, 2-12
  - using 10Base2 cabling, 2-13
  - using 10BaseT cabling, 2-12
  - viewing statistics, 6-3
- Ethernet port administrative status, 3-16
- Ethernet statistics, 6-6
- Ethernet Statistics Menu, chart, 6-4
- Ethernet Status Menu, chart, 6-7
- Ethernet, definition, G-4
- ETSI testing, A-4
- example of setting the IP address, 3-7, 4-7

## F

- filter bridge packets, 3-9, 4-9
- Filter Configuration Menu, 3-8, 4-8
  - ARP broadcast filter, 3-10, 4-10
  - broadcast bandwidth allocation, 3-10, 4-10
  - filter bridge packets, 3-9, 4-9
  - filter fixed nodes, 3-9
  - filter LAN Manager packets, 3-9, 4-9
  - IPX broadcast filters, 3-10, 4-10
  - protocol type filters, 3-9, 4-9
- filter fixed nodes, 3-9
- filter LAN Manager packets, 3-9, 4-9
- filter statistics, 6-6
- filtering rate, A-4
- filters, A-4
- firmware, upgrading, C-3
- flash code version, 6-13
- Forwarding Database table, 6-10
- forwarding DB usage trap threshold, 3-11
- forwarding packets with MAC prefix, 4-15



Frame Mapping Configuration Menu, 4-12, 4-15  
 auto detect wireless frame types, 4-15  
 automatic mapping from LLC2 to EII, 4-15  
 map token ring frame type to, 4-15  
 map token ring SNAP frame type to, 4-15  
 frequency band, A-3  
 frequency hopping, definition, G-4  
 front panel  
 Network LED, 2-5  
 Power LED, 2-5  
 Radio LED, 2-5  
 front panel, understanding, 2-5  
 FTP, using to download new firmware, C-3

**G**

guidelines for configuring, 2-14

**H**

Hardware Filtering Configuration Menu, 4-11, 4-15  
 forwarding packets with MAC prefix, 4-15  
 MAC prefix, 4-15  
 RL2 packet forwarding, 4-15  
 help, 6-12  
 commonly asked questions, 6-14  
 humidity, A-3

**I**

image files, downloading, C-3  
 increasing wireless network performance, 6-11  
 installing the access point, 2-9, 2-10  
 obtaining help, 6-12  
 interference, definition, G-4  
 Internet packet exchange, *See* IPX  
 Internet protocol, *See* IP  
 IP address, 3-5, 4-5  
 definition, G-4  
 example of setting, 3-7, 4-7  
 setting, 2-15  
 IP, definition, G-4  
 IPX broadcast filters, 3-10, 4-10  
 IPX, definition, G-4

**J**

JANUS TCP/IP devices, using with access points, 1-5,  
 1-8, 1-9  
 JANUS UDP Plus devices, using with access points, 1-5

**K**

keyboard format conventions, xiv

**L**

LAN, definition, G-4  
 LEDs  
 front panel, 2-5  
 side panel, 2-6, 2-7

link down trap, 5-8  
 link quality, understanding, B-4  
 link up, 5-8  
 local area network, *See* LAN

**M**

MAC optimize, 3-14, 4-18  
 MAC prefix, 4-15  
 Main Menu  
 Configuration Menu, 2-8, 3-3, 3-7, 4-3, 4-7, 4-9  
 Diagnostics Menu, 2-8, 6-12  
 Download Menu, 2-8, C-3  
 Reset Access Point, 2-8, 2-19  
 Statistics Menu, 2-8, 6-3  
 Status Menu, 2-8, 6-7  
 understanding, 2-8  
 management access, A-4  
 management information base, *See* MIB  
 manual  
 format conventions for commands, xiv  
 format conventions for input, xiv  
 summary, xii  
 terms, xiv  
 manual supplement, 2-3  
 map token ring frame type to, 4-15  
 map token ring SNAP frame type to, 4-15  
 Master LED, 2-6, 2-7  
 master name, 3-14, 4-18  
 MAU, G-5  
 Media Access protocol, A-4  
 media access unit, *See* MAU  
 media supplies, phone number, ii  
 MIB, definition, G-5  
 MIB-II traps, 5-8  
 authorization, 5-8  
 cold start, 5-8  
 link down, 5-8  
 link up, 5-8  
 MIBs, supported by access point, 5-3  
 microwave ovens, 6-11  
 modems, using to configure, 2-10, 2-16  
 mounting options, 2-4  
 mounting the access point, 2-10, 2-12  
 Multi-Ring SR/TB mode, 4-12, 4-13  
 bridge number, 4-12  
 radio ring number, 4-12  
 token ring number, 4-12

**N**

narrow band, definition, G-5  
 network administrator, definition, G-5  
 Network LED, 2-5  
 network map, 5-10  
 no traffic trap, 5-8  
 no traffic trap period, 3-15, 4-19

notes, explanation of, xii  
null modem cable, 2-10, 2-15

## O

obtaining help with your installation, 6-12  
open token ring adapter, 4-21  
options  
    antennas, 2-4  
    cubicle-mount bracket, 2-4  
    environmental box, 2-4  
    power cord, 2-4  
    wall-mount bracket, 2-4  
OSI model, 1-3  
    definition, G-5  
out-of-band, 2-15

## P

packet, definition, G-5  
parameters, viewing on screen, 2-18, 6-7  
PC, using to configure, 2-10  
peer-to-peer network, definition, G-5  
peer-to-peer network, using access points, 1-13  
performing a standard installation, 2-10  
phone number, ii  
ping IP hosts, 6-13  
placing an antenna, 6-11  
plugging in the power supply, 2-13  
power cord, options, 2-4  
Power LED, 2-5  
power supply  
    connecting, 2-10  
    plugging in, 2-13  
protocol type filters, 3-9, 4-9

## Q

quick installation, considerations, 2-9

## R

radio broadcast trap threshold, 3-15, 4-19  
Radio Configuration Menu, 3-12, 4-16, 4-20  
    channel, 3-13, 4-17  
    delay radio reconfigure, 3-14, 4-18  
    domain, 3-13, 4-17  
    MAC optimize, 3-14, 4-18  
    master name, 3-14, 4-18  
    no traffic trap period, 3-15, 4-19  
    radio broadcast trap threshold, 3-15, 4-19  
    radio port administrative status, 3-12, 4-17  
    radio traffic trap threshold, 3-15, 4-19  
    repeating enabled, 3-14, 4-18  
    reset radio, 3-15, 4-19  
    security ID, 3-15, 4-19  
    station type, 3-14  
    subchannel, 3-13, 4-17  
Radio Diagnostics Menu, 6-13, B-3

radio high usage trap, 5-8  
Radio LED, 2-5  
radio port administrative status, 3-12, 4-17  
radio power output, A-3  
radio ring number, 4-12  
radio statistics, 6-6  
Radio Status Menu, 6-9  
radio traffic trap threshold, 3-15, 4-19  
radio type, A-3  
radio, power output, 1-4  
range, A-3  
read/write SNMP community, 5-4  
read/write SNMP manager IP address, 5-4  
read-only SNMP community, 5-4  
read-only SNMP manager IP address, 5-4  
repeating enabled, 3-14, 4-18  
repeating feature, 1-13  
report management, A-4  
Reset Access Point, 2-8, 2-19  
reset radio, 3-15, 4-19  
reset token ring adapter, 4-21  
resetting the access point, 2-19  
resetting the statistics, 6-6  
ring speed, 4-20  
RL2 packet forwarding, 4-15  
roaming, in a token ring network, 1-11  
roaming, using access points, 1-8  
router, definition, G-5  
RSSI, understanding, B-4  
running a broadcast site survey, B-3  
running a directed site survey, B-4

## S

safety information, xi  
security  
    setting the security ID, 3-17, 4-22  
    using the authorization table, 3-17, 4-22  
security ID, 3-15, 4-19  
    setting, 3-17, 4-22  
send BOOTP at boot time, 3-6, 4-6  
sequenced packet exchange, *See* SPX  
serial port down trap, 5-8  
serial port max data rate, A-4  
serial, definition, G-6  
server, definition, G-6  
setting the IP address, example, 3-7, 4-7  
setting the security ID, 3-17, 4-22  
shielded twisted pair cabling, *See* STP cabling  
side panel  
    10BaseT LED, 2-6  
    16 Mbps LED, 2-7  
    4 Mbps LED, 2-7  
    Master LED, 2-6, 2-7  
side panel, understanding, 2-6, 2-7  
simple network management protocol, *See* SNMP

- Single-Ring SR/TB mode, 4-13
    - token ring number, 4-13
  - site survey tools, 6-11
    - broadcast site survey, B-3
    - directed site survey, B-4
  - site survey tools, using, B-3
  - size, A-3
  - SNMP agent, A-4
  - SNMP Configuration Menu, 5-3
    - enable/disable authentication traps, 5-5
    - enable/disable SNMP, 5-4
    - read/write SNMP community, 5-4
    - read/write SNMP manager IP address, 5-4
    - read-only SNMP community, 5-4
    - read-only SNMP manager IP address, 5-4
    - SNMP trap community, 5-5
    - trap target address, 5-5
  - SNMP manager, using to configure, 2-10, 2-17, 5-3
  - SNMP supported authentication traps, 5-8
  - SNMP trap community, 5-5
  - SNMP traps, A-4
  - SNMP, definition, G-6
  - software upgrades, A-4
  - source route statistics menu, 6-7
  - Source Route Table, 6-11
  - specifications
    - architecture, A-4
    - channel, A-3
    - data rate, A-3, A-4
    - domain, A-3
    - electrical rating, A-3
    - Ethernet compatibility, A-4
    - Ethernet interfaces, A-4
    - ETSI testing, A-4
    - filtering rate, A-4
    - filters, A-4
    - frequency band, A-3
    - humidity, A-3
    - management access, A-4
    - Media Access protocol, A-4
    - radio power output, A-3
    - radio type, A-3
    - range, A-3
    - report management, A-4
    - serial port max data rate, A-4
    - size, A-3
    - SNMP agent, A-4
    - SNMP traps, A-4
    - software upgrades, A-4
    - temperature range, A-3
    - token ring interfaces, A-4
    - user authorization table, A-4
    - weight, A-3
    - wireless network management, A-4
  - spread spectrum, definition, G-6
  - SPX, definition, G-6
  - station type, 3-14
  - Statistics Menu, 2-8
    - bridge statistics, 6-6
    - Ethernet statistics, 6-6
    - filter statistics, 6-6
    - radio statistics, 6-6
    - reset statistics, 6-6
    - source route statistics menu, 6-7
    - TCP/IP statistics, 6-6
    - token ring statistics, 6-6
  - statistics, viewing on screen, 6-3
  - Status Menu, 2-8
    - Bridge Status Menu, 6-9
    - Forwarding Database table, 6-10
    - Radio Status Menu, 6-9
    - Source Route Table, 6-11
    - TCP/IP Status Menu, 6-10
    - Token Ring Status Menu, 6-10
    - viewing the parameters, 6-7
  - STP cabling, 2-4, 2-13
  - subchannel, 3-13, 4-17
  - subnet mask, 3-5, 4-5
  - subnet mask, definition, G-6
  - system requirements, 2-4
    - Ethernet cable drop, 2-4
    - PC with Telnet software, 2-4
    - terminal, 2-4
    - token ring cable drop, 2-4
- ## T
- TB mode, 4-14
  - TCP, definition, G-6
  - TCP/IP Configuration Menu, 3-5, 4-5
    - BOOTP server address, 3-6, 4-6
    - browser management, 3-6, 4-6
    - browser password, 3-6, 4-6
    - browser user name, 3-6, 4-6
    - default gateway address, 3-6, 4-6
    - IP address, 3-5, 4-5
    - send BOOTP at boot time, 3-6, 4-6
    - subnet mask, 3-5, 4-5
    - Telnet access, 3-6, 4-6
    - Telnet password, 3-6, 4-6
  - TCP/IP statistics, 6-6
  - TCP/IP Status Menu, 6-10
  - technical support
    - commonly asked questions, 6-14
    - phone number, ii
  - technical support parameters, 6-13
  - Telnet access, 3-6, 4-6
  - Telnet password, 3-6, 4-6
  - Telnet software, 2-10
    - using to configure, 2-15
  - temperature range, A-3

terms used in this manual, xiv  
TFTP, using to download new firmware, C-3  
Token Ring Configuration Menu  
  chart, 5-7  
  close token ring adapter, 4-21  
  contends for active monitor, 4-21  
  open token ring adapter, 4-21  
  reset token ring adapter, 4-21  
  ring speed, 4-20  
  token ring port administrative status, 4-20  
token ring interfaces, A-4  
token ring network, 1-4, 1-7  
  connecting, 2-10  
  connecting the access point, 2-13  
  roaming scenarios, 1-11  
  using STP cabling, 2-13  
  using UTP cabling, 2-13  
  viewing statistics, 6-3  
token ring number, 4-12, 4-13  
token ring port administrative status, 4-20  
token ring statistics, 6-6  
Token Ring Statistics Menu, chart, 6-5  
Token Ring Status Menu, chart, 6-8  
trademark information, ii  
traffic monitor, 5-10  
TRAKKER Antares TCP/IP terminals, using with access points, 1-5  
TRAKKER Antares UDP Plus terminals, using with access points, 1-5  
transmission control protocol, *See* TCP  
transmission range, 6-11  
trap target address, 5-5  
troubleshooting, commonly asked questions, 6-14

## U

unauthorized address trap, 3-18, 4-23  
unauthorized usage trap, 5-8  
understanding the front panel LEDs, 2-5  
understanding the Main Menu, 2-8  
understanding the side panel, 2-6, 2-7  
unpacking the access point, 2-3  
unshielded twisted pair cabling, *See* UTP cabling  
update authorization configuration of all APs, 3-18, 4-23  
upgrading multiple access points, C-4  
upgrading one access point, C-4  
upgrading the access points, C-3  
  using BOOTP/TFTP, C-3  
  using FTP, C-3  
  using TFTP, C-3  
  using Xmodem, C-3  
user authorization table, A-4  
using the antenna pointing tool, B-6  
using the authorization table, 3-17, 4-22  
UTP cabling, 2-4, 2-13

## V

viewing the download status, C-6  
viewing the parameters, 6-7  
viewing the statistics, 6-3

## W

wall-mount bracket, 2-4  
warranty information, xi  
Web browser  
  discover APs, 5-10  
  network map, 5-10  
  supported browsers, 5-9  
  traffic monitor, 5-10  
  understanding the device management options, 5-10  
  understanding the main screen, 5-9  
  understanding the network management options, 5-10  
  using to configure, 2-10, 5-9  
weight, A-3  
wired network, connecting to, 2-12  
wireless network management, A-4  
wireless networks  
  increasing performance, 6-11  
WLI Forum OpenAir radio, 1-4

## X

Xmodem, using to download new firmware, C-3