Aironet™

Wireless Communications, Inc.

Technical Reference Manual

Wireless Access Point for Ethernet and Token Ring

Products Supported: AP4500-E, AP4500-T, AP4800-E, and AP4800-T

DOC 710-004242-B0

Aironet Wireless Communications, Inc.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Aironet Wireless Communications, Inc. Information in this document is subject to change without notice. Aironet Wireless Communications, Inc. makes no representations or warranties with respect to the contents or use of this manual and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Printed in USA

DOC-710-004242-B0

Contents

Chapter 10 - Using Filters 10-1

Chapter 11 - Setting Up Event Logs 11-1

List of Figures

■ List of Tables

About the Technical Reference Manual

This manual covers the installation, configuration, control, and maintenance of your Aironet Access Point.

Please read **Chapter 1** - Installing the Aironet Access Point before attempting to install, or use the hardware and software described in this manual.

The technical reference manual is arranged as follows:

Chapter 1 - Installing the Aironet Access Point - Describes the physical installation of the Aironet Access Point.

Chapter 2 - Accessing the Console Port - Introduces you to the Console Port and shows you how to set up and configure the Console Port parameters.

Chapter 3 - Before You Begin - Provides you with an overview of the Configuration Menu and how to save and restore your configurations.

Chapter 4 - Configuring the Radio Network - Contains detailed procedures for configuring your Radio Network.

Chapter 5 - Configuring the Ethernet or Token Ring Port - Contains detailed procedures for configuring the Ethernet or Token Ring port.

Chapter 6 - Setting Network Identifiers - Outlines the procedures for setting the Aironet Access Point's Network Identifiers.

Chapter 7 - Configuring SNMP - Describes how to configure the Aironet Access Point for use with the Simple Network Management Protocol.

Chapter 8 - Viewing Statistics - Describes how to use the Statistics Menu to monitor the performance of the Aironet Access Point.

Chapter 9 - Setting Up the Association Table - Provides you with an introduction to the association process and detailed procedures for setting up the Aironet Access Point's Association Table.

Chapter 10 - Using Filters - Describes how to control the forwarding of multicast messages.

Chapter 11 - Setting Up Event Logs - Outlines the procedures for setting up Event Logs and lists the common error log messages received on the Aironet Access Point.

Chapter 12 - Performing Diagnostics - Provides you with detailed procedures for restarting your unit, returning to your default configuration and loading new firmware versions.

Appendix A - Aironet Access Point Specifications - Details the Aironet Access Point radio and physical specifications.

Appendix B - Console Menu Tree - Provides you with a listing of all menus, sub-menus and options contained in the Console Port.

Appendix C - SNMP Variables - Lists the SNMP variables supported by the Aironet Access Point.

Appendix D - Aironet Technical Support **-** Describes how to contact Aironet for technical support.

Typographical Conventions

When reading the technical reference manual, it’s important to understand the symbol and formatting conventions used in the documentation. The following symbols and formatting are used in the manual.

Convention	Type of Information
ⓘ	Indicates a note which contains important information set off from the normal text.
⚠	A caution message that appears before procedures which, if not observed, could result in loss of data or damage to the equipment.
Bold type	An action you must perform such as type or select.
`Monospaced font`	Information and menus that are visible on the Console Port screens.

Welcome to the Aironet Access Point

The Aironet Access Point provides transparent, wireless data communications between the wired LAN (and/or within the Wireless Infrastructure) and fixed, portable or mobile devices equipped with a wireless adapter employing the same modulation.

Data Transparency and Protocols

The Aironet Access Point transports data packets transparently as they move through the Wireless Infrastructure.

The Access Point is also protocol independent for all packets, except those either addressed specifically to the Access Point, or sent as multicast address packets.

Depending on the address, packets will be processed as follows:

- All packets, except those either addressed specifically to the Access Point or sent as multicast address packets, will be processed without examining the contents of the packet, and without regard to the protocol used.
- Packets addressed specifically to the Access Point will be examined by looking at the protocol header. If the protocol is recognized the packet will be processed.
- Multicast address packets will also be examined by looking at the protocol header, but will be processed whether the protocol is recognized or not.
- If protocol filtering is enabled then the appropriate parts of the packet will be examined.

Ethernet or Token Ring Compatibility

The Ethernet Access Point can attach directly to 10Base2 (Thinnet), 10Base5 (Thicknet) or 10BaseT (Twisted Pair) Ethernet LAN segments. These segments must conform to IEEE 802.3 or Ethernet Blue Book specifications.

The Token Ring Access Point can attach directly to Shielded Twisted Pair (STP) or Unshielded Twisted Pair (UTP) Token Ring LAN segments. These segments must conform to IEEE 802.5.

If the existing infrastructure to which the Access Point is to be attached is not Ethernet or Token Ring-based, an Ethernet or Token Ring segment can be added by installing an Ethernet or Token Ring Network Interface Card (NIC) in the File Server or by adding a third-party bridge.

The Access Point appears as an Ethernet or Token Ring node and performs a routing function by moving packets from the wired LAN, to remote workstations (personal computers, laptops and hand held computing devices) on the wireless infrastructure.

Remote Management Protocols Supported

Protocols supported:

- TCP/IP based protocol products
- SNMP Protocol - The resident agent is compliant with the MIB-I and MIB-II standards, TCP/IP based internets, as well as a custom MIB for specialized control of the system.

Radio Characteristics

The 4500 and 4800 Series uses a radio modulation technique known as Direct Sequence Spread Spectrum transmission (DSSS). It combines high data throughput with excellent immunity to interference. The Access Point operates in the 2.4 GHz license-free Industrial Scientific and Medical (ISM) band. Data is transmitted over a half-duplex radio channel operating at up to 2 Megabits per second (Mbps) rate (4500) or 11 Mbps rate (4800).

Radio Ranges

The following section provides general guidelines on factors that influence network performance.

Site Survey

Because of differences in component configuration, placement and physical environment, every infrastructure application is a unique installation. Before installing the system, users should perform a site survey in order to determine the optimum utilization of networking components and to maximize range, coverage and network performance.

Here are some operating and environmental conditions that need to be considered:

- **Data Rates.** Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. There will be a decrease in receiver threshold as the radio data rate increases.
- **Antenna Type and Placement.** Proper antenna configuration is a critical factor in maximizing radio range. As a general guide, range increases in proportion to antenna height. The Access Point allows connection to two antennas at the same time. This can be configured either as two separate remote antennas or as the single unit diversity antenna supplied by Aironet. Two antennas allow the Access Point to detect and use the strongest signal coming from either of the antennas.

For a detailed explanation of antenna types and configurations along with guidelines on selecting antennas for specific environments, see the Aironet Antenna Guide, document number 710-003725.

- **Physical Environments.** Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.
- **Obstructions.** A physical obstruction such as shelving or a pillar can hinder the performance of the Access Point. Avoid locating the computing device and antenna in a location where there is a barrier between the sending and receiving antennas.
- **Building Materials.** Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks.

Radio Antenna

The Access Point comes equipped with two dipole antennas that operate in diversity mode. Diversity antenna systems can improve reception in environments where multipath interference is a problem. Aironet’s direct sequence spread spectrum radios are designed to utilize a spacial diversity antenna system.

A benefit of a diversity system is improved coverage. At the edges of the RF coverage or fringe areas, there are very often multiple signals reaching the receiver, all from the same transmitter. These signals travel in different paths (multipath) and are caused by reflection and shadows of the RF signals. When the signals combine, the receiver may have trouble decoding the data. The Aironet radio’s ability to switch and sample between these antennas allows it to select the optimum antenna for receiving the packet.

Security Features

The Aironet Access Point employs Spread Spectrum Technology, previously developed for military “anti-jamming” and “low probability of intercept” radio systems.

The Aironet Access Point must be set to the same System Identifier (SSID) as all other Aironet devices on the wireless infrastructure. Units with a different SSID will not be able to directly communicate with each other.

Terminology

When configuring your system, and when reading this manual, keep in mind the following terminology:

Association - Each root unit or repeater in the infrastructure contains an association table that controls the routing of packets between the Access Point and the wireless infrastructure. The association table maintains entries for all the nodes situated below the Access Point on the infrastructure including repeaters and client nodes.

End Node - A client node that is located at the end of the Network Tree.

Infrastructure - The wireless infrastructure is the communications system that combines Access Points, mobile nodes, and fixed nodes. Access Points within the infrastructure can be either root units, which are physically wired to the LAN backbone, or can act as wireless repeaters. Other RF enabled devices serve as fixed nodes or mobile client nodes.

Parent/Child Node - Refers to the relationships between nodes in the wireless infrastructure. The complete set of relationships is sometimes described as a Network Tree. For example, the Access Point (at the top of the tree) would be the parent of the end nodes. Conversely, the end nodes would be the children of the Access Point.

Power Saving Protocol (PSP) and Non-Power Saving Protocol - The Power Saving Protocol allows computers (usually portable computers) to power up only part of the time to conserve energy. If a client node is using the Power Saving Protocol to communicate with the network, the Access Point must be aware of this mode and implement additional features such as message store and forward. If the client node is powered from an AC line, PSP should not be used.

Repeater - A repeater is an Access Point that extends the radio range of the infrastructure. A repeater is not physically attached to the wired LAN, but communicates via radio to another Access Point, which is either a root unit or another repeater.

Root Unit - The root unit is an Access Point that is located at the top, or starting point, of a wireless infrastructure. A root unit provides the physical connection to the wired LAN (such as Ethernet or Token Ring) and contains configuration information in its association table that covers all nodes that access the wired network. All Access Points directly attached to the wired LAN backbone are root units.

Access Point System Configurations

The Aironet Access Point can be used in a variety of infrastructure configurations. How you configure your infrastructure will determine the size of the microcell, which is the area a single Access Point will provide with RF coverage. You can extend the RF coverage area by creating multiple microcells on a LAN.

Examples of some common system configurations are shown on the pages that follow, along with a description of each.

Figure 0.1 - Wireless Workstations on LAN

One or more physically separated, wireless workstations — each equipped with an Aironet Wireless LAN Client Card — can link to the LAN to communicate with the file server, via an Aironet Access Point. Multiple repeater hops are supported in the path to the LAN.

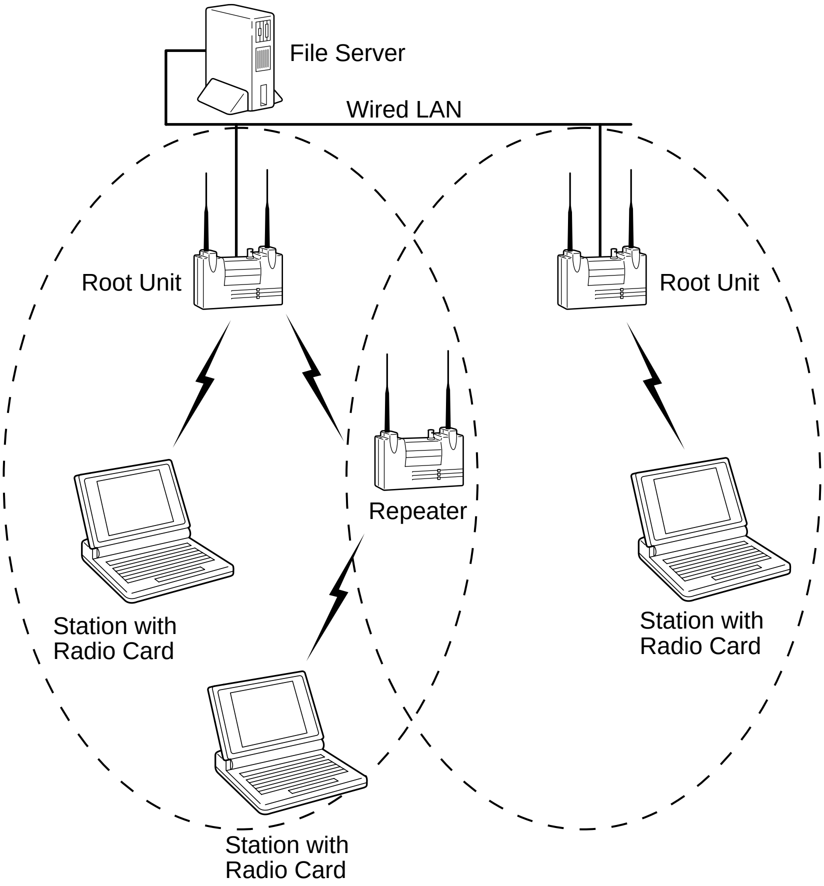


Figure 0.2 - Wireless LAN

In an all wireless LAN, the Aironet Aironet Access Point can operate as a stand-alone Access Point. In this configuration, the Aironet Access Point is not attached to the LAN, but functions as a hub, linking all workstations together.

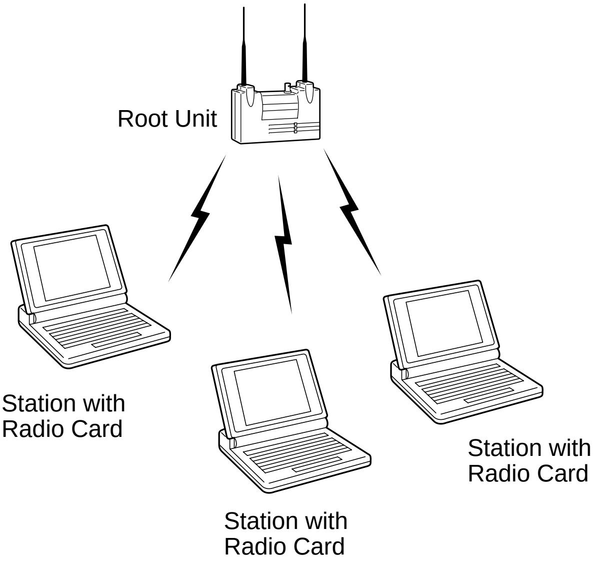
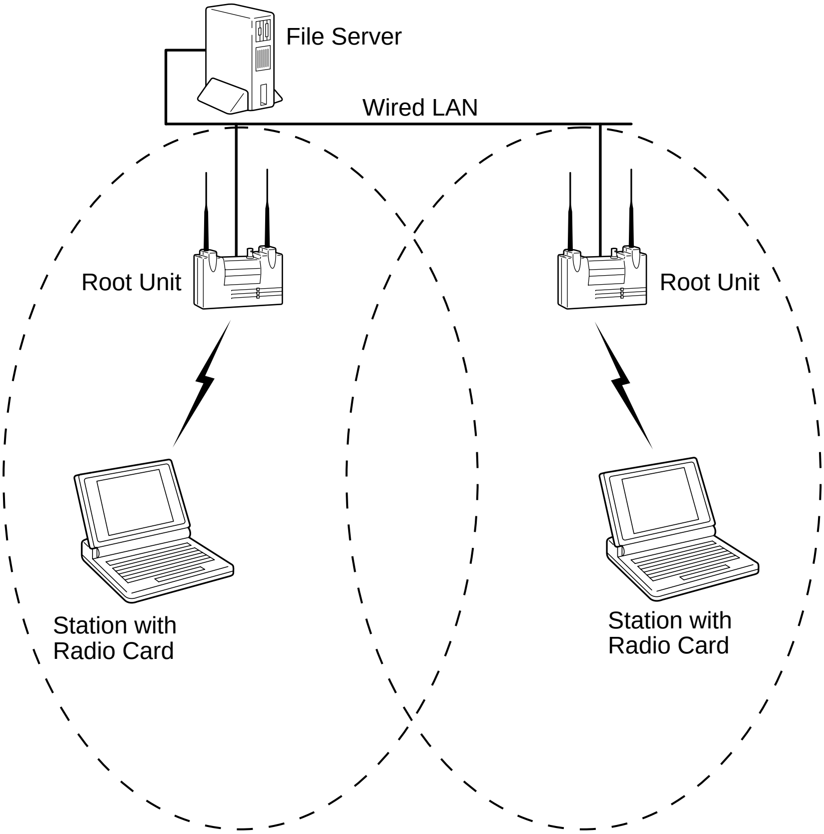


Figure 0.3 - Multiple Microcells On Cabled LAN

A Micro-Cellular Network can be created by placing two or more Aironet Access Points on the LAN. The Access Point's enhanced roaming protocols allow remote workstations to move from the domain of one microcell to another. The process is seamless and transparent, and the connection to the file server or host is maintained without disruption. This configuration is particularly useful with portable or mobile infrastructure workstations that move out of radio range of one Access Point and into the radio range of another.



1

CHAPTER 1

Installing the Access Point for Ethernet or Token Ring

This chapter describes the procedures for installing the Ethernet or Token Ring Access Point.

Here’s what you’ll find in this chapter:

- Before You Start
- Installation
- Attaching the AC/DC Power Pack and Powering On the Ethernet or Token Ring Access Point
- Viewing the Indicator Displays

Before You Start

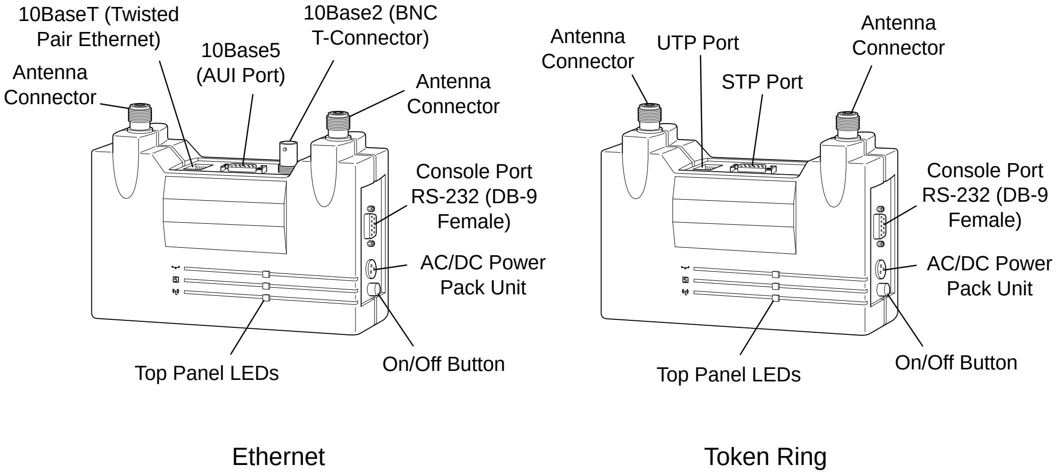
After unpacking the system, make sure the following items are present and in good condition:

- Access Point (Ethernet or Token Ring model)
- Power Pack. The power pack will be either 120VAC/60Hz or 90-264VAC/47-63Hz to 12-18VDC, whichever is appropriate for country of use.
- Two Standard 2 dBi Dipole Antennas

If any item is damaged or missing, contact your Aironet supplier. Save all shipping and packing material in order to repack the unit should service be required.

NOTE: Any remote antennas or associated coaxial cables are ordered and packed separately.

Figure 1.1 - Overview of the Ethernet or Token Ring Access Point



Installation

This section describes the procedures for installing the Aironet Access Point.

Installing the Antennas

The Access Point comes with two antennas.

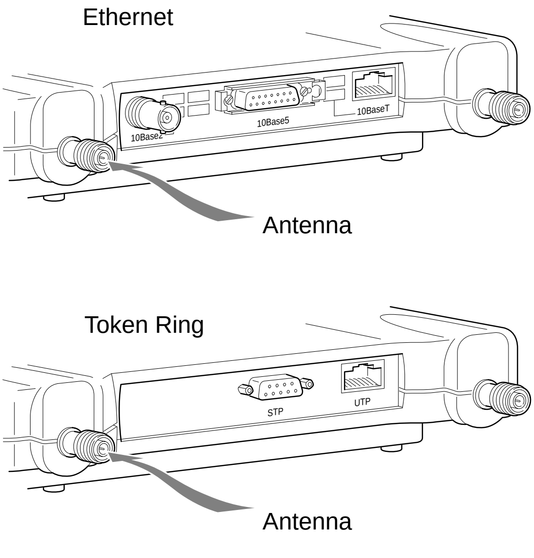
1. With the unit powered off, attach both antennas to the antenna connectors. (**Figure 1.2**)

NOTE: Do not over-tighten; finger tight is sufficient. Position the antennas vertically for best omni-directional signal reception.

2. If you are using the Access Point with a remote antenna, connect the coaxial cable to the antenna connector. Only use antennas and cables supplied by Aironet Wireless Communications.

NOTE: Due to FCC and DOC Regulations, the antenna connectors on the Access Point are of reverse polarity to the standard TNC connectors.

Figure 1.2 - Attaching the Antennas



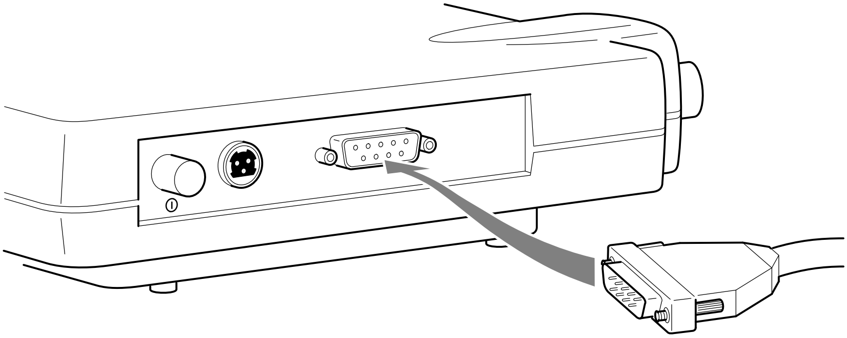
Installing the Console Port Cable

1. Attach the Console Port cable to the Serial Port. Attach the other cable end to the Serial Port on a terminal or a PC running a terminal emulation program. Use a 9-pin male to 9-pin female straight through cable (**Figure 1-3**).

NOTE: This connection is required for setting up initial configuration information. After configuration is completed, this cable may be removed until additional configuration is required via the Serial Port.

2. Set the terminal to **9600** Baud, **No**-Parity, **8** data bits, **1** Stop bit, and ANSI compatible.

Figure 1.3 - Console Port Connection



Installing the Ethernet Connection

NOTE: If you are installing a Token Ring Access Point, proceed to page 1-8.

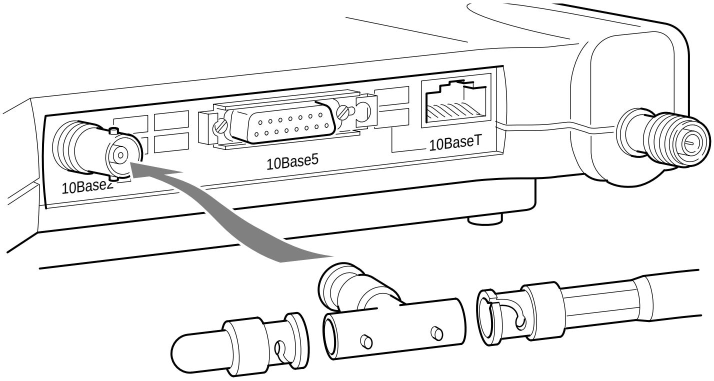
The Aironet Access Point for Ethernet supports three connection types:

- 10Base2 (Thinnet)
- 10Base5 (Thicknet) AUI connector
- 10BaseT (Twisted Pair)

➔ **To Attach 10Base2 (Thinnet) Cabling:**

1. Make sure the unit is powered off.
2. Attach the Thinnet cabling to each end of a BNC T-connector, if applicable.
3. Attach the T-connector to the 10Base2 BNC connector as shown in **Figure 1.4**. If the unit is at the end of the Ethernet cable, a 50-Ohm terminator must be installed on the open end of the T-connector.

Figure 1.4 - Attaching 10Base2 (Thinnet) Cabling

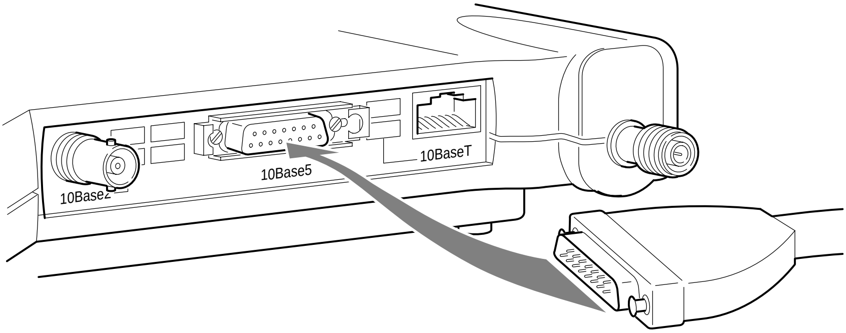


CAUTION: Removing a terminator to install extra cable, or breaking an existing cable to install a T-connector, will cause a disruption in Ethernet traffic. Consult with your LAN administrator before you change any Ethernet cabling connections.

➔ **To Attach the 10Base5 (Thicknet) Cabling:**

1. Make sure the unit is powered off.
2. Attach the transceiver connector to the 10Base5 AUI port as shown in **Figure 1.5**.
3. Slide the locking mechanism in place.
4. Attach the other end of the transceiver drop cabling to an external transceiver.

Figure 1.5 - Attaching 10Base5 (Thicknet) Cabling



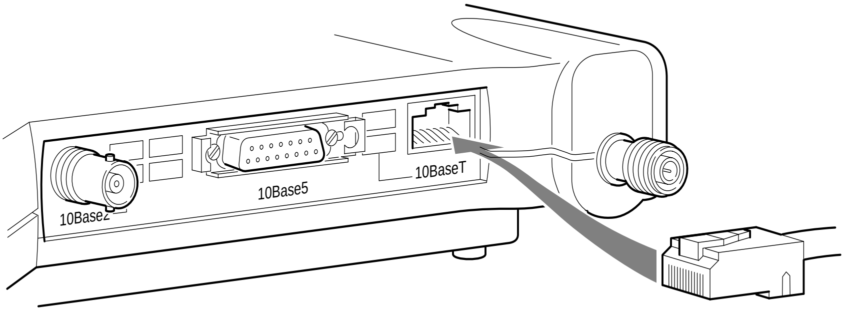
➔ To Attach the 10BaseT (Twisted Pair) cabling:

1. Make sure the unit is powered off.

2. Plug the RJ-45 connector into the 10BaseT (Twisted Pair) socket as shown in **Figure 1.6**.

3. Connect the other end of the Twisted Pair cabling to the LAN connection (such as a hub or concentrator).

Figure 1.6 - Attaching 10BaseT (Twisted Pair) Cabling



Installing the Token Ring Connection

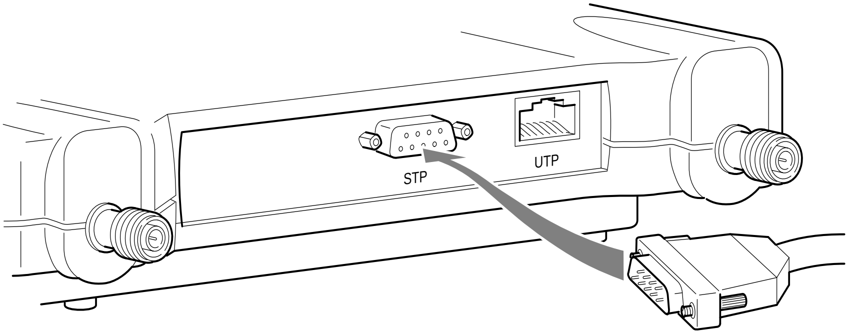
The Aironet Access Point for Token Ring supports two connection types:

- Shielded Twisted Pair (STP)
- Unshielded Twisted Pair (UTP)

➔ **To Attach STP (Shielded Twisted Pair) Cabling:**

1. Make sure the unit is powered off.
2. Attach the transceiver connector to the DB-9 port.
3. Attach the other end of the transceiver drop cabling to a Token Ring Multi-Station Access Unit (MAU).

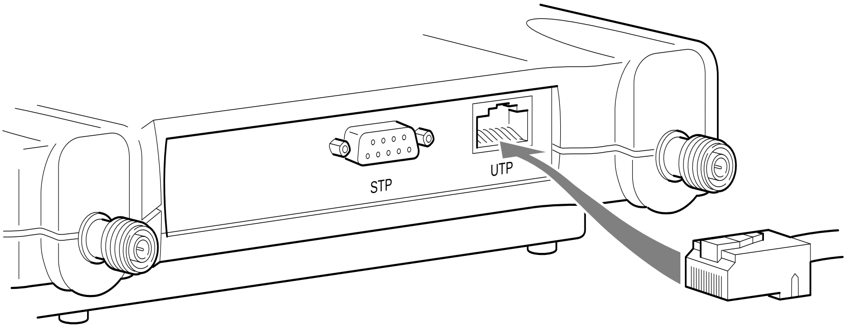
Figure 1.7 - Attaching STP (Shielded Twisted Pair) Cabling



➔ **To Attach the UTP (Unshielded Twisted Pair) Cabling:**

1. Make sure the unit is powered off.
2. Plug the RJ-45 connector into the UTP port.
3. Connect the other end of the UTP cabling to a Token Ring Multi-Station Access Unit (MAU).

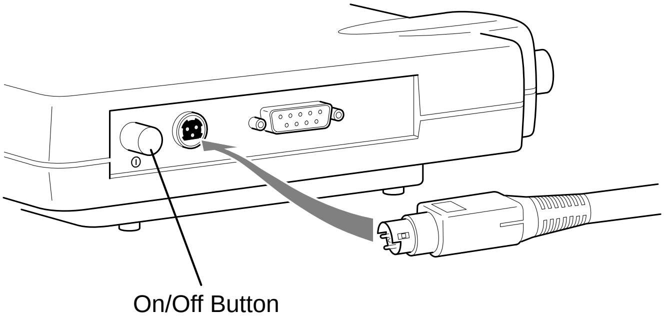
Figure 1.8 - Attaching UTP (Unshielded Twisted Pair) Cabling



Attaching the AC/DC Power Pack and Powering On the Ethernet or Token Ring Access Point

1. Insert the small plug on the end of the AC/DC power pack cord into the power port.
2. Plug the AC/DC power pack into an electrical outlet. (120VAC/60Hz or 90-264VAC/47-63Hz as appropriate)
3. Power on the Access Point by pushing the On/Off button as shown in **Figure 1.9**.

Figure 1.9 - AC to DC Power Pack Connections and On/Off Button



When power is initially applied to the Aironet Access Point, all three indicators will blink in sequence to test the functionality of the indicators.

Viewing the Indicator Displays

Top Panel Indicators

The indicators are a set of displays located on the top panel of the Access Point unit.

- **Ethernet or Token Ring Indicator** – Used to indicate infrastructure traffic activity. The light is normally off, but will blink green whenever a packet is received or transmitted over the Ethernet or Token Ring interface.
- **Status Indicator** – Shows solid green when the Aironet Access Point has accepted a radio association.
- **Radio Indicator** – Used to indicate radio traffic activity. The light is normally off, but will blink green whenever a packet is received or transmitted over the radio.

When the Access Point is initially powered up, all three displays will blink amber, red and then green, in sequence. If a power-on test fails, the status indicator will go solid red and the unit will stop functioning. See **Table 1.1** for a detailed explanation of the Top Panel indicators.

Figure 1.10 - Top Panel Indicators

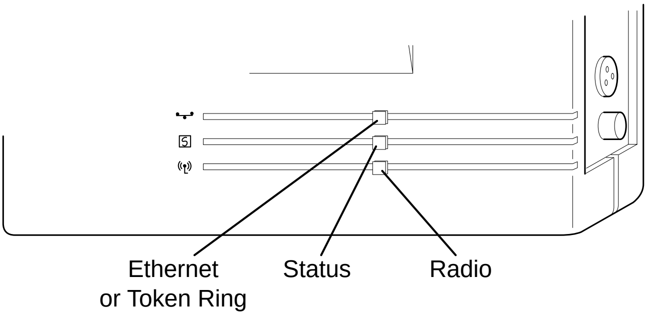


Table 1.1 - Top Panel Indicator Description

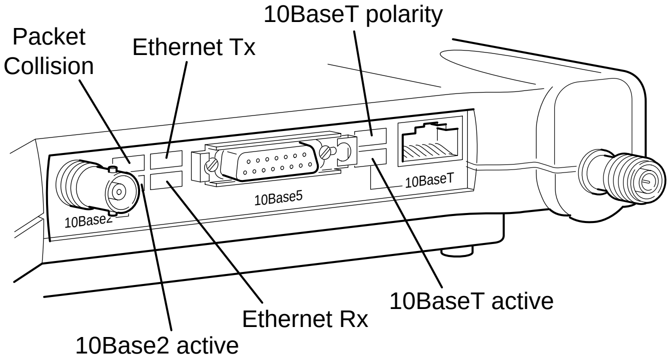
Type	Indicator Display			Description
	Ethernet or Token Ring	Status	Radio	
Nonassociated Node		Blinking Green		No nodes associated
Operational		Green		One or more nodes associated
		Green	Blinking Green	Transmitting/Receiving wired LAN traffic
	Blinking Green	Green		Transmitting/Receiving Radio packets
Error/Warning		Green	Blinking Amber	Maximum retries/buffer full occurred on radio
	Blinking Amber	Green		Transmit/Receive errors on the wired LAN
		Blinking Amber		General warning, check the logs
Failure	Red	Red	Red	Software failure
Firmware Upgrade		Red		Flashing the firmware

Back Panel Indicators (Ethernet Only)

The back panel indicators shown in **Figure 1.11** are:

- **10BaseT polarity**: Solid amber to indicate the 10BaseT polarity is reversed. Check cable connections.
- **10BaseT active**: Solid green to indicate the 10BaseT has been configured as the active port.
- **Ethernet Rx**: Blinks green when an Ethernet packet has been received.
- **Ethernet Tx**: Blinks green when an Ethernet packet has been transmitted.
- **10Base2 active**: Solid green to indicate the 10Base2 has been configured as the active port.
- **Packet Collision**: Blinks amber to indicate a packet collision has occurred.

Figure 1.11 - Back Panel Indicators



2

CHAPTER 2

Accessing the Console System

This chapter describes the methods used to access the Console system of the Aironet Access Point. This system contains all commands necessary to configure and monitor the operation of the unit.

Here’s what you’ll find in this chapter:

Access Methods

There are many ways in which you may configure and monitor the Aironet Access Point. When the unit is powered up, basic configuration must initially be performed by accessing the Console Serial Port. To gain access through the Serial Port, the Aironet Access Point must be connected to a terminal or a PC running a terminal emulation program. See **Chapter 1** “Installing the Aironet Access Point for Ethernet or Token Ring”. Set the terminal to **9600** Baud, **No**-Parity, **8** data bits, **1** stop bit, and ANSI compatible.

Once the Aironet Access Point has been assigned an IP address, you may then access the Console remotely using:

- Telnet protocol from a remote host or PC
- HTML browser, such as Netscape Navigator from a remote host
- Simple Network Management Protocol (SNMP) from a remote network management station

Using the Console

The Console system is organized as a set of menus. Each selection in a menu list may either take you to a sub-menu or display a command that will configure or display information controlling the unit.

When the Aironet Access Point is powered up, the Main Menu will be displayed.

```
                          Main Menu
    Option             Value       Description
1 - Configuration  [ menu  ]   - General configuration
2 - Statistics     [ menu  ]   - Display statistics
3 - Association    [ menu  ]   - Association table maintenance
4 - Filter         [ menu  ]   - Control packet filtering
5 - Logs           [ menu  ]   - Alarm and log control
6 - Diagnostics    [ menu  ]   - Maintenance and testing commands
7 - Privilege      [ write ]   - Set privilege level
8 - Help                       - Introduction

Enter an option number or name
>
```

Each menu contains the following elements:

- **Title Line**: Contains the product name, firmware version and menu name. It also contains the unique name assigned to the unit. See **Chapter 6** “Setting Network Identifiers”.
- **Option Column**: Displays the menu options and option number.
- **Value Column**: Displays either the value as [menu] or displays the current settings for the option. If the value is [menu], there are additional sub-menus available.
- **Description Column**: Provides a brief description of each option on the menu.
- **Enter an Option Number or Name** >: The cursor prompt used to enter option numbers, names, or commands.

To select an item from the menu you may either enter the number displayed beside the selection, in which case you are immediately taken to the selection, or you may type the name listed in the option column followed by a carriage return. If you use the name method, you only need to enter enough characters to make the name unique from the other selection names in the menu.

When you are entering names or command information you may edit the selection by using the **BACKSPACE** character to delete a single character or the **DELETE** character to delete the entire line.

Sub-Menus

If the selection you chose was a sub-menu, the new menu will be displayed. You may now either choose a selection from this menu or return to the previous menu by pressing the **ESCAPE** key**.** If you want to return to the Main Menu, type the **equal key (=)** at the menu prompt.

Commands and Information

If your selection is a command you may be prompted for information before it executes. Information may be one of the following types:

- **Token**: A list of one or more fixed strings. To select a particular token, you need only enter enough of the starting characters of the token to allow it to be uniquely identified from the characters of the other tokens in the list.

  ```
  Enter one of {off, readonly, write] : w
  ```

  You would need only enter: “o”, “r”, or “w” followed by a carriage return.

- **String**: An arbitrary amount of characters. The prompt will indicate the allowable size range of the string.

  ```
  Enter a name of from 1 to 10 characters: “abc def”
  ```

  If the string contains a space, enclose the string in quotation marks. If you wish to enter an empty string, use two quotation marks with nothing between them.

- **Integers**: A decimal integer. The prompt will indicate the range of allowed values.

  ```
  Enter a size between 1 and 100 : 99
  ```

  hexadecimal integer – a number specified in hexadecimal using the characters 0-9 and a-f or A-F.

  ```
  Enter a hex number between 1h and ffh : 1a
  ```

- **Network address**: An infrastructure or MAC level address of 12 characters or less. Omit leading zeros when entering an address.

  ```
  Enter the remote network address : 4096123456
  ```

- **IP address**: An internet address in the form of 4 numbers from 0-255 separated by dots (.). Leading zeros in any of the numbers may be omitted.

  ```
  Enter an IP address : 192.200.1.50
  ```

Once all information has been entered the command will execute. If the information entered changed a configuration item, the new value will be displayed in the menus.

Some configuration commands only allow the choice between two fixed values. When the menu item is selected, the opposite value to the current value is chosen. For example, if the configuration item is only a selection between on and off, and the current value is on, then selecting the menu option will select the off value.

Some commands which have a severe effect on the operation of the unit (such as the restart command) will prompt to be sure you want to execute the command.

```
Are you sure [y/n] :
```

If you enter anything other than a “y” or a “Y” the command will not be executed.

If you are being prompted for information, you may cancel the command and return to the menu by typing **ESCAPE**.

Commands That Display Information

There are several types of commands that display information to the operator. All displays end with a prompt before returning back to the menus. If nothing is entered at the prompt for 10 seconds, the display will automatically refresh.

- Single page non-statistical displays end with the following prompt.

  ```
  Enter space to re-display, q[uit] :
  ```

  Any character other than **space** will cause the display to exit.

- Single page statistical displays end with the following prompt.

  ```
  Enter space to re-display, C[lear stats], q[uit] :
  ```

  Entering a “C” (capital) will reset all statistics to zero.

- Multiple page table displays end with the following prompt.

  ```
  Enter space to redisplay, f[irst], n[ext], p[revi-
  ous], q[uit] :
  ```

  Parts of the prompt may or may not be present depending on the display. If you are not at the first page of the display, you may enter “f” to return to the first page or “p” to return to the previous page. If you are not at the last page you may enter “n” to go to the next page.

Command Line Mode

Another way to move within the Console is to enter commands directly from the Main Menu. Commands allow you to bypass the menu system and go directly to any level sub-menu or option. Enter the list of sub-menus, command names, and information separated by space characters.

Example 1: To access the Radio Configuration Menu (located two sub-menus down):

1. At the Main Menu prompt type:

   ```
   configuration radio
   ```

2. Press **ENTER**. The Radio Configuration Menu appears.

Example 2: To access the packet size option from the Radio Link Test Menu (located three sub-menus down):

1. At the Main Menu prompt type:

   ```
   configuration radio linktest size 25
   ```

2. Press **ENTER** and the Main Menu is re-displayed.

Telnet Access

Once the Aironet Access Point has been assigned an IP address and connected to the infrastructure, you may connect to the Console system from a remote PC or host by executing the telnet command.

Once the connection has been made, the Main Menu will appear. The Main Menu functions the same for both telnet access and Serial Port connections.

While a telnet session is in progress, you may not use the Console Port to gain access to the menus. If any characters are entered, the following message is printed identifying the location of the connection.

```
Console taken over by remote operator at 192.200.1.1
<use BREAK to end>
```

If you enter a break sequence, the remote operator will be disconnected and control of the Console is returned to the Console Port.

You may disable telnet access to the Aironet Access Point with a menu configuration command. See “Enabling Telnet or HTTP Connections (Telnet or HTTP)”.

NOTE: If you are leaving telnet enabled, make sure you set passwords to secure the Console. See “Setting Privilege Levels and Passwords (Rpassword, Wpassword)”.

Web Access

The Aironet Access Point supports access to the Console system through the use of an HTML browser. To start a connection use:

```
http://ip address of Aironet Access Point/
```

A typical menu will be displayed:

```
                    Association Menu
     Option        Value     Description
    Display                  Display the table
    Summary                  Display the table summary
    Monitor        [menu]    Monitor network associations
    Maximum        [1024]    Maximum allowed child nodes
    Autoassoc      [ on ]    Allow automatic table additions
    Add                      Control node association
    Remove                   Remove association control
    Niddisp       [numeric]  Node Ids display mode

    Enter an option number or name, “=” main menu, <ESC> previous menu
    >_
```

- **Option**: Contains the menu selections as a list of hyper-links. If the selection is a sub-menu, the selection name will end with the word “Menu”.
- **Value**: Displays the current value of configured items.
- **Description**: Explains the menu selection.

The bottom of each menu page contains hyper-links to immediately return to the Main Menu or previous menus.

To select a menu item, click with the mouse or select a link with the required keyboard commands. If the selection is a sub-menu, the new menu will display. If the selection is a command, it will prompt for information on separate pages.

When entering information, fixed tokens may be selected by clicking on the hyper-link associated with the token. All other types of information must be entered in dialogue boxes. The command execution may be aborted from any prompt by selecting the <abort> hyper-link at the bottom of each page.

For those commands that display pages of information, the prompts function the same as those on the Console Port, except instead of having to type characters to select the different options, the option is a hyper-link.

You may disable web access to the Aironet Access Point with a menu configuration command. See “Enabling Telnet or HTTP Connections (Telnet or HTTP)”.

NOTE: If you are leaving web access enabled, make sure that you set passwords to secure the Console. See “Setting Privilege Levels and Passwords (Rpassword, Wpassword)”.

About the Menus

Perform the following general functions using menus:

- **Configuration**: Allows you to configure Ethernet or Token Ring and Radio Parameters, establish Network Identifications, and set SNMP values. See **Chapters 3-7**.
- **Statistics**: View a variety of statistical information such as transmit and receive data throughput, Ethernet or Token Ring and radio errors, and the general status of the Aironet Access Point unit. See **Chapter 8** “Viewing Statistics”.
- **Association Table**: A table that contains the addresses of all radio nodes associated below the Aironet Access Point on the infrastructure. You may use the association table to display, add and remove static entries, and allow automatic additions to the table. See **Chapter 9** “Setting Up the Association Table”.
- **Filter**: Controls packet filtering. The filter menu allows you to control forwarding of multicast messages by blocking those multicast addresses and protocols that are not used on the radio network. See **Chapter 10** “Using Filters”.
- **Logs**: Keeps a record of all events and alarms that occur on the unit. With the Logs Menu, you can view and/or print a history of all log entries, set alarm levels, and determine the type of logs you want to save. See **Chapter 11** “Setting Up Event Logs”.
- **Diagnostics**: Allows you to run link tests between the Aironet Access Point and other infrastructure nodes to test the quality of the radio link. Use the Diagnostics function to load new code versions of the Aironet Access Point’s firmware. See **Chapter 12** “Performing Diagnostics”.
- **Privilege**: Allows you to set privilege levels and passwords to restrict access to the Console Port’s menus and functions.
- **Help**: A brief help screen outlining the procedures for accessing menus and entering commands.

Using the Configuration Console Menu

The Console system is configured using the Configuration Console Menu shown below. To access this menu, select **Configuration** from the Main Menu then select **Console** from the Configuration Menu.

```
                   Configuration Console Menu
          Option          Value        Description
      1 - Type          [ teletype ]   - Terminal type
      2 - Port          [   menu   ]   - Port set-up
      3 - Rpassword                    - Set readonly privilege password
      4 - Wpassword                    - Set write privilege password
      5 - Linemode      [   off    ]   - Console expects complete lines
      6 - Remote        [   menu   ]   - Control remote access

      Enter an option number or name, "=" main menu, <ESC> previous menu
      >_
```

Setting the Terminal Type (Type)

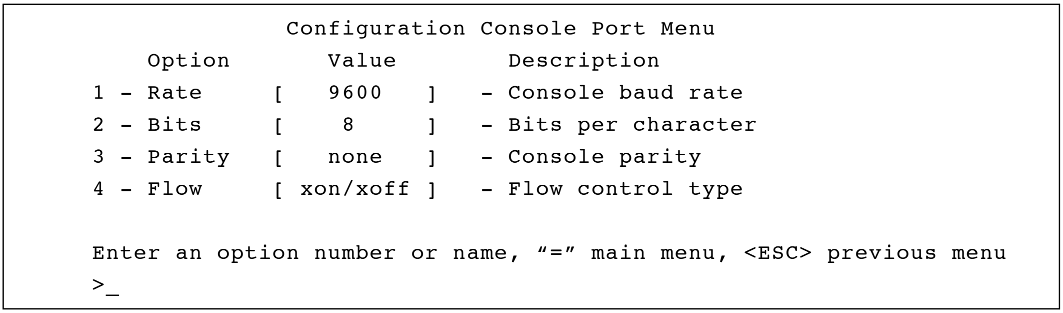
The terminal type may be set to Teletype (TTY) or ANSI using the Configuration Console Menu.

If the terminal or emulation program you are using supports the ANSI escape sequences, you should use ANSI.

- **Teletype mode**: Displays text with little or no formatting. Screens are not cleared prior to new screens appearing.
- **ANSI mode**: Provides text in a formatted manner. In addition, the screen will be cleared before each new screen is displayed.

Setting the Communication Port Parameters (Port)

Use the *port* option to set the following Aironet Access Point port communication parameters: Baud Rate, Data Bits, Parity, and Flow. When the *port* option is selected, the Configuration Console Port Menu appears. Any changes are effective immediately.



```
                Configuration Console Port Menu
      Option       Value         Description
  1 - Rate      [   9600   ]   - Console baud rate
  2 - Bits      [    8     ]   - Bits per character
  3 - Parity    [   none   ]   - Console parity
  4 - Flow      [ xon/xoff ]   - Flow control type

  Enter an option number or name, "=" main menu, <ESC> previous menu
  >_
```

- Baud rate selections include 300, 1200, 2400, 9600, 19200, 38400, 56800, or 115200 bits per second.
- Character size selection may be: 7 or 8 bits per character.
- Parity may be: even, odd, or none.
- Flow control selections include:

  Off: No flow control. Input or output may be lost if the Aironet Access Point cannot handle inputs or outputs from your terminal quickly enough.

  Xon/Xoff: The Aironet Access Point will use ASCII Xon/Xoff characters to control the input received from your terminal to prevent input buffer overflow. The unit will also control its output of characters to the terminal.

  Hardware: The Aironet Access Point will use the RTS and CTS lines to control the flow of characters. The Aironet Access Point sends characters while RTS is high, and will assert CTS when the terminal is allowed to send. This mode is used for flow control by passing the Xon/Xoff characters. Make sure the DTR signal is also present on the cable. See “Monitoring of the DTR Signal”.

  Both: Uses both hardware and Xon/Xoff flow control.

Setting Privilege Levels and Passwords (Rpassword, Wpassword)

You can restrict access to the menus by setting privilege levels and passwords. Privilege levels are set from the Main Menu. Passwords are set from the Configuration Console Menu.

There are three privilege levels contained in the Console Port:

- **Logged Out Level (Off)**: Access denied to all sub-menus. Users are only allowed access to the *privilege* and *help* options of the Main Menu.
- **Read-Only Level (Readonly)**: Read-only privileges for all submenus. Only those commands that do not modify the configuration may be used.
- **Read-Write Level (Write)**: Allows users complete read and write access to all sub-menus and options.

Keep in mind the following when setting Privilege Levels and Passwords:

- Only Read-Only and Read-Write privilege levels can be password protected.
- You can always go from a higher privilege level to a lower privilege level without a password. If you try to go to a higher privilege level, you will be required to enter the password.
- Passwords are upper/lower case sensitive.

➔ To Set a Privilege Level:

1. Select **Privilege** from the Main Menu.

   ```
   Enter one of [off, readonly, write] :
   ```

2. Type the first letter of your selection and press **ENTER**.

➔ To Set a Password:

1. Select **Configuration** from the Main Menu.
2. Select **Console** from the Configuration Menu.
3. Select the appropriate password option from the Configuration Console Menu.

   ```
   Enter one of [none, a password of between 5 and 10 char-
   acters] :
   ```

   - **Rpassword**: For Read-Only privilege
   - **WPassword**: For Read-Write privilege
   - **None**: Enter this text string if no password is needed

4. Type your password and press any key.

   ```
   Enter the password again, one of [none, a password of
   between 5 and 10 characters] :
   ```

5. Retype your password for confirmation.

NOTE: After a privilege level has been assigned, anyone attempting to access that level will be prompted for the password. This allows you to set various privilege levels for individuals, providing them with access to some options, while denying them access to others. Remember passwords are case sensitive. If an incorrect password is entered, the console will pause briefly before reprompting. If connected via telnet, the connection will be dropped after three consecutive failures and a severe error log will be displayed.

CAUTION: Make sure you write down the passwords you have established and keep them in a safe place. If you forget your password, the unit will have to be returned for factory servicing. Please contact Aironet Technical Support for further instructions.

Enabling Linemode (Linemode)

Enable *linemode* when working with telnet and terminal emulators that do not send characters when typed, but rather save them until the operator presses the carriage return at the end of a line.

The Console will not automatically complete any typed commands or information when a space or carriage return is inserted.

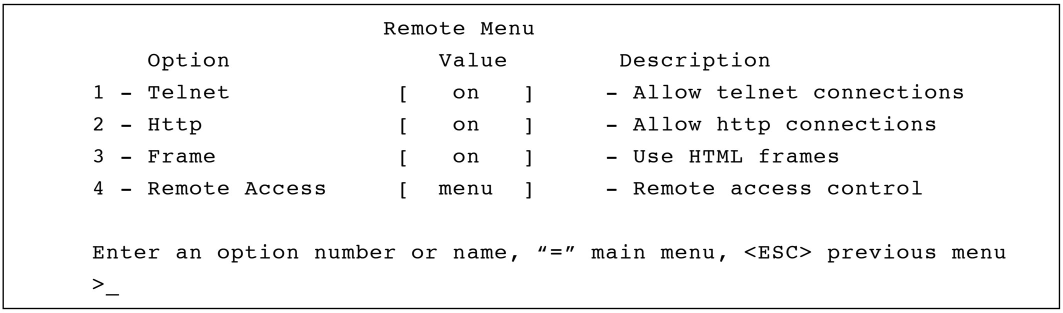
To enable linemode:

1. Select **Configuration** on the Main Menu.
2. Select **Linemode** on the Configuration Console Menu.
3. Enter “On” to enable line mode.

NOTE: Some telnet programs will automatically invoke linemode by sending the appropriate telnet commands when they connect to the Aironet Access Point.

Using the Remote Menu

When the *remote* option is selected, the Remote Menu appears.



```
                           Remote Menu
          Option                  Value         Description
      1 - Telnet              [    on    ]      - Allow telnet connections
      2 - Http                [    on    ]      - Allow http connections
      3 - Frame               [    on    ]      - Use HTML frames
      4 - Remote Access       [   menu   ]      - Remote access control

      Enter an option number or name, "=" main menu, <ESC> previous menu
      >_
```

Enabling Telnet or HTTP Connections (Telnet or HTTP)

Any node on the infrastructure (or radio) that supports the telnet protocol may connect to the Console Port. Also any node on the infrastructures that can run a Web browser may access the Console menus. See “Telnet Access” and “Web Access”.

Enabling Frames (Frame)

Any node on the infrastructure (or radio) that supports HTML frames may connect to the Console Port.

Using the Remote Access Control Menu

The Remote Access Control Menu is used to restrict remote access to a list of specific hosts. The list controls access to the Access Point via telnet, HTTP, or FTP. SNMP access is controlled separately on the Configuration SNMP Menu.

If the list is empty, any host in the infrastructure is allowed to attempt to connect. When the appropriate password is provided, the connection is allowed. If the list contains entries, any host not on the list will not be allowed access. An entry in the list may be specified as either an IP address or a MAC address.

```
                     Remote Menu
    Option       Value           Description
1 - Display                    - Display the remote host list
2 - Add                        - Add a remote host
3 - Remove                     - Remove a remote host

Enter an option number or name, “=” main menu, <ESC> previous menu
>_
```

Displaying a Host List (Display)

Use the *host* option to display the list of remote hosts.

Adding a Remote Host (Add)

Use the *add* option to add a host the remote host list. You will be prompted for the name of the host to add.

Removing a Remote Host (Remove)

Use the *remove* option to remove a host from the remote host list. You will be prompted for the name of the host to remove.

Monitoring of the DTR Signal

The Aironet Access Point monitors the state of the Data Terminal Ready (DTR) signal. This signal is used to indicate the presence or absence of a DTE device connected to the Console Port.

If the state of the signal changes (up or down) the following actions will occur (unless a telnet session is in progress):

- Any currently executing command or display will be terminated
- Current menu will be returned to the Main Menu
- Console Privilege Menu will be set back to the highest level not requiring a password.

If the Console is configured for hardware flow control and the DTR signal is currently down, all output will be discarded. The Aironet Access Point would assume flow is off and the Console would eventually lock up.

If the cable used does not have the DTR signal connected it will not change state and no action will be taken.

3

CHAPTER 3

Before You Begin

This chapter provides a general introduction to the Configuration Menu and describes the procedures for saving and restoring your configurations. See **Chapters 4 - 10** for more information on configurations.

Here's what you'll find in this chapter:

- Viewing the Configuration Menu
- Menu Descriptions
- Saving Configuration Parameters
- Backing up your Configuration
- Restoring your Configuration

Viewing the Configuration Menu

Once you have completed the installation, the next step is to use the Configuration Menu commands to configure the Aironet Access Point.

To access the Configuration Menu, select **Configuration** from the Main Menu.

```
                 Configuration Menu
       Option        Value      Description
   1 - Radio       [ menu ]   - Radio network parameters
   2 - Ethernet/   [ menu ]   - Ethernet or Token Ring configuration
       Token Ring
   3 - Ident       [ menu ]   - Identification information
   4 - Console     [ menu ]   - Console set-up
   5 - Snmp        [ menu ]   - Set snmp values
   6 - More        [ menu ]   - More items
   7 - Dump                   - Dump configuration to console

   Enter an option number or name, "=" main menu, <ESC> previous menu
   >_
```

Menu Descriptions

Radio: Used to set radio network parameters, such as system ID, frequency, and bitrate. See **Chapter 4** “Configuring the Radio Network”.

Ethernet or Token Ring: Used to set the Ethernet or Token Ring Parameters See **Chapter 5** “Configuring the Ethernet or Token Ring Port”.

Ident: Used to set various infrastructure identifiers such as Node Names, Network ID, and Internet Address. See **Chapter 6** “Setting the Network Identifiers”.

Console: Used to set up the Console Port. See **Chapter 2** “Accessing the Console System”.

Snmp: Used to configure the Aironet Access Point for use with the Simple Network Management Protocol. See **Chapter 7** “Configuring SNMP”.

More: Used to configure vendor specific items.

Dump: Used to dump the configuration commands to the Console Port. See “Backing up your Configuration (Dump)”.

Saving Configuration Parameters

Although there is no explicit save command, your configuration parameters are automatically saved to non-volatile flash memory each time a parameter is set or modified. This will ensure the configuration is maintained during power failures or intentional power downs.

Most configuration settings become effective as soon as the command is executed. Those that do not immediately become effective will be noted in the command information.

Backing up your Configuration (Dump)

Once you have set the configuration parameters for the Aironet Access Point, use the *dump* option to dump the configuration commands to the Console Port and save them as an ASCII file on a diskette, using a PC terminal emulation program.

If the non-volatile flash memory should ever become corrupted (and you lose your saved configuration), you can use a communications program to send the configuration commands to the Console Port. The system will automatically restore your configuration based on these commands.

➔ **To Back Up Configurations:**

NOTE: Commands may vary depending on the communications program used.

1. In the terminal emulation program, set Save to File to **On**.
2. Select **Configuration** from the Main Menu then select **Dump**. The following message appears:

```
Enter one of [all, non-default, distributable]:
```

- **All**: The entire configuration will be displayed.
- **Non-default**: Only the configuration options that are different from the original default settings will be displayed.
- **Distributable**: Only the configuration options that are not considered unique to this unit are displayed. You may use the “diagnostics load distribute” command to send this configuration to other units in the network.

3. Enter one of [standard, encoded] :

   - **Standard**: The configuration is displayed in normal readable text form.
   - **Encoded**: The configuration is displayed with each configuration command replaced by a unique number. This type of configuration is the best to save since the number will never change over the life of the product. Text may change or move as more items are added to the menus. The configuration commands will now appear on the screen.

4. Enter your configuration command choice.
5. Save the file after the commands have been dumped.
6. Turn Save to File to **Off**.
7. Press any key to clear the screen.

Restoring your Configuration

If your configuration is ever lost or corrupted, you can restore your configuration using the program’s ASCII upload commands.

4

CHAPTER 4

Configuring the Radio Network

This chapter describes the procedures for configuring the Aironet Access Point Radio Network.

Here's what you'll find in this chapter:

Overview

When configuring the radio network, all units should be configured while in close proximity to each other. This will allow your units to communicate with other radio nodes on your infrastructure as the units' parameters are set.

Once configuration is complete, the units can then be moved to their permanent location. Tests can be run to check the reliability of the radio links. See "Running a Link Test (Linktest)".

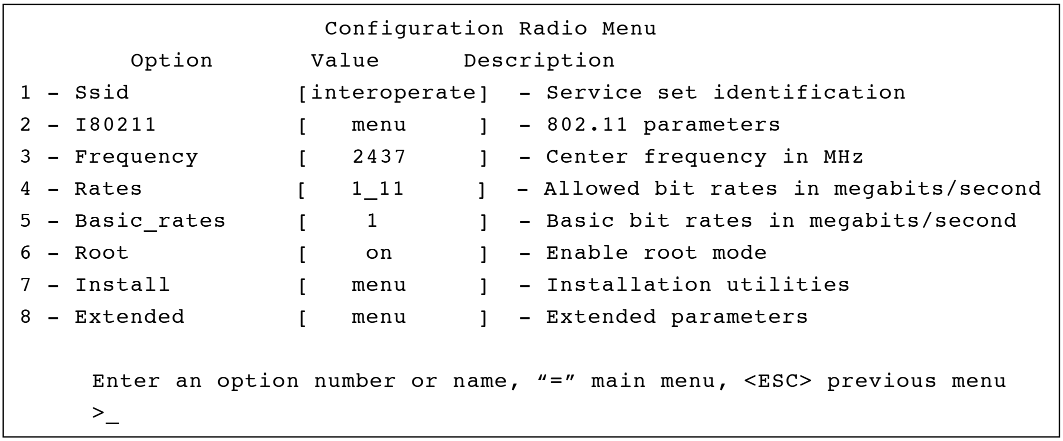
The radio network parameters should be set in the order shown below:

1. Establish a system identifier.
2. Select the bit rate.
3. Select a frequency.
4. Set Access Point operating parameters.
5. Enable root or repeater mode.
6. Set any extended parameters (optional).

CAUTION: Changing any of the radio parameters after you have completed your configurations will cause the unit to drop all radio connections and restart with the changes you have made. Consequently, there will be a disruption in radio traffic through the unit.

Using the Configuration Radio Menu

The radio network is configured using the Configuration Radio Menu. To access this menu, select **Configuration** from the Main Menu then select **Radio** from the Configuration Menu.



```
                      Configuration Radio Menu
        Option        Value      Description
1 - Ssid             [interoperate]  - Service set identification
2 - I80211           [    menu     ]  - 802.11 parameters
3 - Frequency        [    2437     ]  - Center frequency in MHz
4 - Rates            [    1_11     ]  - Allowed bit rates in megabits/second
5 - Basic_rates      [     1       ]  - Basic bit rates in megabits/second
6 - Root             [     on      ]  - Enable root mode
7 - Install          [    menu     ]  - Installation utilities
8 - Extended         [    menu     ]  - Extended parameters

     Enter an option number or name, "=" main menu, <ESC> previous menu
     >_
```

Establishing a SSID (SSID)

This string functions as a password to join the radio network. Nodes associating to the Access Point must supply a matching value, determined by their configurations, or their association requests will be ignored.

Selecting Frequency (Frequency)

The actual frequency allowed depends on the regulatory body that controls the radio spectrum in the location in which the unit is used.

Selecting Bit Rates (Rates, Basic_rates)

Use the *rates* option to set the list of data rates at which the unit will be allowed to send and receive radio packets. The rate must be configured as an inclusive range such as 1_11 Mbps or 2_5.5 Mbps. When the client node associates with the Access Point, the list of allowed rates must be supplied. The Access Point will track the lists on a client by client basis and communicate accordingly. The Access Point will transmit packets at the highest possible rate listed. If the client’s retry rate is high, the Access Point will transmit at a lower rate in the list.

Use the *basic_rates* option to determine the rate at which every client in the cell must support. If the *basic_rate* is not supported, the client will not be allowed to associate. The lowest *basic_rate* controls the rate at which all multicast and broadcast packets are transmitted. The highest *basic_rate* controls the bit rate at which the management packets are transmitted.

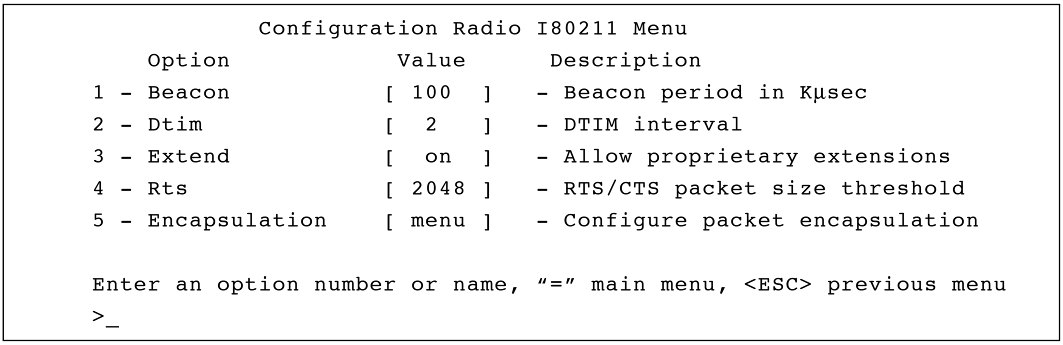
Enabling Root Mode (Root)

Use the *root* option to enable or disable root mode.

Access Points serving as root units are connected to the primary backbone infrastructure and should have Root Mode set to “On.” Those that are serving as repeaters should have root mode set to “Off”. The default setting is “On”.

When a unit is changed from a root to a repeater, the cabled connection, by default, is disabled. Repeaters will not route network traffic through their LAN ports. Re-enable the port only if you wish to gain access to the Aironet Access Point (over its wired LAN). Packets received from a repeater’s LAN connection will only be processed by the unit itself and will not be forwarded to the radio network.

Using the Configuration Radio IEEE 802.11 Menu



```
                Configuration Radio I80211 Menu
        Option            Value      Description
    1 - Beacon           [ 100  ]   - Beacon period in Kμsec
    2 - Dtim             [  2   ]   - DTIM interval
    3 - Extend           [  on  ]   - Allow proprietary extensions
    4 - Rts              [ 2048 ]   - RTS/CTS packet size threshold
    5 - Encapsulation    [ menu ]   - Configure packet encapsulation

    Enter an option number or name, "=" main menu, <ESC> previous menu
    >_
```

Setting the Beacon Period (Beacon)

The beacon interval is the time (in kilo-microseconds) between transmissions of the IEEE 802.11 beacon packet. The beacon packets are primarily used for radio network synchronization.

The beacon is also used to inform clients in power save mode that there are buffered packets waiting at the Access Point. Once the client wakes up, it will request the Access Point send the packets.

A long beacon period may slow down power save nodes since they are not notified as frequently. A short beacon period may take up a significant portion of the radio bandwidth.

Setting the Forwarding Time Interval (DTIM)

DTIM frames are special beacon frames which convey information useful for power save operations. The DTIM internal is defined in increments of the beacon interval (i.e. every fourth beacon will be a DTIM). If power save nodes are present, multicast and broadcast packets are buffered by the Access Point and will only be sent after a DTIM beacon. This ensures all nodes are awake to receive the packets. This parameter sets the upper limit on the amount of time any power save node in the cell may stay asleep.

Adding IEEE 802.11 Management Packet Extensions (Extend)

If this parameter is enabled, the Aironet Access Point will add extensions to some of the IEEE 802.11 management packets. This passes more information to other radio nodes allowing them to associate to the best Access Point.

Even with the extensions enabled, other manufacturer’s nodes should ignore the extra information. However, if they become confused, this parameter may be disabled.

Setting the RF RTS/CTS Parameter (RTS)

This parameter determines the minimum size transmitted packet that will use the RTS/CTS protocol. The value entered must be in the range of 100 to 2048 bytes.

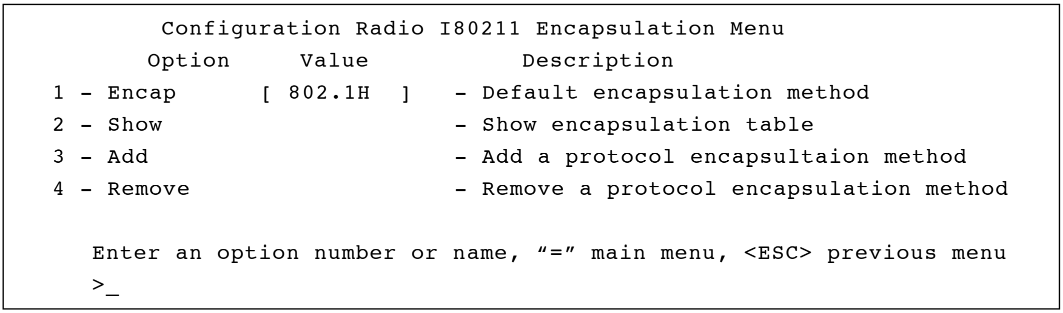
This protocol is most useful in networks where the mobile nodes may roam far enough so the nodes on one side of the cell cannot hear the transmission of the nodes on the other side of the cell.

When the transmitted packet is large enough, a small packet is sent out (an RTS). The destination node must respond with another small packet (a CTS) before the originator may send the real data packet. A node at the far end of a cell will see the RTS to/from the Access Point or the CTS to/from the Access Point. The node will know how long to block its transmitter to allow the real packet to be received by the Access Point. The RTS and CTS are small and, if lost in a collision, they can be retried more quickly and with less overhead than if the whole packet must be retried.

The downside of using RTS/CTS is that for each data packet you transmit, you must transmit and receive another packet, which will affect throughput.

Using the Configuration Radio I80211 Encapsulation Menu

To access the Configuration Radio I80211 Encapsulation Menu, select **80211** from the Configuration Radio Menu then select **Encapsulation** from the Configuration Radio 80211 Menu.



```
           Configuration Radio I80211 Encapsulation Menu
          Option     Value          Description
   1 - Encap      [ 802.1H  ]    - Default encapsulation method
   2 - Show                      - Show encapsulation table
   3 - Add                       - Add a protocol encapsultaion method
   4 - Remove                    - Remove a protocol encapsulation method

      Enter an option number or name, “=” main menu, <ESC> previous menu
      >_
```

Encapsulation (Encap)

The *Encap* option and the related encapsulation table commands of *Show*, *Add*, and *Remove* are of concern only when both of the following conditions exist:

- You are assembling a wireless LAN that incorporates non-Aironet equipment.
- The non-Aironet equipment uses a proprietary method of packet encapsulation that is different from the method used by Aironet.

If your wireless LAN consists only of Aironet components, use the default Encapsulation value of 802.1H and disregard the information in following discussion “Packet Encapsulation in Mixed Networks.”

Packet Encapsulation in Mixed Networks

Aironet LAN software allows you to assemble a wireless infrastructure using components from different suppliers. When combining equipment from different sources into a wireless LAN, you might need to accommodate different methods of packet encapsulation and conversion. The complete subject of packet addressing is beyond the scope of this manual, and our purpose here is to provide only basic guidelines and considerations.

To combine a mix of equipment from alternate suppliers into a wireless LAN, you need to know the packet encapsulation methods used by the different suppliers. If you determine that your infrastructure will be mixing packet encapsulation methods, you will first need to determine your primary method, or standard, and choose that as the default setting with the *encap* option. All methods other than the primary, or default, method need to be entered in the Encapsulation Table.

For all Aironet equipment, the defined packet encapsulation standard is 802.1H. The Show, Add, and Remove options allow you to manage a table of alternate, non-802.1H encapsulation methods that might be required to read data packets sent from the other, non-Aironet equipment. The primary alternate to the 802.1H standard is RFC 1042.

On an Ethernet LAN, the data portion of a frame may be in one of two formats: DIX or DSAP/SSAP. The two formats differ both in packet size specifications and in the manner of heading, or starting, the data portion. An 802 wireless LAN requires packets to start with the DSAP/SSAP format and therefore must provide a method of conversion. DSAP/SSAP packet types are easily converted since the header is already in the required style. DIX packet types present more of a problem since there are many different formats and no standard conversion method.

Aironet's 802.1H conversion protocol accommodates both DIX and DSAP/SSAP packet types. In an 802.1H conversion, DIX type packets are prepended with a header that mimics the DSAP/SSAP header. In an Aironet infrastructure, this header style is not used by any wired Ethernet nodes so the remote radio node is always able to accurately reconvert the packet.

Using the Configuration Radio Install Menu

The options in this menu can be used to determine system performance on individual nodes as well as individual node radio performance.

```
         Configuration Radio Install Menu
    Option       Value      Description
1 - Linktest  [  menu ]   - Run a link test
2 - Strength              - Run a signal strength test

Enter an option number or name, "=" main menu, <ESC> previous menu
>_
```

Running a Signal Strength Test (Strength)

The *strength* option sends a packet once per second to each station in the association table. This packet is echoed back to the Aironet Access Point which records and displays the RF signal strength associated with that particular node.

It can be used to quickly check the link to each radio partner or could be monitored while aligning directional antennas between two nodes. As the antennas are moved, the signal strength could be monitored until the maximum value is achieved.

```
                       SIGNAL LEVELS
APxxxx   00409611d1e5 Strength  In ********************************
                               Out ***********************************
(^C to exit)                       |---------------------------------|
```

Running a Link Test (Linktest)

The *linktest* option is used to test the transmission quality between Aironet Access Point nodes and other nodes on the radio network.

A link test sends special control packets to a specified destination which in turn echoes the packets back to the source. Each control packet sent has a sequence number that allows the sender to know whether packets were lost either on the way to the destination or on the way back to the source node.

```
                Configuration Radio Install Linktest Menu
        Option          Value      Description
    1 - Multicast                - Run a multicast test
    2 - Unicast                  - Run a unicast test
    3 - Remote                   - Run a remote test
    4 - Destination   [ any  ]   - Target address
    5 - Size          [ 512  ]   - Packet size
    6 - Count         [ 100  ]   - Number of packets to send
    7 - Errors                   - Radio error statistics
    8 - Autotest      [ once ]   - Auto linktest mode
    9 - Continuous    [  0   ]   - Repeat test once started

    Enter an option number or name, "=" main menu, <ESC> previous menu
    >_
```

Running a Multicast Test (Multicast)

The *multicast* option is used to test transmission conditions within local radio cells. Packets are sent between the source and destination nodes without any acknowledgments or retries (as multicasts). This test provides a good indication of the raw state of the path to the node since no attempt is made to recover from any radio errors.

```
    Testing link to 00409611d1e5 with 100 multicast packets of size 512
    Please wait:
    GOOD (  9% Lost)       Time   Strength %
                           msec      In   Out
                           ----  ----- -----
           Sent: 100,  Avg:  19      78    85
    Lost to Tgt:   8,  Max:  29      85    92
    Lost to Src:   1,  Min:  17      71    85
```

The time is displayed in milliseconds. Each packet contains the time it was sent. When a packet is received by the source, the time difference indicates the round trip time. Longer times indicate that the processor's or the radio's bandwidth is full.

The signal strength numbers indicate the strength of the radio signal at the time the packets were received at each end. Signal strength is expressed as a percentage of full power.

Running A Unicast Test (Unicast)

The *unicast* option can be used to test the path between the Aironet Access Point and any other Aironet node in the wired or radio network. The packets are sent with the same error recovery as normal user data so round trip times indicate the infrastructure throughput and congestion.

```
Testing link to 00409611d1e5 with 100 unicast packets of size 512
GOOD (8% Retries)      Time   Strength %        Retries
                       msec     In   Out        In  Out
                       ----  ----- -----      ---- ----
       Sent: 100,  Avg:  25     78    85  Tot:   3   14
Lost to Tgt:   0,  Max:  91     85    92         1    2
Lost to Src:   0,  Min:  21     78    85         0    0
```

If the path to the target node was over the radio, a total number of radio retries necessary to complete the test is also displayed. If the total number of retries is large, there may be problems with the link. Look for sources of interference.

Running a Remote Linktest (Remote)

Use the *remote* option to run a multicast link test between a client node associated somewhere in the infrastructure and its parent Access Point. You will be prompted for the infrastructure address of the client node. A broadcast request will be made. The Access Point with this associated node will run the link test and return the results which will be displayed to the operator locally.

```
Remote linktest from 00409610d258 to 0040961064de

Sent 100 of 100 512 byte packets, Destination received
90, Source received 90
```

Specifying the Target Address (Destination)

The *destination* option is used to indicate the target node address for the link test. You may enter an infrastructure address or the string “any”. If you select “any”, the Aironet Access Point will direct the test to the first legal address found in the association table.

Setting the Packet Size and Count (Size, Count)

The *size* and *count* options are used to indicate the size and number of packets to be sent. The default values are 100 packets of 512 bytes each. Both the size and the count can be changed. The packet size may be set from 24 to 1450 bytes and the count of the number of packets to transmit may be set from 1 to 999 packets.

When running the link test, use the highest data bit rate possible to test the reliability of your data bit rate and frequency combination. The more packets you send and the larger the packet size, the more accurate the test.

NOTE: Multiple large packets will increase test time.

Viewing Errors (Errors)

The *errors* option is used to view the Radio Error statistics that may have occurred during the link test. See **Chapter 8** “Viewing Statistics”.

Setting the Automatic Link Test Mode (Autotest)

The *autotest* option is used to control the automatic running of a link test whenever a repeater associates to its parent. The test will use the currently configured test parameters which, by default, runs a test to the parent node.

- **Off**: An automatic test is never run.
- **Once**: Only one test is run the first time the unit associates to a parent after powering on.
- **Always**: The test is run each time the unit associates to a parent.

During an automatic link test the three indicators on the unit will turn green in a cyclic pattern to indicate a test is in progress. At the end of the test, the indicators will be set to a solid pattern for 4 seconds to indicate the test results. The particular pattern that will be displayed depends on the percentage of packets lost during the test as shown in Table 4.1

Table 4.1 - Auto Link Test Display Patterns

Radio	Status	Ethernet or Token Ring	% of Packets Lost	Quality
Green	Green	Green	0-2	Excellent
Green	Green	Amber	3-5	Very Good
Green	Green	Off	6-25	Good
Green	Amber	Off	26-50	Satisfactory
Amber	Off	Off	51-75	Fair
Red	Off	Off	76-100	Poor

The Autotest procedure can be used to help determine the placement of repeater units. For example, at each prospective location, an installer could cycle the power on the unit and watch the indicator displays for the results of the link test. As the test begins to fail, the installer could determine the radio range to the infrastructure and adjust the location accordingly.

Continuously Running a Link Test (Continuous)

The *continuous* option is used to continuously repeat the link tests. If the value for the parameter is zero the tests are not repeated; otherwise, the value determines the delay (in seconds) between tests.

Using the Configuration Radio Extended Menu

The extended radio parameters are not normally modified, but some may have to be changed when certain situations arise.

```
                    Configuration Radio Extended Menu
      Option            Value            Description
  1 - Parentid        [   any   ]   - Parent node Id
  2 - Parent_timeout  [   off   ]   - Time to look for specified parent
  3 - Parent_wait     [   500   ]   - How long to look for previous parent
  4 - Time_retry      [    8    ]   - Number of seconds to retry transmit
  5 - Count_retry     [    0    ]   - Maximum number transmit retries
  6 - Refresh         [   100   ]   - Refresh rate in 1/10 of seconds
  7 - Diversity       [   on    ]   - Enable the diversity antennas
  8 - Power           [   full  ]   - Transmit power level
  9 - Fragment        [   2048  ]   - Maximum fragment size

     Enter an option number or name, “=” main menu, <ESC> previous menu
     >_
```

The Menu will display different options, depending on whether your unit is serving as an infrastructure or a repeater.

Setting the Parent ID (Parentid, Parent_wait)

This parameter appears when the unit is configured to be a repeater. The parameter is used to control to which Access Point the unit associates. If the value is set to “any”, the Aironet Access Point will associate with its best choice of parent based on signal quality and load. If the value is set to a network address, the Aironet Access Point will only associate with the Access Point having the matching address.

If the *parent_wait* option is also set to a value in seconds, then after the association is lost, the unit will only attempt to associate to the specified Access Point for the given time. If the Aironet Access Point still has not found the requested parent after the time expires, the unit will give up and associate to the best Access Point. If the time-out is set to off, the unit will only associate to the specified Access Point.

Setting Retry Transmission Time (Time_Retries, Count_Retries)

These settings allow the user to establish a particular level of radio performance by controlling the RF packet retry level. The lesser of the two values will be used. If the retry count is reached before the retry time is met, then retry process on this particular packet is stopped. If the destination was a child node, it will be disassociated. If the destination was a parent Access Point, the unit will begin scanning for a new parent.

The retry time may be set in the range of 1 to 30 seconds. The Aironet Access Point will continually retry the packet in this time period while contending for the air waves with other transmitting nodes.

The retry count may be set in the range of 0 to 64 times. If the count is set to zero, only the retry time applies.

Use the retry count field if the Aironet Access Point is mobile and you want to move from Access Point to Access Point very quickly after moving out of range. In non-mobile applications, since you can’t move out of range, it is most likely there is some temporary interference. Retry at a later time.

Setting the Refresh Time (Refresh)

This parameter will only appear if the Aironet Access Point is configured as a repeater. If there has been no non-broadcast traffic between the unit and its parent for the specified amount of time, the Aironet Access Point will send a special refresh packet to ensure the parent is still reachable. The value may be set from 5 to 150 1/10ths of a second. Leave the default value unless the Aironet Access Point is mobile and needs to quickly know that it has moved out of range (faster than once every 15 seconds).

Enabling Diversity Antennas (Diversity)

This parameter tells the unit whether you have two antennas installed. Set the parameter to “Off” if one antenna is installed. The single antenna must be installed on the right connector when facing the back of the unit with the LED display facing up.

Setting Power Level (Power)

This parameter may be used to reduce the power level of the radio transmitter down from the maximum allowed by the regulatory commissions. Depending on where you are located, you may be allowed to set the power to 50 milliwatts, 100 milliwatts, or to full power.

Setting Fragment Size (Fragment)

This parameter determines the largest packet size that may be transmitted. Packets that are larger than this size will be broken into pieces that are transmitted separately and rebuilt on the receiving side.

If there is a lot of radio interference or collisions with other nodes, the smaller lost packets can be retried faster and with less impact on the airwaves. The disadvantage is if there is limited interference, long packets will take more time to transmit due to the extra packet overhead and acknowledgments for the fragments.

Set the fragment size between 256 and 2048 bytes.

5

CHAPTER 5

Configuring the Ethernet or Token Ring Port

This chapter describes the procedures for configuring the Ethernet or Token Ring Access Point Port.

Here's what you'll find in this chapter:

- Using the Configuration Ethernet or Token Ring Menu
- Using the Token Ring Extended Menu
- Using the Token Ring Address menu

Using the Configuration Ethernet or Token Ring Menu

The Ethernet or Token Ring Port is configured using the Configuration Ethernet or Token Ring Menu. To access this menu, select **Configuration** from the Main Menu then select **Ethernet** or **Token Ring** from the Configuration Menu.

```
                 Configuration Ethernet Menu
          Option        Value       Description
      1 - Active      [ on   ]    - Connection active
      2 - Size        [ 1518 ]    - Maximum frame size
      3 - Port        [ auto ]    - Port selection
      4 - Fallback    [ off  ]    - Become repeater on LAN cable fault

      Enter an option number or name, "=" main menu, <ESC> previous menu
      >_
```

```
                    Configuration Token Ring Menu
          Option        Value           Description
   1 - Active     [      off      ]   - Connection active
   2 - Speed      [       16      ]   - Ring speed
   3 - Method     [ source_route  ]   - Routing method
   4 - Fallback   [      off      ]   - Become repeater on LAN cable fault
   5 - Extended   [      menu     ]   - Extended configuration
   6 - Address    [      menu     ]   - Config address conversions

   Enter an option number or name, "=" main menu, <ESC> previous menu
   >_
```

Activating/Disabling the Ethernet or Token Ring Port (Active)

NOTE: Do not activate the Ethernet or Token Ring port until all other parameters have been set correctly.

The *active* option is used to enable or disable the Ethernet or Token Ring Port connection. The default setting for active is “On”.

The *active* option should be disabled if the port on the Aironet Access Point is not going to be used. This informs the software not to route packets to the port and stops the use of processing power for scanning for Ethernet or Token Ring activity.

Setting the Maximum Frame Size (Size) Ethernet Only

The *size* option allows you to increase the maximum size of frames transmitted to and from the Ethernet infrastructure. Do not set the maximum frame size greater than 1518 unless you are running proprietary software that allows you to exceed this maximum. You may set the value between 1518 to 4096.

NOTE: After the parameter is changed, the unit must be restarted either by powering it "Off" and then "On," or by using the "Diagnostics Restart" command for the change to occur.

Setting the Port Interface Type (Port) Ethernet Only

If this parameter is set to "Auto", the Ethernet Access Point will scan for a cable at all three connections. When the Access Point is wired to an Ethernet card that also scans, this parameter should be set to the port that is being configured. You may select AUI for 10base5 for thicknet, 10baseT for twisted pair, or 10base2 for coax and thinnet.

Setting the Fallback Option (Fallback)

The *fallback* option controls how the Access Point will react when the Ethernet or Token Ring connection is no longer operating properly.

- **Off**: No extra action is taken.
- **On**: If the unit is configured as a root and the Ethernet or Token Ring connection goes down, the unit will become a repeater. Once the Ethernet or Token Ring connection is restored the unit will return to being a radio root. By becoming a repeater, the unit will try and associate with a working root unit in range to try and maintain connectivity to the backbone LAN for all of its associated radio nodes.
- **Disconnect**: If the Ethernet or Token Ring connection goes down, the unit will remove all nodes associated to it and not accept any new associations until the backbone LAN connection is restored. The Access Point effectively removes itself from the infrastructure. This may be used in situations where each client is in range of more than one Access Point and you do not want clients to associate to a repeater. The disadvantage with this mode is the Access Point has no way of reporting the failure to a central site.

Setting the Token Ring Speed (Speed) Token Ring Only

The Access Point may be connected to Token Ring infrastructures that operate at either 4 megabits per second or 16 megabits per second. The Speed option allows you to configure the clock on the Access Point to match the infrastructure speed. The Access Point will not be able to open its ring connection if the speed does not match.

Setting the Routing Method (Method) Token Ring Only

The Access Point may be configured to operate with infrastructures:

- whose packets are transparently routed by bridges based on the destination MAC address.
- whose packets must contain a source routing mode header to guide their path through the infrastructure.

Transparent:
It is assumed that there are no source routing headers in the packets. The unit will monitor all packets sent around the Token Ring infrastructure. Only packets with destination addresses which match the address of a radio node associated to the Access Point or multicasts will be forwarded out to the radio. No source routing header will be added to any packets sent out the Token Ring.

Source routing:
The unit must watch all traffic on the LAN.

The packet will be forwarded to a radio network if:

- The unit identifies a packet with a source route that ends at the ring number on which the unit is located
- The destination address belongs to a radio mode
- The destination is a multicast

The unit will also record the source route back to the originator of the packet for later use. Since all radio nodes are configured as though they are connected to an Ethernet LAN (which always uses transparent routing), the Token Ring Access Point must add source routes to any outgoing packets. If the destination is in the list of learned routes, the route is used, otherwise the packet is sent with a broadcast route. Once the destination responds, the Token Ring Access Point will learn the new address.

Using the Token Ring Extended Menu

```
                  Configuration Tokenring Extended Menu
         Option        Value     Description
     1 - Partition   [ 4  ]   - Number of bits in bridge numbers
     2 - Earlyrls    [ 18 ]   - Maximum route field length
     3 - Sap         [ aa ]   - Set control frame SAPs
```

Setting the Size of a Bridge Number (Partition) Token Ring Only

This option only appears if the Access Point is in source route mode. In the routing information field of a packet header, the ring and bridge numbers are packed into 16 bit integers. The option determines how many of the 16 bits are used for the bridge number portion. The default value of 4 allows up to 15 bridges to be connected to the same set of rings (zero is not an option).

Typically, this parameter is not changed and should only be changed after consulting with your network administrator.

Early Token Release (Earlyrls) Token Ring Only

This option only appears when used with a 16 Mbit ring. Typically, a station transmits a packet after receiving the token and retransmits the token once it has seen the packet come back after traversing the ring. The *early release* option allows the unit to transmit the token immediately after transmitting a packet. This allows for more than one packet to be traversing the ring at a time. The default value for 16 Mbit ring is on. This option should only change after consolidating with your network administrator.

Control Frame Saps (Sap) Token Ring Only

This item is for manufacturer’s internal use only.

Using the Token Ring Address Menu

```
                   Configuration Tokenring Address Menu
          Option       Value     Description
      1 - Display              - Display the conversion entries
      2 - Add                  - Add a conversion entry
      3 - Remove               - Remove a conversion entry
```

When a radio client node is associated to a Token Ring Access Point and needs to communicate with a Token Ring node, conversion of multicast addresses may be necessary. The radio node reads as though it is attached to an Ethernet port. The Token Ring nodes are only able to receive a restricted form of multicast address.

Destination addresses, in the association table, are converted to the Ethernet form on receipt from the Token Ring. The addresses are then converted to the Token Ring form when transmitted to the Token Ring.

To add an entry, enter the Ethernet address and the equivalent Token Ring address. To delete an address, specify all addresses or a specific Ethernet address.

6

CHAPTER 6

Setting Network Identifiers

This chapter describes the procedures for setting the Aironet Access Point network identifiers.

Here's what you'll find in this chapter:

- Using the Configuration Ident Menu
- Establishing a Node Name
- Resetting the Default Network ID
- Assigning an IP Address
- Specifying the IP Subnet Mask
- Setting SNMP Location and Contact Identifiers
- Configuring the IP Routing Table

Using the Configuration Ident Menu

Network identifiers are entered using the Configuration Ident Menu. To access this menu, select **Configuration** from the Main Menu then select **Ident** from the Configuration Menu.

```
                   Configuration Ident Menu
    Option          Value         Description
1 - Name    ["AP4800E_21eeec"] - Node name
2 - Nid     [   00409621eeec ] - Network address
3 - Inaddr  [ 149.023.130.044] - Internet address
4 - Inmask  [ 255.255.000.000] - Internet subnet mask
5 - Routing [      menu      ] - IP routing table configuration
6 - Location[        ""      ] - SNMP system location
7 - Contact [        ""      ] - SNMP system contact name

Enter an option number or name, “=” main menu, <ESC> previous menu
>_
```

Establishing a Node Name (Name)

The *name* option is used to establish a unique node name for the Aironet Access Point. The *name* is a text string of up to 20 characters that appears on all Console Port Menus. It is passed in association messages to other nodes on the radio network. See **Chapter 9** “Setting Up the Association Table”.

Resetting the Default Network ID (NID)

The *NID* option displays the network ID of the Aironet Access Point. The default network ID, assigned at the time of manufacture, is a global administered unique, 6-byte network address.

Typically, there is no need to use a value other than the default network ID. However, if your LAN addresses are locally administered, you may want to change the value of this parameter to match those used on your LAN. No two units can be assigned the same address.

To set the value to the default programmed into the hardware, select “default” when prompted.

NOTE: After the network ID is changed, the unit must be restarted either by powering it “Off” and then “On,” or by using the “Diagnostics Restart” command for the change to come into effect.

Assigning an IP Address (Inaddr)

Use the *inaddr* option to establish an IP (Internet Protocol) address for the Aironet Access Point. An IP address must be assigned to the unit before it can be accessed by either telnet, HTTP, or SNMP.

The IP address may either be assigned manually from this menu or by a BOOTP or DHCP server on the infrastructure. See “Downloading Using the Internet Boot Protocol (Bootp/DHCP)” in **Chapter 12**.

Specifying the IP Subnet Mask (Inmask)

Use the *inmask* option to assign an IP Subnetwork mask to the Aironet Access Point. The subnetwork mask determines the portion of the IP address that represents the subnet ID. A digit in a “bit” of the mask indicates that the corresponding “bit” in the IP address is part of the subnet ID. This item may also be assigned by a BOOTP or DHCP server. See “Downloading Using the Internet Boot Protocol (Bootp/DHCP)” in **Chapter 12**.

Setting SNMP Location and Contact Identifiers (Location, Contact)

Use the *location* and *contact* options to specify the location of the SNMP workstation and the contact name of the individual responsible for managing it in the event of problems. See **Chapter 7** “Configuring SNMP”.

You may enter an arbitrary string of up to 20 characters for each item.

Configuring the IP Routing Table

The IP routing table is entered using the Configuration Ident Routing Menu. To access this menu, select **Routing** from the Configuration Ident Menu.

```
                      Configuration Ident Routing Menu
          Option                 Value              Description
      1 - Display                                 - Display route table entries
      2 - Host                                    - Add a static host route
      3 - Net                                     - Add a static network route
      4 - Default         [ 149.023.130.050  ]    - Internet default gateway
      5 - Delete                                  - Delete a static route

      Enter an option number or name, "=" main menu, <ESC> previous menu
      >_
```

The IP routing table controls how IP packets originating from the Access Point will be forwarded.

If the destination IP address exactly matches a host entry in the table, the packet will be forwarded to the MAC address corresponding to the next hop IP address from the table entry.

If the destination address is on another subnet and matches the infrastructure portion of a net entry in the table (using the associated subnet mask) the packet will be forwarded to the MAC address corresponding to the next hop IP address from the table entry.

If the destination address is on another subnet and does not match any entry in the table, the packet will be forwarded to the MAC address corresponding to the default gateway's IP address.

Displaying the Routing Table (Display)

This menu item displays the entries in the table.

```
                             Routing Table
         Destination           Next Hop              Mask         Flags   Use
      ----------------     ---------------     ---------------  ------  ---
      149.023.166.000      149.023.165.071      255.255.255.000   S  N     0
              default      149.023.165.050      000.000.000.000   S  N     0
      149.023.130.020      149.023.165.060      255.255.255.000   S  H     0
```

The Flags column displays letters identifying the type of entry:

- **S**: Entry is static (entered by operator)
- **N**: Entry is an infrastructure route
- **H**: Entry is a host route

The Use column indicates the number of packets that have been forwarded using this table entry.

In the sample table, all addresses that match 149.23.166.xxx would be forwarded to the router at address 149.23.165.71. Any packet for address 149.23.130.20 would be forwarded to the address 149.23.165.60. All other packets not on the current subnet would be forwarded to the router at 149.23.165.50.

Entering a Host Route (Host)

Host routes control the forwarding of packet to a single host address. You will be prompted for the host's IP address along with the IP address to which the packets should be forwarded to reach the host.

Entering a Network Route (Net)

Infrastructure routes control the forwarding of packet to another subnet of the infrastructure. You will be prompted for the net's IP address, along with the subnet mask to be applied during the address comparison. You will also be prompted for the IP address to which the packets should be forwarded to reach the infrastructure.

Entering Default Route (Default)

The default route is used when forwarding a packet to another subnet of the infrastructure and none of the other table entries apply. You will be prompted for the IP address to which the packets should be forwarded to reach the other networks. This item may also be assigned by a BOOTP or DHCP server.

If the value is left as 0.0.0.0, the Access Point will use the true destination address and assume that a gateway will respond to ARP requests for the remote destination.

Deleting a Route (Delete)

Use this menu item to remove entries from the table. You may delete all entries or only specific IP addresses.

7

CHAPTER 7

Configuring SNMP

This chapter describes how to configure the Aironet Access Point for use with the Simple Network Management Protocol (SNMP).

Here's what you'll find in this chapter:

Overview

The Simple Network Management Protocol (SNMP) provides an industry standard mechanism for the exchange of management information in a TCP/IP based internet environment.

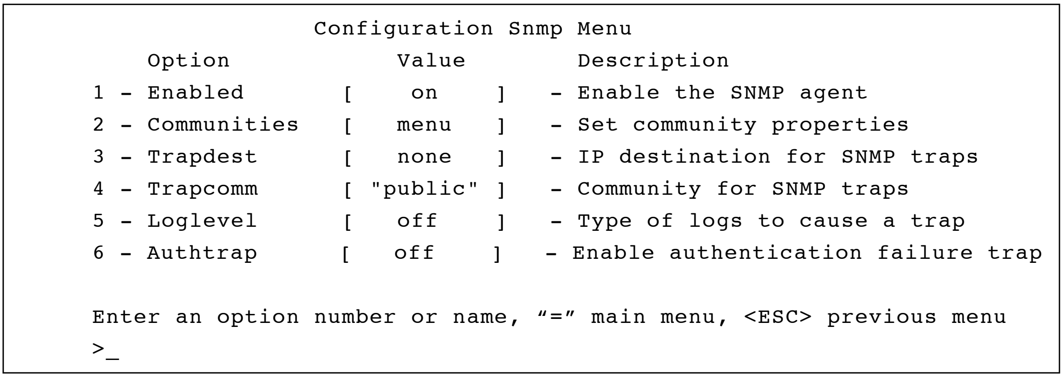
The resident SNMP agent in the Aironet Access Point is compliant with subsets of the Management Information Base (MIB-I, and MIB-II) for TCP/IP based internets, as defined in Internet’s Request for Comment’s (RFC) 1156 and 1213.

A custom MIB has been defined allowing you access to all radio network statistics. See **Appendix C** “SNMP Variables”.

One advantage of SNMP is the ability to set all Console Port configurations from an SNMP Network Management Station (NMS) connected to the infrastructure. In doing so, you eliminate the need to physically connect a terminal to the Aironet Access Point unit in order to complete the configuration and manage the unit. This is especially helpful if the unit is in an inconvenient or remote location.

Using the Configuration SNMP Menu

SNMP is configured using the Configuration SNMP Menu. To access this menu, select **Configuration** from the Main Menu then select **SNMP** from the Configuration Menu.



```
                    Configuration Snmp Menu
        Option            Value        Description
   1 - Enabled        [    on    ]   - Enable the SNMP agent
   2 - Communities    [   menu   ]   - Set community properties
   3 - Trapdest       [   none   ]   - IP destination for SNMP traps
   4 - Trapcomm       [ "public" ]   - Community for SNMP traps
   5 - Loglevel       [   off    ]   - Type of logs to cause a trap
   6 - Authtrap       [   off    ]   - Enable authentication failure trap

   Enter an option number or name, “=” main menu, <ESC> previous menu
   >_
```

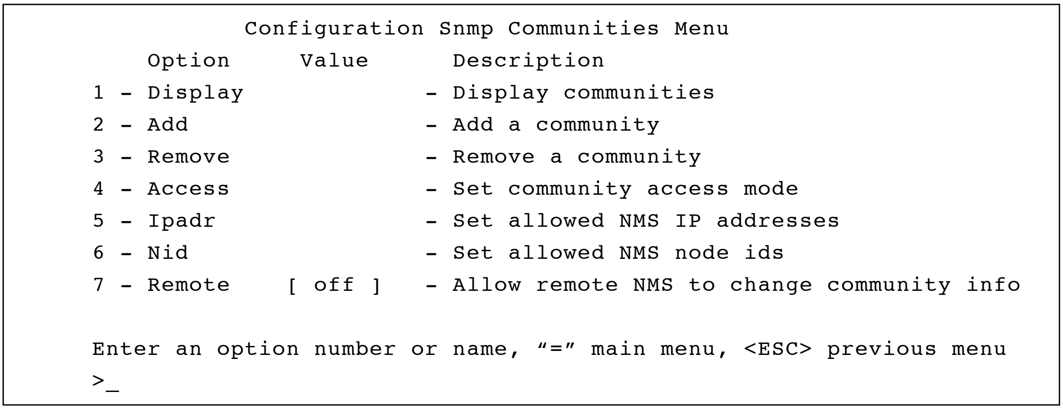
NOTE: The IP address must be assigned before the Aironet Access Point can be accessed by an NMS running SNMP. See **Chapter 6** “Setting Network Identifiers”.

Enabling the SNMP Agent (Enabled)

The *enabled* option functions as an On/Off switch for the SNMP agent. The default setting is “On.” If the parameter is turned “Off,” all incoming SNMP messages will be ignored and no outgoing traps will be generated.

Setting Up SNMP Communities (Communities)

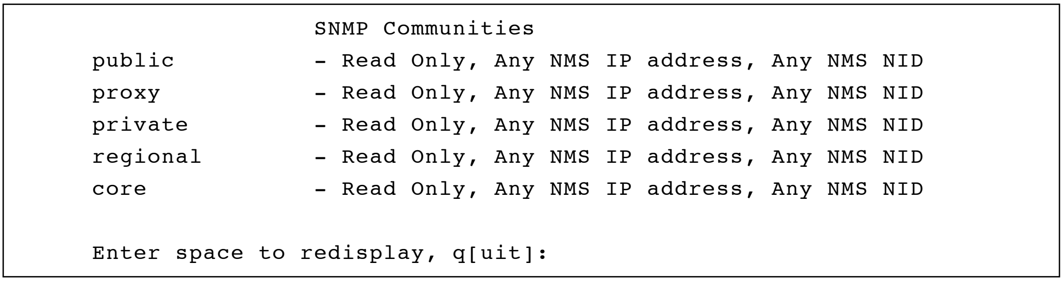
The *communities* option contains a menu that allows control access to the SNMP agent. When you select the *communities* option, the Configuration SNMP Communities Menu appears.



```
              Configuration Snmp Communities Menu
       Option     Value      Description
   1 - Display             - Display communities
   2 - Add                 - Add a community
   3 - Remove              - Remove a community
   4 - Access              - Set community access mode
   5 - Ipadr               - Set allowed NMS IP addresses
   6 - Nid                 - Set allowed NMS node ids
   7 - Remote    [ off ]   - Allow remote NMS to change community info

   Enter an option number or name, “=” main menu, <ESC> previous menu
   >_
```

Displaying Communities (Display)

The *display* option lists the communities you have set. When you select *display*, an SNMP communities list screen similar to the following appears.



```
                   SNMP Communities
   public          - Read Only, Any NMS IP address, Any NMS NID
   proxy           - Read Only, Any NMS IP address, Any NMS NID
   private         - Read Only, Any NMS IP address, Any NMS NID
   regional        - Read Only, Any NMS IP address, Any NMS NID
   core            - Read Only, Any NMS IP address, Any NMS NID

   Enter space to redisplay, q[uit]:
```

An SNMP community consists of the following:

- **Name**: The default set of communities is “Public, Proxy, Private, Regional, and Core”. You can define up to 5 community names. When an NMS requests information from the unit’s agent, the community name in the request must match one of the names on the SNMP communities list.
- **Access Mode**: Displays the community access modes – “Read-Write” and “Read-Only”. The default access mode is “Read-Only.”
- **NMS IP Addresses**: (Optional) Displays a list of allowed Network Management Station IP addresses of the community. You can define up to 5 IP addresses. The default setting is “Any.”
- **NMS NID (Node ID)**: (Optional) Displays a list of allowed node IDs of the community. You can define up to 5 node IDs. The default setting is “Any.”

Adding a Community (Add)

Use the *add* option to add a new community to the SNMP communities list. The default community settings for the new community names are “Read-Only access”, “Any NMS IP address”, and “Any NID.”

Removing a Community (Remove)

Use the *remove* option to remove a community from the SNMP communities list. You will be prompted for the name of the community to remove.

Setting a Community Access Mode (Access)

Use the *access* option to set the community access mode. There are two types of access modes — “Read-Only” and “Read-Write”.

- **Read-Only**: Allows “gets” and “get-nexts” on any readable variable.
- **Read-Write**: Allows “gets” and “get-nexts” on any variable, as well as “set” requests on writable variables.

The default access setting for all community names is “Read-Only” access.

NOTE: An error response will be returned to the NMS, if the NMS is trying a “set” request is used with a community that has Read-Only access.

Setting or Removing Allowed NMS IP Addresses (Ipadr)

Use the *ipadr* option to set or remove allowed NMS IP addresses. If the community has a list of allowed IP addresses, only requests from an NMS with an IP address in the SNMP communities list will be allowed. If there is no list, any IP address is allowed. The default list is “Any.”

You will be prompted for:

1. The name of the community to change.
2. Whether you want to add or remove an IP address.
3. The IP address.

Setting or Removing Allowed NMS Node IDs (Nid)

Use the *nid* option to set or remove allowed NMS node IDs. If the community has a list of allowed node IDs, then only requests from an NMS with a node ID in the list will be allowed. If there is no list, then any node ID is allowed. If any of the above checks fail, the request will be ignored. The default list is “Any.”

You will be prompted for:

1. The name of the community to change.
2. Whether you want to add or remove an infrastructure address.
3. The infrastructure address.

Enabling Remote NMS to Change Community Setup (Remote)

The *remote* option controls whether the section of the custom MIB for the Aironet Access Point allowing access to the community name configuration is enabled or disabled.

- **On**: A remote NMS with write access will be able to change the configuration and access rights for the community names.
- **Off**: No NMS will be able to change this part of the configuration.

Setting SNMP Trap Destinations (Trapdest)

Use the *trapdest* option to generate SNMP trap messages to a particular NMS whenever a significant event occurs.

If SNMP is enabled and the *trapdest* option is configured with a valid IP address, then the system will generate SNMP trap messages. If the *trapdest* option is set to “none,” then traps will not be sent. Setting the *trapdest* option to address 0.0.0.0 is the same as disabling trap generation by using “none.”

The following trap messages will be sent as they occur:

- A cold start trap will be sent when the unit first powers up.
- A link up trap is sent when the configuration is changed or restored for a severe error condition.
- A link down trap is sent when the configuration is changed or encounters a severe error condition.
- A link up trap is sent for an Aironet Access Point as soon as the radio is configured.
- An authentication failure trap will be sent if an SNMP request is received with an unknown community name. This trap may be disabled by setting the “authtrap” parameter to “Off”. See “Enabling Authentication Failure Trap (Authtrap)” .
- Any normal alarms and logs you have configured to be sent by setting the “loglevel” parameter.

NOTE: Since the path to the trap destination may be through a failed or not yet established radio link, it is possible that cold start and link down traps could be lost.

Specifying Community Names for Trap Messages (Trapcomm)

Use the *trapcomm* option to specify the community name that will be used in the trap message.

Specifying the Type of Log to Cause an SNMP Trap (Loglevel)

The Aironet Access Point may be configured to generate an enterprise specific trap whenever a log of a given severity or higher is produced. The trapdest parameter must “On”.

The generated trap will contain the text of the log message along with the severity of the log. See the MIB definition files for the exact layout of the trap. The different severities are:

- **Error/Severe**: Displays all Error and Severe Logs
- **Severe**: Displays Severe Error Logs only
- **All**: Displays all Error, Severe, and Information Logs
- **Off:** No Event Logs will be displayed

See **Chapter 11** “Setting Up Event Logs”.

Enabling Authentication Failure Trap (Authtrap)

Use the *authtrap* option to control the generation of SNMP authentication failure traps.

The failure traps may be sent if an NMS sends a request with an unknown community name or a community name that it is not allowed for use. You can enable or disable this option. The default setting is “Off”.

8

CHAPTER 8

Viewing Statistics

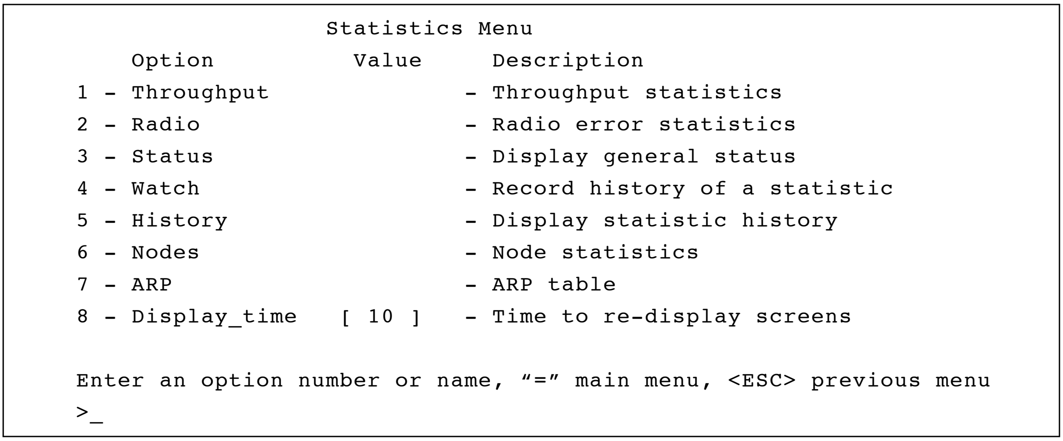
This chapter describes how to use the Statistics Menu to monitor the performance of the Aironet Access Point.

Here’s what you’ll find in this chapter:

- Viewing the Statistics Menu
- Throughput Statistics
- Radio Error Statistics
- Displaying Sources Routes (Token Ring Only)
- Displaying Overall Status
- Recording a Statistic History
- Displaying a Statistic History
- Displaying ARP Information
- Setting Screen Display Time

Viewing the Statistics Menu

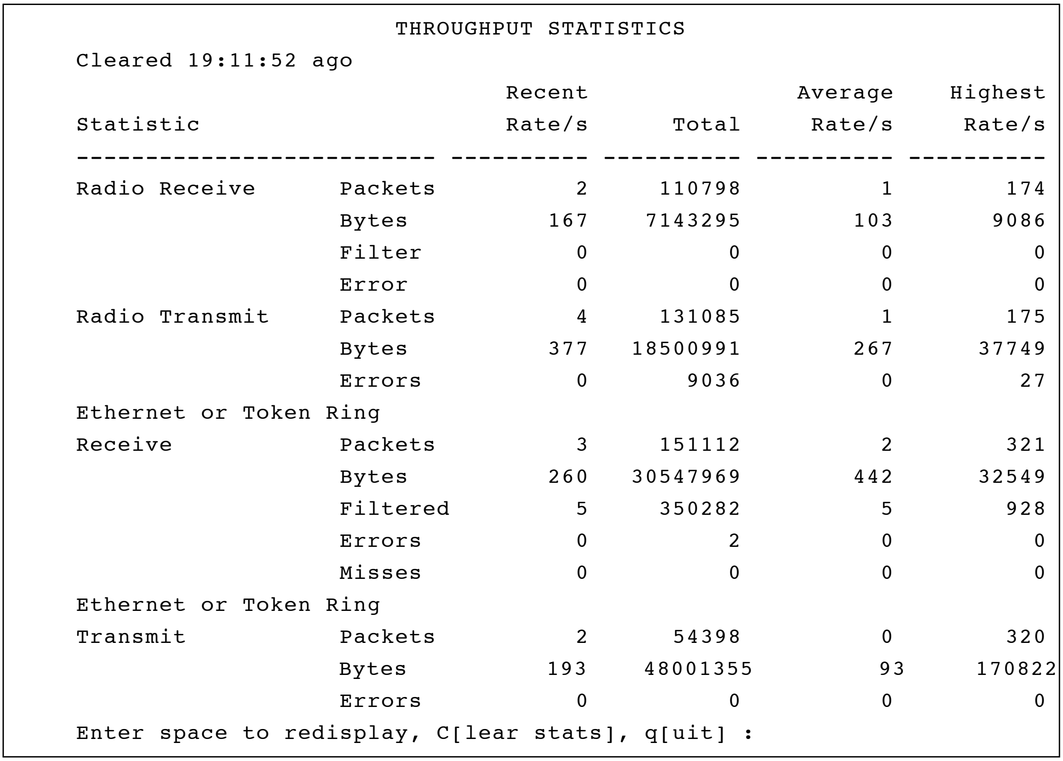
The Statistics Menu provides easy access to a variety of statistical information regarding the Aironet Access Point's performance. You can use the data to monitor the unit and detect problems when they occur. To access this menu, select **Statistics** from the Main Menu.



```
                  Statistics Menu
    Option          Value     Description
1 - Throughput              - Throughput statistics
2 - Radio                   - Radio error statistics
3 - Status                  - Display general status
4 - Watch                   - Record history of a statistic
5 - History                 - Display statistic history
6 - Nodes                   - Node statistics
7 - ARP                     - ARP table
8 - Display_time   [ 10 ]   - Time to re-display screens

Enter an option number or name, "=" main menu, <ESC> previous menu
>_
```

Throughput Statistics (Throughput)

The Throughput Statistics Display provides a detailed summary of the radio data packets passing through your unit. To access this display, select **Statistics** from the Main Menu then select **Throughput** from the Statistics Menu.



```
                           THROUGHPUT STATISTICS
     Cleared 19:11:52 ago
                                Recent                Average    Highest
     Statistic                  Rate/s      Total      Rate/s     Rate/s
     ------------------------- ---------- ---------- ---------- ----------
     Radio Receive      Packets          2     110798          1        174
                        Bytes          167    7143295        103       9086
                        Filter           0          0          0          0
                        Error            0          0          0          0
     Radio Transmit     Packets          4     131085          1        175
                        Bytes          377   18500991        267      37749
                        Errors           0       9036          0         27
     Ethernet or Token Ring
     Receive            Packets          3     151112          2        321
                        Bytes          260   30547969        442      32549
                        Filtered         5     350282          5        928
                        Errors           0          2          0          0
                        Misses           0          0          0          0
     Ethernet or Token Ring
     Transmit           Packets          2      54398          0        320
                        Bytes          193    48001355          93     170822
                        Errors           0          0          0          0
     Enter space to redisplay, C[lear stats], q[uit] :
```

- **Recent Rate/s**: Displays the event rates, per second, averaged over the last 10 seconds.
- **Total**: Displays the number of events that have occurred since the statistics were last cleared.
- **Average Rate**: Displays the average event rates, per second, since the statistics were last cleared.
- **Highest Rate**: Displays the highest rate recorded since the statistics were last cleared.
- **Packets**: Displays the number of packets transmitted or received.
- **Bytes**: Displays the total number of data bytes in all the packets transmitted or received.

- **Filtered**: Displays the number of packets that were discarded as a result of an address filter being setup.
- **Errors**: Displays the number of errors that may have occurred.
- **Enter space to redisplay, C[lear stats], q[quit]**: To redisplay statistics, enter a space by pressing the space bar. To clear the statistics, press “C” (case sensitive). To exit the Statistics Menu, press “q”.

Radio Error Statistics (Radio)

The Radio Error Statistics Display provides a detailed summary of the radio receiver and transmitter errors that have occurred on the unit.

To access this display, select **Statistics** from the Main Menu then select **Radio** from the Statistics Menu.

```
                           RADIO ERROR STATISTICS
Cleared 19:23:22 ago
Receive                                 Transmit
--------------------------------------  ------------------------------------
Buffer full frames lost         0       Retries                         0
Duplicate frames                0       Max retries / frame             0
CRC errors                      0       Excessive retries               0
                                        Queue full discards             0
```

- **Buffer Full Frames Lost:** Number of frames lost due to a lack of buffer space in the unit.
- **Duplicate Frames:** Number of frames that were received more than once. This is usually due to a frame acknowledgment being lost.
- **CRC Errors:** Number of frames received with an invalid CRC. Usually caused by interference from nearby radio traffic. Occasional CRC errors can also occur due to random noise when the receiver is idle.
- **Retries:** A cumulative count of the number of times a frame had to be retransmitted due to an acknowledgment not being received.
- **Max Retries / Frame:** The maximum number of times any one frame had to be retransmitted. Excessive retries may indicate a poor quality radio link.
- **Queue Full Discards:** Number of times a packet was not transmitted due to too many retries occurring to the same destination. Discards will only occur if packets destined to this address are taking up more than their share of transmit buffers.

Displaying Sources Routes (Routes) (Token Ring Only)

The *route* option displays the Token Ring source routes to the LAN nodes that the radio node is communicating with. They may be displayed in ring order, node order, or as a single node.

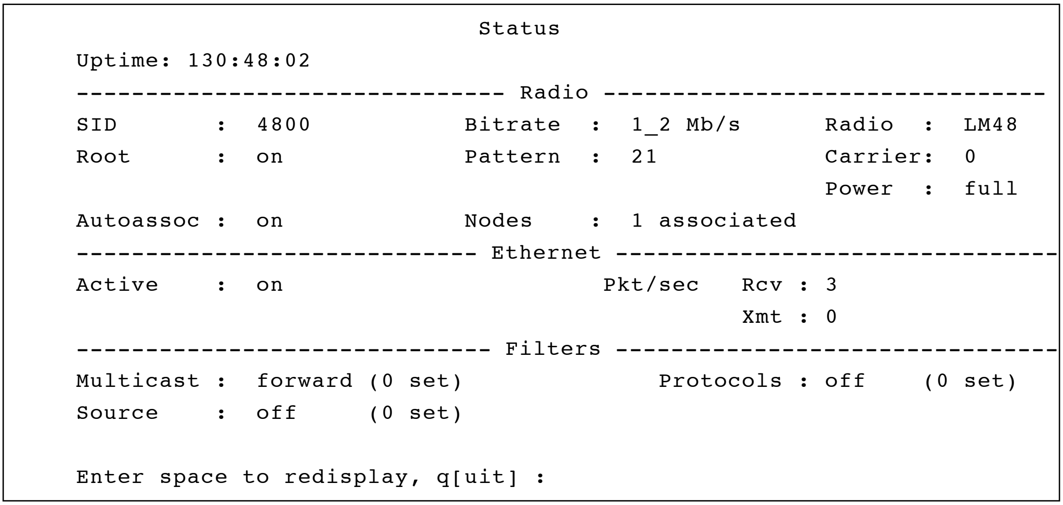
```
Ring Order
                    SOURCE ROUTES

Ring   20    40-1  1-1  20

  004096003532 0040960035e0 00409612a5e 00409610a23c 00409610c483
  004096206892  00409620afbd

Ring   2     40-1  1-1  30

  00409611134f

Ring 30      40-1  1-1  30

  00409610acd7     00409610e821

Address Order

                    SOURCE ROUTES

     Address       Route  (Ring-Bridge)
    -----------   -------------------------
    004096003532      40-1  1-1  20
    0040960035e0      40-1  1-1  20

  Single Address

                  SINGLE ROUTE
   004096003532      40-1  1-1  20
```

Displaying Overall Status (Status)

This display shows the settings of the most important configuration parameters of the Ethernet or Token Ring unit as well as important run-time statistics. Use the display to see if anything major is configured incorrectly. It is broken into sections describing:

- The radio
- Any LAN connections
- Any filtering being done

All items in the display are self explanatory or are explained in other sections of this manual.



```
                             Status
Uptime: 130:48:02
------------------------------- Radio ---------------------------------
SID       :  4800           Bitrate  :  1_2 Mb/s      Radio  :  LM48
Root      :  on             Pattern  :  21            Carrier:  0
                                                      Power  :  full
Autoassoc :  on             Nodes    :  1 associated
----------------------------- Ethernet ---------------------------------
Active    :  on                       Pkt/sec   Rcv : 3
                                                Xmt : 0
------------------------------ Filters ---------------------------------
Multicast :  forward (0 set)             Protocols : off    (0 set)
Source    :  off     (0 set)

Enter space to redisplay, q[uit] :
```

Recording a Statistic History (Watch)

Use the *watch* option to record the values of a chosen Ethernet or Token Ring statistic over time. Once you select a statistic and a time interval, the unit will start a timer. At each timer expiration, the unit will record the current value of the statistic. The last 20 samples are saved.

➔ **To Record a Statistic History:**

1. Select the *watch* option.

```
1. ra  Radio
2. re  Radio Error
3. et  Ethernet or Token Ring
4. ee  Ethernet or Token Ring Error
Enter category, one of [a number from 1 to 4, short form]:
```

2. Type the applicable category number and press **ENTER**. For example, if you choose “Radio” the following information would appear:

```
                    Radio

     Receive                        Transmit

     1 rpa Packets                  5 tpa Packets

     2 rby Bytes                    6 tby Bytes

     3 rfi Filtered                 7 ter Errors

     4 rer Errors

     Enter one of [a index from 1 to 7, a short form]:
```

3. Type the applicable statistic index number and press **ENTER**.

```
Enter a sample time in seconds from 1 to 3600 :
```

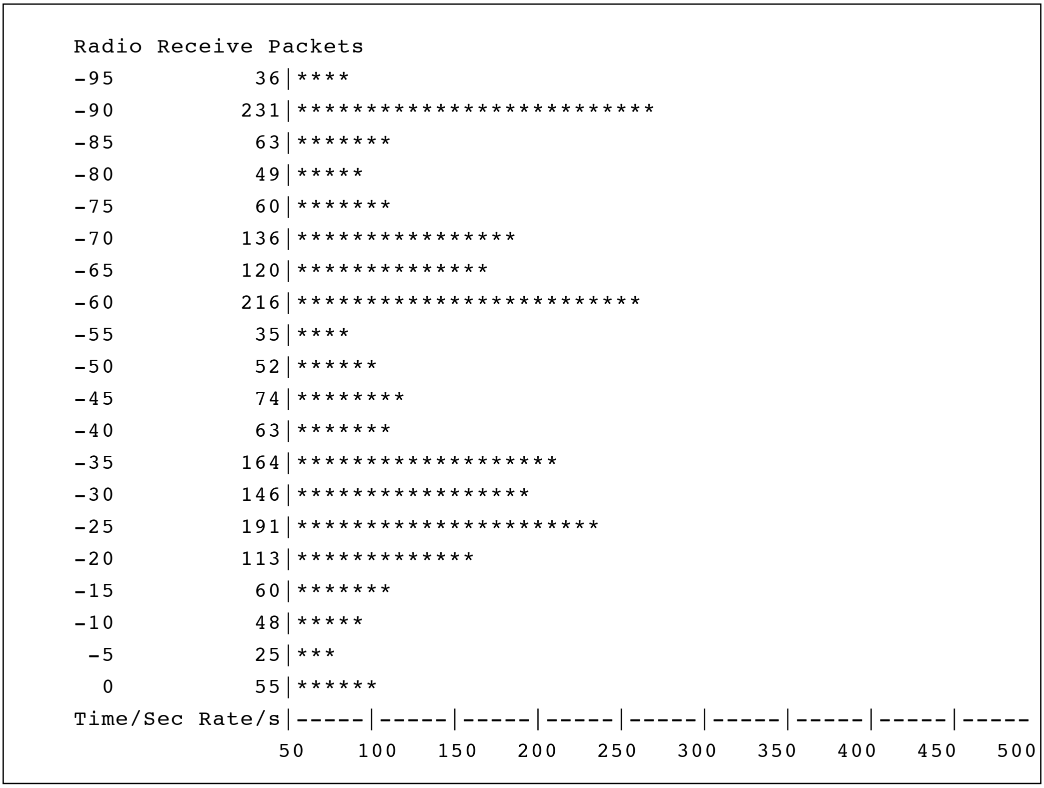
4. Type a time interval between samples and press **ENTER**. The longer time you specify, the further back in time the samples will be saved (to a maximum of 20 samples).

Displaying a Statistic History (History)

Use the *history* option to display the Ethernet or Token Ring history of the statistic that is currently being recorded.

➔ **To Display a Statistic History:**

1. Select the *history* option. Depending on your *watch* option selections a display screen similar to the one below will appear.



```
Radio Receive Packets
-95            36|****
-90           231|**************************
-85            63|*******
-80            49|*****
-75            60|*******
-70           136|****************
-65           120|**************
-60           216|*************************
-55            35|****
-50            52|******
-45            74|********
-40            63|*******
-35           164|*******************
-30           146|*****************
-25           191|**********************
-20           113|*************
-15            60|*******
-10            48|*****
 -5            25|***
  0            55|******
Time/Sec Rate/s|-----|-----|-----|-----|-----|-----|-----|-----|-----
               50    100   150   200   250   300   350   400   450   500
```

- **Time (sec)**: Displays the number of seconds elapsed from the time the statistic sample was recorded.
- **Rate/s**: Displays the actual value of the statistic. The chart will change scale based on the largest value displayed.

Displaying Node Information (Node)

The *node* command displays current Ethernet or Token Ring information about the client.

```
                            Radio Node Statistics
 ID   Address  Signal  Tx Pkt  Tx Byte  Tx Retry   Rx Pkt   Rx Byte   Rate
---   -------  ------  -----   -------  --------   ------   -------   -----
    004096128e76 45     1012     204322    39        1673    112386
     Enter space to redisplay, q[uit]:
```

- **Address**: Displays the address of the client.
- **Signal**: Displays the signal strength of the client.
- **Tx Pkt**: Displays the number of packets transmitted from the client.
- **Tx Byte**: Displays the actual number of bytes transmitted from the client.
- **Tx Retry**: Displays the number of transmitted packets that were resent by the client.
- **Rx Pkt**: Displays the number of packets the client has received.
- **Rx Byte**: Displays the actual number of bytes received by the client.
- **Rate**: Current bit rate used to transmit to the client.

Displaying ARP Information (ARP)

The *ARP* command displays the ARP table of IP address to MAC address. It also displays whether the node supports Ethernet Type II or IEEE 802.2 framing. The last column displays the time until the entry times out.

```
                     INTERNET ADDRESS TABLE
Internet Address  Network Address  ETHII   802.2     Time
----------------  ---------------  -----  ------  ----------
149.023.165.175      0000c0d9657f   Yes           0:14:57
149.023.165.040      0800099e0b1a   Yes           0:14:57
Enter space to redisplay, q[uit] :
```

Setting Screen Display Time (Display_Time)

Use the *display time* option to set the Ethernet or Token Ring time interval for the automatic redisplay of any repeating display. The default value is 10 seconds.

9

CHAPTER 9

Setting Up the Association Table

This chapter describes the procedures for setting up the Association Table for the Aironet Access Point.

Here’s what you’ll find in this chapter:

- Overview
- Using the Association Menu
- Displaying the Association Table
- Displaying the Association Table Summary
- Association Monitor Menu
- Setting the Allowed Number of Child Nodes
- Controlling Associations with Static Entries
- Specifying How Node Addresses are Displayed

Overview

Client nodes and repeater Access Points request to be associated with a parent Access Point so the parent will forward data frames. This exchange of radio packets passes back and forth information such as a node’s address, device, association type, and ASCII name. This information is entered into the Access Point’s association table along with the address of the parent Access Point. Each Access Point maintains entries in its table for all nodes associated to it and all nodes associated to any repeater serving it. There may be up to 2048 entries in the table.

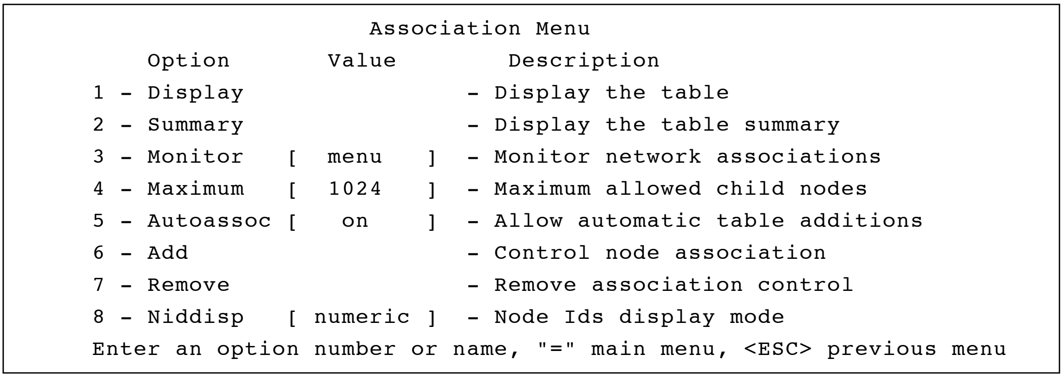
An Access Point will accept an association from any node that requests it. The operator may set up entries in the association table to control which nodes are allowed to associate. See “Association Monitor Menu (Monitor)”.

Using the information in the association table, the Access Point can perform a variety of traffic-control functions in moving packets to their proper destination on the infrastructure. When packets are received from the Ethernet or Token Ring or radio network, the Access Point will look in its table for the packet’s destination address and do one of the following:

- If the entry shows the radio node is associated to this unit, then the packet can be forwarded directly.
- If the entry indicates that the entry is associated to a repeater serving this unit, then the packet is forwarded to the repeater.
- If the address is not found, a root unit will forward the packet to the wired LAN, while a repeater will forward the packet to its own parent Access Point.

Using the Association Menu

The Association Menu contains options that allow you to view the table entries, add entries, and control the routing of packets on your radio network. To access this menu, select **Association** from the Main Menu.



```
                         Association Menu
    Option       Value        Description
1 - Display                 - Display the table
2 - Summary                 - Display the table summary
3 - Monitor   [  menu   ]  - Monitor network associations
4 - Maximum   [  1024   ]  - Maximum allowed child nodes
5 - Autoassoc [   on    ]  - Allow automatic table additions
6 - Add                     - Control node association
7 - Remove                  - Remove association control
8 - Niddisp   [ numeric ]  - Node Ids display mode
Enter an option number or name, "=" main menu, <ESC> previous menu
```

Displaying the Association Table (Display)

Use the *display* option to view the association table entries. Select "display" to enter the type of entries to be displayed.

- **All**: Displays all entries in the table.
- **Connected**: Displays only nodes that are actively connected to the Ethernet or Token Ring Access Point.

- **Hierachy**: A special shortened display which shows the association tree with children indented from their parents.
- **Static**: Displays only nodes for which a static entry has been made to control the nodes' association.
- **Multicast-filters**: Displays only those entries for multicast addresses for which filters have been added. See **Chapter 10** "Using Filters".
- **Node-filters**: Displays only those entries for node address for which filters have been added. See **Chapter 10** "Using Filters".

The typical hierarchy display will resemble:

```
                       RADIO HIERARCHY
Device                  Address   Name
-------------------- ------------ --------------------
AP4800E              00409611cd0e AP4800E_11cd0e
  AP4800T            00409611d1e5 AP4800T_11e701
    UC4500E          004096207206 UC4800E_207206
  AP4500E            00409611d602 AP4800E_11d602
    UC4800E          0040962068b0 UC4800E_2068b0
  LM4500             00409620222a
```

The rest of the displays will be similar to the one below.

```
                        RADIO NODES
   Address      Device  Type    Parent    Name               Src
------------- --------- ---- ------------ ------------------ ---
 00409611cd0e   AP4800E   Me              AP4800E_11cd0e     Fwd
 00409611d1e5   AP4500T  Rep        Local AP4800T_11e701     Fwd
N00409611d602   AP4800E  Rep        Local AP4800E_11d602     Fwd
 00409620222a    LM4500             Local                    Fwd
 0040962068b0   UC4800E      00409611d602 UC4800E_2068b0     Fwd
 004096207206   UC4800E      00409611d1e5 UC4800E_207206     Fwd
Enter space to redisplay, q[uit] :
```

- **Address Column**: Displays the address (in ascending numerical order) for each node on the infrastructure. An "N" before the address indicates that the node is a static entry and not associated. An "R" before the address indicates that the node is static and associated. The letters "N" and "R" only appear beside static entries.

- **Type Column**: Displays the node association type. The following types may appear in the table:

  Me: Represents this Aironet Access Point.

  Psp: Indicates the node that is using the Power Saving Protocol (PSP) to communicate with the system. Some radio nodes, usually wireless client devices, only power up part of the time to conserve energy. Therefor the Access Point must communicate to these nodes using PSP.

  Prnt: Indicates a repeater’s parent node.

  Rep: Indicates a repeater Access Point.

- **Parent Column**: Displays the node ID of the parent to which the node is associated. In place of a node ID, the column may display the following:

  A blank entry: The node is not associated.

  Local: The node is associated to this unit.

  Local block: The node has been blocked and will not be allowed to associate with the local system directly. See “Association Monitor Menu (Monitor)”.

- **Name Column**: Displays the node name.

  Rdst, Src: Displays the type of multicast filter action that has been set for Radio (RDst) and Source (Src) packets. A blank means that the action is forward. See **Chapter 10** “Using Filters”.

Displaying the Association Table Summary (Summary)

Use the *summary* option to view a summary of the number of nodes associated to your unit. When you select the *summary* option, the Association Table Summary Display appears:

```
                          ASSOCIATION TABLE SUMMARY
                               Non-Psp     Psp  Repeaters
                               ------- ------- ----------
      Direct associations   :        1       0          2
      Indirect associations :        2       0          0
```

- **Direct Associations**: Number of Non-PSP, PSP, or repeater nodes associated to this Access Point.
- **Indirect Associations:** Number of Non-PSP, PSP, or repeater nodes associated to Access Points below the current Access Point, on the radio network tree.

Association Monitor Menu (Monitor)

The commands in this menu allow you to monitor the location and movement of all of the radio nodes in the local infrastructure.

```
                 Association Monitor Menu
    Option    Value      Description
1 - Map                - Show network map
2 - Trace    [ off ]   - Trace network associations

Enter an option number or name, “=” main menu, <ESC> previous menu
>_
```

Displaying the Network Map (Map)

This command causes the Access Point to poll all of the other Access Points in the local infrastructure for information about the radio nodes associated to them. Nodes that are associated to parents are displayed one level from their parents on the display.

The other Access Points in the network are polled once every 30 seconds. Since all radio nodes will respond, this could generate a significant amount of traffic. You may not want to leave these displays running constantly.

```
                         NETWORK MAP
Device         Node Id       IP Address     Ver   Name
----------- ------------  ---------------  -----  -----------------
AP4800E     00409611cd0e  149.023.165.163  4.1G   AP4800E_11cd0e
  AP4500T   00409611d1e5  149.023.165.169  4.1G   AP4800T_11e701
    UC4800E 004096207206  149.023.165.176  4.1G   UC4800E_207206
  LM4500    00409620222a  149.023.165.238
AP4500E     00409611855b  149.023.165.160  4.1B   AP4500E_11855b
  LM4500    00409620222d
Enter space to redisplay, q[uit]:
```

The version column displays the firmware release level currently running on the unit. If the responding unit is connected to a Token Ring or an RS-485 LAN, then its LAN address is displayed after the name column.

Network Map (Trace)

This command builds a table similar to the Network Map Table but does not continuously display the table. Whenever the contents of the table changes, a log message appears indicating the changes. The command is most useful for watching the movement of the radio nodes through the infrastructure.

```
LM4800 202271 found associated to AP4800T 112c80
unit_112c80 Lobby_112c80 lost
```

NOTE: Press Enter to exit screen.

Setting the Allowed Number of Child Nodes (Maximum)

This command determines the maximum number of allowed child nodes that can be associated to the Access Point.

Controlling Associations With Static Entries (Autoassoc/Add/Remove)

Use the *auto-association* parameter and the static association table entries to control associations.

In its default configuration, the Access Point will allow any radio node in range to associate to it. For a more secure installation you must add static entries to the association table for these nodes. This allows control over which radio rodes are allowed to associate with which Access Point.

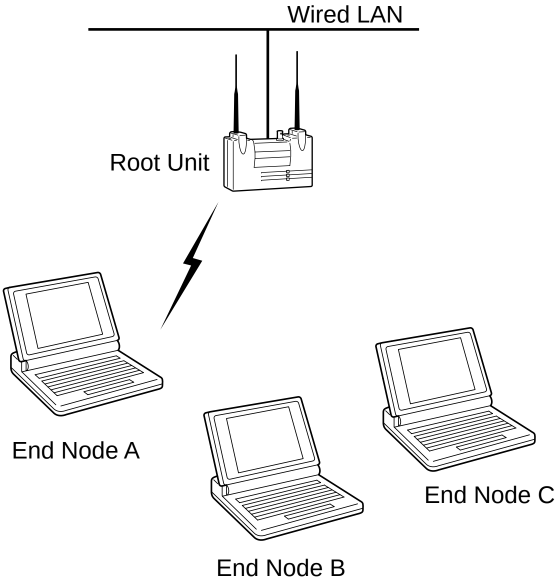
If *auto-association* is “On”, any radio node will be allowed to associate. If the parameter is “Off”, only nodes whose address matches a static table entry will be allowed to associate.

Static table entries are association table entries added manually by the operator and saved in the configuration memory. To add an entry, use the *add* option on the Association Menu. *Add* supplies the address of the node that is to be controlled.

For example, suppose there is an Access Point on your accounting LAN and three End Nodes (A, B, and C) within radio range of the Access Point. Only End Node A should be allowed access to the LAN.

1. Disable auto-association.
2. Add End Node A as a static entry. End Node A is allowed to associate to the root unit.
3. End Nodes B and C are not allowed to associate.

Figure 9.1 - Example of Using Static Entry to Restrict Association



As another example, suppose you only wanted to block End Node C and did not care about any other nodes. In this case you would leave auto-association “On” and add a static entry for End Node C to block it.

If you are going to use static entries to control associations, then the “association add all” command is a quick way to set up the table.

1. Leave auto-association “On” and let the nodes automatically associate to the Access Point.

2. Once they have associated, select *add* from the Association Menu and type “All”. All entries currently in the table are now made static.

3. Turn off auto-association. You can now remove extra entries or add missing entries manually.

Specifying How Node Addresses are Displayed (NIDdisp)

Use the *NIDdisp* option to specify how the node addresses are displayed on the Association Display Screen. The Aironet Access Point has the ability to display node addresses as follows:

- If you specify “numeric”, the addresses are displayed entirely in numeric form (default).
- If you specify “name”, the Organizational Unique Identifier (OUI) portion of the address (the first three bytes) is examined to see if it is one of the known types. If it is in the list, the first three bytes will be replaced by the name of the company that owns the OUI. Otherwise the numeric value is displayed. For example, the address of a SUN workstation could be displayed as either **080020ladecc** or **Sunladecc**.
- If you specify “tokenring” (Token Ring Only), all addresses will be displayed in Token Ring order. Addresses on a Token Ring are in reverse order from those on an Ethernet, making address matching difficult.

NOTE: If Niddisp is set to Token Ring, all addresses will be displayed in Token Ring order. However, all addresses entered as command options must still be entered in Ethernet order.

10

CHAPTER 10

Using Filters

This chapter describes how to control the forwarding of multicast messages.

Here’s what you’ll find in this chapter:

- Overview
- Using the Filter Menu
- Filtering Multicast Addresses
- Filtering Node Addresses
- Filtering Protocols
- Access Packet Direction

Overview

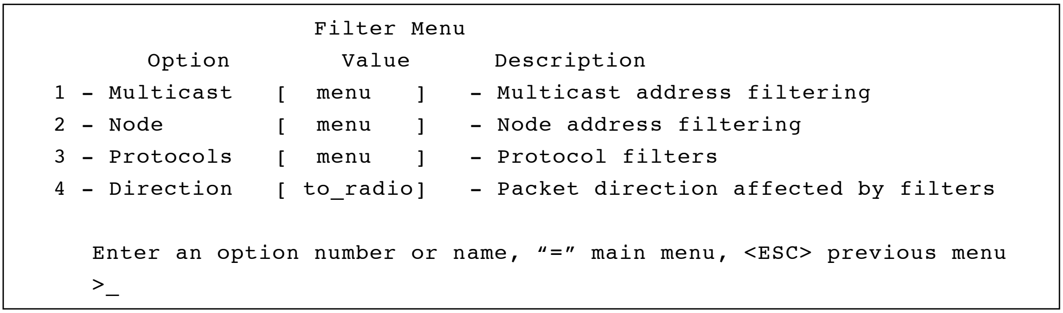
If your Aironet Access Point is connected to an infrastructure with a large amount of multi-protocol traffic, you may be able to reduce the amount of radio traffic by blocking out (filtering) those addresses or protocols that are not needed.

This filtering is especially important for battery operated radio nodes which might otherwise have to waste considerable battery power receiving multicast messages which are not relevant and will only be discarded.

Filtering is only applied to traffic coming from the wired LAN. No filtering is done of traffic coming from the radio nodes.

Using the Filter Menu

The Filter Menu is used to control the forwarding of data packets. To access this menu, select **Filter** from the Main Menu.

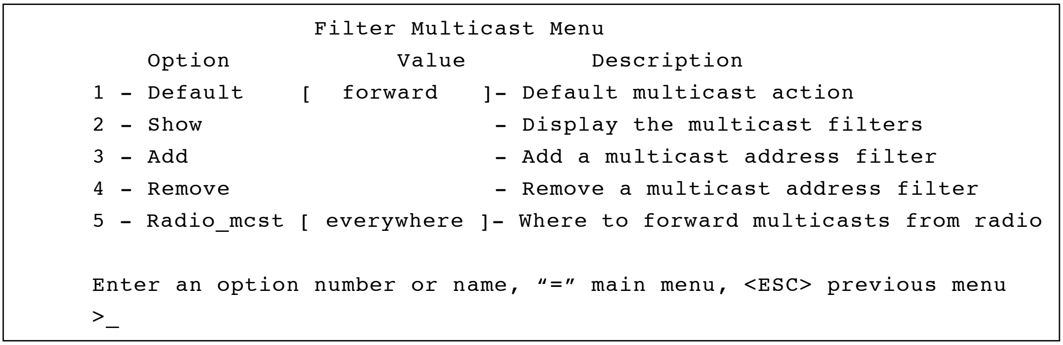


```
                      Filter Menu
          Option        Value      Description
   1 - Multicast   [  menu   ]   - Multicast address filtering
   2 - Node        [  menu   ]   - Node address filtering
   3 - Protocols   [  menu   ]   - Protocol filters
   4 - Direction   [ to_radio]   - Packet direction affected by filters

      Enter an option number or name, "=" main menu, <ESC> previous menu
      >_
```

NOTE: In order to achieve consistent performance on your infrastructure, any configurations that you set in the Filter Menu should be duplicated on all Aironet Access Points. This maintains consistency as nodes roam.

Filtering Multicast Addresses (Multicast)

The multicast menu allows you to control the filtering of multicasts based on the actual multicast address. When you select the *Multicast* option the Filter Multicast Menu appears.



```
                  Filter Multicast Menu
    Option            Value         Description
1 - Default    [  forward   ]- Default multicast action
2 - Show                     - Display the multicast filters
3 - Add                      - Add a multicast address filter
4 - Remove                   - Remove a multicast address filter
5 - Radio_mcst [ everywhere ]- Where to forward multicasts from radio

Enter an option number or name, “=” main menu, <ESC> previous menu
>_
```

Setting the Default Action (Default)

The *default* option controls the filtering of multicasts whose address is not in the table. You may pick one of the following actions:

- **Discard**: Multicasts with no table entries will not be forwarded out the radio network.
- **Forward**: Multicasts with no table entries will be forwarded out the radio network.
- **Accesspt**: Multicasts with no table entry will only be forwarded to other Access Points and Bridges, not to the client nodes.
- **Nonpsp**: Multicasts with no table entries will be forwarded out the radio network to non-power saving end nodes, not to any nodes using the PSP.

Displaying The Filters (Show)

Use the *show* option to display the multicast filters. When you select the *show* option the Multicast Filters screen appears.

The filters are stored in the association table. The display of the multicast filters follows the format of the normal association display. At the end of each line the filter action for each address will be displayed.

This same display may also be produced with the “association display” command with either the “all” or “multicast-filters” information. See **Chapter 9** “Setting Up the Association Table”.

```
                          MULTICAST FILTERS
       Address       Device  Type    Parent    Name
    ------------- --------- ---- ------------ ------------------
    N010203040506      Mcst                                         forward
```

Adding A Multicast Filter (Add)

Use the *add* option to add a multicast filter if there are special multicast addresses you want to filter differently than the default. You will first be prompted for the address and then for an action to be applied to this address only.

Removing a Filter (Remove)

Use the *remove* option to remove one or all of the non-default filters. The action for the removed entries will revert to the default action.

Filtering Radio Multicasts (Radio_Mcast)

If you know that the radio nodes are not going to communicate with each other, but will only communicate with nodes on the wired LAN, set this parameter to “lan_only”. With this setting multicasts received from the radio nodes are not re-broadcast to the radio cell but are forwarded to the wired LAN.

For example, if you have a system with a large number of radio clients which only talk to the network server, enabling multicast filtering will result in much less radio traffic congestion.

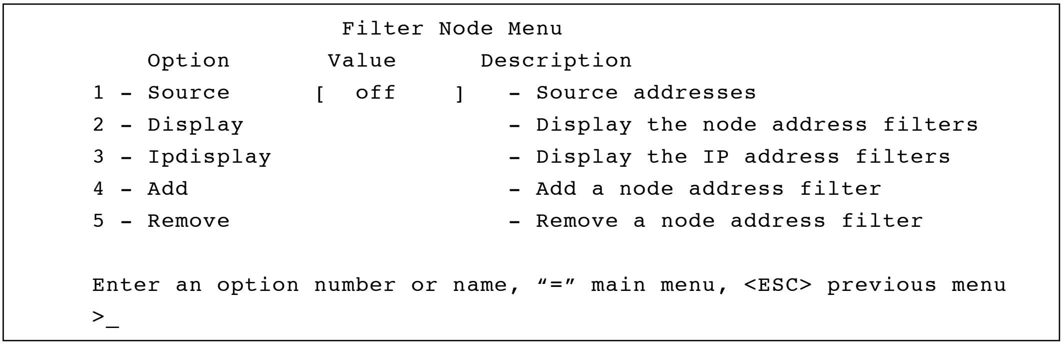
If the parameter is left at the default setting of “everywhere”, then radio nodes may broadcast to each other.

Filtering Node Addresses (Node)

The *node* option allows you to control the forwarding of packets based on the source node addresses. As with multicast filtering, there is a default action for those addresses not in the table. You may enter actions for specific addresses to override the default action.

Specific node filters may be entered by specifying either the 6 byte infrastructure address of the node or by specifying its IP address. If the IP address is used, the Aironet Access Point will determine the infrastructure address associated with the IP address and use this for the actual filtering.

You may filter packets based on the source address in the received packet. For example, if you wanted to prevent all but a limited number of hosts to communicate with nodes on the radio network, you would set the default action to discard. Then add entries for the specific hosts whose action is “forward”.



```
                  Filter Node Menu
    Option       Value      Description
1 - Source      [  off    ]   - Source addresses
2 - Display                   - Display the node address filters
3 - Ipdisplay                 - Display the IP address filters
4 - Add                       - Add a node address filter
5 - Remove                    - Remove a node address filter

Enter an option number or name, “=” main menu, <ESC> previous menu
>_
```

Setting the Default (Source)

The default applies to those packets whose address does not have an entry in the filter table.

Source address filtering is “Off” by default. This saves processing power since the unit has to look up the source address of each incoming packet to see if a filter is to be applied. Before any individual source filters can be made active, one of the other values for the default must be chosen. You may set the action to:

- Off (no filtering is done)
- Forward
- Discard

Displaying The Node Address Filters (Display)

Use the *display* option to view the table of controlled addresses. The filters are stored in the association table so that they may be accessed quickly. The display of the filters follows the format of the normal association display. At the end of each line the filter action for each address will be displayed.

This same display may also be produced using the “association display” command with either the “all” or “multicast-filters” information. See **Chapter 9** “Setting Up the Association Table”.

```
                         NODE FILTERS
   Address      Device  Type    Parent    Name                 Src
------------- --------- ---- ------------ ------------------ ---
N000102030405     Unkwn                                          Fwd
Enter space to redisplay, q[uit]:
```

Displaying the IP to Network Address Table (IPdisplay)

When a node address filter is entered by IP address, the Aironet Access Point first determines the infrastructure address associated with this IP address. The actual filtering is done based on the network address.

```
                  IP ADDRESS FILTERS
   IP Address    MAC Address Src
--------------- ------------ ---
149.023.165.186  004096206892 Fwd
Enter space to redisplay, q[uit]:
```

Updating Specific Node Address Filters (Add/Remove)

Use the *add* option to add filters for specific addresses to the filter table.

You will be prompted for the infrastructure address or IP address of the node to which the filter applies. You will then be asked for the filter action to be applied to this address which may be:

- Filter
- Discard

To remove one or all specific node filters use the *remove* option. You may enter either the keyword "all", a single nodes infrastructure address, or a single node's IP address. Once removed, the filter action for the removed addresses will revert to the default value.

Filtering Protocols (Protocols)

Protocol filtering bases the filtering decision on the type of protocol used to encapsulate the data in the packet. This type of filtering can have the most value in almost all situations and is the preferred method of filtering. With this type of filtering you may set the Aironet Access Point to only forward those protocols, over the radio, that are being used by the remote radio nodes. Selecting protocols is easier than setting up filters based on addresses.

The Aironet Access Point may be set up to monitor and record the list of protocols currently being forwarded over the radio. It will record the protocols found, how may packets were encountered and whether the packet came from the LAN or the radio.

To set up the protocol filters, start the monitor and let it run for a while under normal use. Add filters by selecting the protocols from the monitor list.

There is a default action for those protocols not in the list of explicitly filtered protocols. If you know exactly which protocols are going to be used by the radio nodes, set the default action to discard and add filters to forward only those protocols that will be used. If you are not sure of all the protocols that will be used but you know that there are certain protocols you will not use, you would set the default to forward and add filters to discard only those protocols you will not use.

For filtering purposes the Access Point assumes that the data portion of the packets is in one of two forms:

- The first 16 bits of the data portion contains a value that is greater than the maximum data size (1500). The value is assumed to be a protocol identifier that may be used to determine which protocol is being used within the packet.
- The first 16 bits of the data portion contains a value that is less than the maximum data size. The value is interpreted as a frame length and it is assumed that a IEEE 802.2 Logical Link Control (LLC) header follows the length.

The format of the LLC header is as follows:

DSAP, 8 bits, Destination Service Access Point (DSAP)

SSAP, 8 bits, Source Service Access Point (SSAP)

CTL, 8 bits, Control field

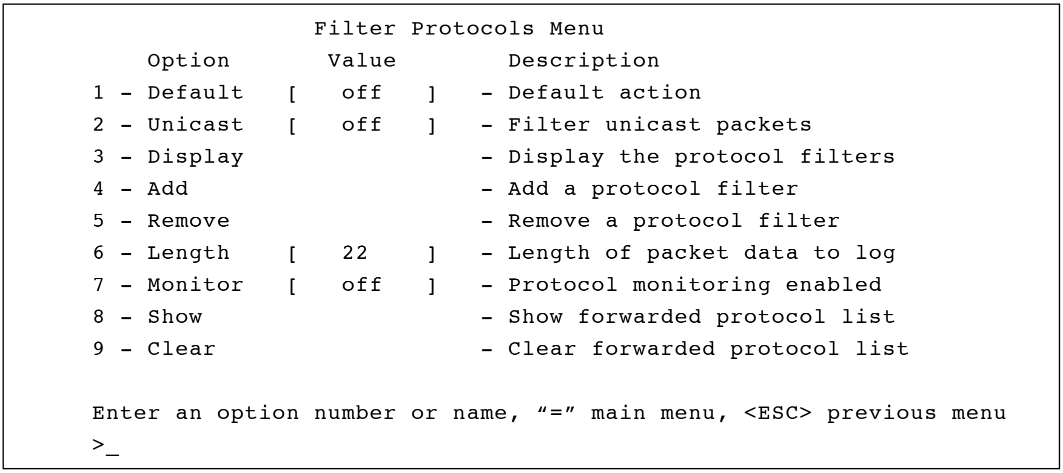
If the control field has a value 3 (for an un-numbered information frame), then this header may be followed by:

OUI, 24 bits, Organization Unique Identifier (OUI)

SAP-PROT, 16 bits, Protocol Identifier

You may set up filters based on either a protocol identifier or a DSAP/SSAP combination. If the filter is based on SAPs, and the control field has a value of 3, the packet may also be optionally filtered based on the OUI and LLC protocol fields.

Both types of filters may also use a variable length bit mask of the packet contents to further specify which packets should be filtered.



```
                Filter Protocols Menu
    Option       Value        Description
1 - Default   [   off   ]   - Default action
2 - Unicast   [   off   ]   - Filter unicast packets
3 - Display                 - Display the protocol filters
4 - Add                     - Add a protocol filter
5 - Remove                  - Remove a protocol filter
6 - Length    [   22    ]   - Length of packet data to log
7 - Monitor   [   off   ]   - Protocol monitoring enabled
8 - Show                    - Show forwarded protocol list
9 - Clear                   - Clear forwarded protocol list

Enter an option number or name, “=” main menu, <ESC> previous menu
>_
```

Setting the Default Action (Default)

The *default* action is used for a packet whose protocol does not match any entry found in the table. It may be set to:

- **Off**: Protocol filtering is not done. It is a waste of processing power for the unit to examine each packet for its protocol only to discover no protocols need monitoring.
- **Discard**: The packet will not be forwarded out the radio network.
- **Forward**: The packet will be forwarded out the radio network.
- **Accesspt**: The packet will only be forwarded to other Access Points and Bridges and not to the client nodes.
- **Nonpsp**: The packet will be forwarded out the radio network to non-power saving end nodes and not to any nodes using PSP.

Enabling Unicast Packet Filtering (Unicast)

By default, the Aironet Access Point only applies the protocol filters to multicast packets. If a packet is directed to a radio node, it is likely the protocol in the packet is being used by the radio node. If you want to use the protocol filters as a security measure, you may set the option to “On” to ensure that all packets of a given protocol will be filtered.

Displaying the Filters (Display)

Use the *display* option to view the list of protocol filters you have added.

```
                       PROTOCOL FILTERS
                                   ----------LLC--------- Masks
     Name       Action   Protocol  SAPs   OUI    Protocol
-------------- --------  --------  ---- ------  ---------
 1. novell      discard    8137
 2. novell      discard            aaaa  000000    8137
 3. novell      discard            e0e0
 4. Ethertalk   discard            aaaa  080007    809b
 5. IPX-RIP     discard            ffff                   18- 0453, 0
Enter space to redisplay, q[uit]:
```

Name: The name assigned to the protocol.

Action: The action that has been assigned for each protocol.

Protocol and LLC: The protocol header.

Masks: A bit mask applied to the packet that must match the packet contents before the protocol is identified. The mask is displayed in the following form:

18- (start position),   0453 (value), 0 (don’t care mask)

Adding A Filter (Add)

Use the *add* option to add a protocol filter and specify the type of action required. There are several ways to add a filter:

- Predefined filter
- Manually add all the data
- Use an entry from the monitor table built by the unit

➔To Add a Predefined Filter

1. Select the *add* option.
2. Select one of the predefined strings: inet, novell, or netbios. The inet filter adds filters for both the IP and ARP protocols. The novell filter adds filters for all the types of allowed novell protocol headers.
3. You will then be prompted for the action to take when the protocol is encountered. Enter one of the actions described under the default setting above, with the exception of “Off”.

The following display shows the results if all predefined filters were added.

```
                                   ----------LLC---------
     Name       Action   Protocol  SAPs   OUI    Protocol
-------------- --------  --------  ---- ------  ---------
 1. novell      discard    8137
 2. novell      discard            aaaa  000000    8137
 3. novell      discard            ffff
 4. novell      discard            e0e0
 5. inet        forward    0800
 6. inet        forward            aaaa  000000    0800
 7. inet        forward    0806
 8. inet        forward            aaaa  000000    0806
 9. netbios     forward            f0f0
```

➔ To Add a Filter Using the Monitor

If protocol monitoring has been enabled, once you select the *add* command, the current monitor table will be displayed. To select a monitored protocol:

1. Enter the number displayed at the start of each line of the monitor display.

2. If the monitored protocol was un-recognized and was not given a name, you will then be prompted to assign a name.

3. You will be prompted for the action to take when the protocol is encountered. Enter one of the actions described under the default setting above, with the exception of “Off”.

➔To Add a Filter Manually:

To start adding a filter manually:

1. Enter the *add* command and give the filter a name that does not start with a number and does not match one of the pre-defined names.

2. You will be prompted for the action to take when the protocol is encountered. Enter one of the actions described under the default setting. If this value is chosen, the packet is not filtered, and the contents of the data portion of the packet are displayed in an information log. See “Length of Data Displayed in Log Action (Length)”.

3. Choose whether the protocol is defined by an Ethernet or Token Ring protocol identifier or by a LLC header.

If you type “protocol”:

a. The following prompt appears:

```
Enter a value in hex from 200h to ffffh :
```

b. Type the value for the protocol identifier to be filtered and press **ENTER**.

```
Enter one of [a mask start position, none] :
```

This allows you to specify a bit mask and corresponding hexadecimal value to be applied to the packet. These two values must match the packet contents before the protocol is identified.

You must first specify a mask start position in the packet and match the mask value. The mask start position value should be a 0-based byte offset from the start of the data portion of the frame (after the MAC layer header). If you set the position to “none”, no mask is tested.

c. Type a mask start position value (or “none”, if applicable) and press **ENTER**.

```
Enter a hex value of 1 to 30 characters :
```

d. Type the value to be matched as a string of up to 30 hexadecimal digits and press **ENTER**. If the numbered digits is odd, the mask value will be adjusted to ignore the low 4 bits of the corresponding byte.

```
Enter a hex don’t care mask of 1 to 6 characters :
```

This allows you to enter a string of hexadecimal digits to indicate which bits of the packet data are meaningful.

A bit set in this value causes the corresponding bit in the packet to be ignored. Therefore, a 0 mask means that the packet contents must exactly match the previous value entered. If the mask entered is shorter than the value entered it is automatically extended to the correct length with zeros.

e. Type the applicable hexadecimal digits and press **ENTER**.

For example, to enter a mask that matches the value 4128H in the 16th byte data portion of the packet and have the high bit of each byte ignored, complete as follows:

```
Enter one of [a mask start position, none] : 15

Enter a hex value of 1 to 30 characters : 4128
Enter a hex don’t care mask of 1 to 4 characters :
8080
```

If you type **llc**:

a. When you select **llc**, the following prompt appears:

```
Enter a value in hex of ffffh or less :
```

b. Type a 16 bit value for the DSAP/SSAP combination (with the DSAP being in the high 8 bits) and press **ENTER**.

```
Enter one of [a OUI value in hex of ffffffh or
less, any] :
```

This is used to specify an OUI value to further refine the protocol identification.

If you enter “a OUI value in hex of ffffffh or less”, it must match the protocol field in addition to the SAP value.

If you enter “any”, then the protocol values are not checked and the protocol is defined only by the SAP values.

c. Type the applicable OUI value or “any” and press **ENTER**. If you typed an OUI value, the following appears:

```
Enter one of [a LLC protocol value in hex of ffffh
or less, any] :
```

This is used to specify a LLC protocol identifier.

If you enter “a LLC protocol value in hex of ffffh or less”, it must match the protocol field in addition to the SAP and OUI values.

If you enter “any”, then the protocol values are not checked and the protocol is defined only by the SAP and OUI values.

d. Type the applicable LLC protocol value or “any” and press **ENTER**.

e. You will be prompted for a mask description as described in the protocol section above.

Removing an Entry (Remove)

Use the *remove* option to remove a protocol filter entry. You may either remove all filters by entering the keyword “all” or a single entry by entering the number assigned to the filter and shown at the start of the line in the filter display.

Length of Data Displayed in Log Action (Length)

Use the *length* option to display the contents of packets being forwarded to the radio.

Use this option to setup the filter mask values to properly narrow down which packets are filtered.

If you add a protocol filter whose action is “log”, each time the filter matches, the contents of the data portion of the packet (after the MAC header) will be displayed on the console (in hex) for a length in bytes determined by the value of this option.

The contents of the data portion displayed in the information log will consist of:

- “p”
- Id number of the filter shown on the Protocol Filters screen
- Bytes of the packet displayed in hexadecimal

More than one protocol at a time can be set with a filter action of “Log”.

The following is an example of a protocol filter log entry:

```
p2: 01 e0 ff ff 01 eo 00 04 00 00 01 65 ff ff ff ff ff
ff 04 52 00 00
```

Protocol Monitoring (Monitor/ Show/ Clear)

The Aironet Access Point allows you to create and display a list of the protocols currently being forwarded by the unit. This allows you to test if packets that contain data for unused protocols are being forwarded to the radio nodes.

Once enabled by the *monitor* option, the Aironet Access Point will then begin to examine the protocol used in each packet forwarded. If the protocol is not already in the list, an entry is created. Otherwise, the packet count for the given protocol is incremented.

The *show* option will display the list of currently forwarded protocols.

```
                        PROTOCOLS FOUND
                                            --------LLC----------
      Name      Source      Count Protocol  SAPs   OUI   Protocol
--------------- ------- --------- --------  ---- ------- --------
  1. IP         RadLan       7207   0800
  2. ARP        RadLan        782   0806
  3. NetBIOS    Lan            39           f0f0
  4. ARP        RadLan         63           aaaa  000000   0806
  5. DEC MOP    Lan             3   6002
Enter space to redisplay, C[lear stats], q[uit] :
```

- **Name**: If the protocol is recognized, it will be given a name. Otherwise, the name field is left blank.
- **Source**: This will contain the string “Rad” if a packet was received from the radio and “Lan” if a packet was received from the wired LAN.
- **Count**: Displays the number of times a packet with the given protocol was encountered.
- **Protocol and LLC**: The protocol header found.

You may clear the list of found protocols either with the “clear” command or by entering a “C” (case sensitive) at the re-display prompt of the “show” command.

Access Packet Direction (Direction)

Use the *direction* options to control the direction a packet is traveling before affected by the filters.

- **To_radio**: Only packets from the LAN will have filters applied. Packets from the radio will not be filtered. This options reduces the amount of LAN traffic to the infrastructure.
- **Both**: Packets in both directions will be filtered. This option allows control of the type of traffic the radio nodes may use.

11

CHAPTER 11

Setting Up Event Logs

This chapter describes how to use the Logs Menu to setup and view event logs on the Aironet Access Point.

Here’s what you’ll find in this chapter:

Overview

The Aironet Access Point produces logs that record the occurrence of significant events occurring within your unit and on the infrastructure. The type of events that are recorded as logs are:

- **Information Logs**: Records status changes that occur in the normal operation of the system. For example, when an end node associates to an Aironet Access Point.
- **Error Logs**: Records errors that occur occasionally, but are easily recovered from by the unit. For example, errors that occur during the reception and transmission of packets to and from the unit.
- **Severe Error Logs**: Records errors which drastically affect the operation of the system. The system will continue to run, but action is required to return the unit to normal operating standards.

Information Logs

All logs apply to both Ethernet and Token Ring unless indicated.

BOOTP/DHCP set new IP address

The BOOTP/DHCP server answered the request and assigned the unit an IP address different than the configured value.

Ethernet or Token Ring disabled due to root mode disable

When a root unit is changed to a repeater, it will not route traffic through any wired LAN connection on the unit. The Ethernet or Token Ring connection is disabled by default.

The connection can be enabled by operator command, however, it may only be used to communicate with the Access Point to do downloads or telnets.

Ethernet or Token Ring enabled due to root mode enable

When a repeater is changed to a root unit, the Ethernet or Token Ring Port will be enabled by default. It can be disabled by operator command.

Inserted into the Token Ring (Token Ring Only)

The unit has successfully inserted itself into the Token Ring and is ready to transmit and receive frames.

Node “node address” “device name” added

A non-volatile entry was added to the association table.

Node “node address” “device name” added locally “ASCII name”

A new node associated with the local unit.

Node “node address” “device name” restarted “ASCII name”

A node that is currently associated to the local unit was reset.

Node “node address” “device name” “ASCII name” removed, max radio retries

A node was removed from the table because a response was not received from the node after attempts were made to transmit a packet to it. The node may have failed or it moved to another cell.

Node “node address” “device name” “ASCII name” removed, staled out

A node was removed from the table because data was not received from the node within the stale-out period. Different devices have different stale-out times. PSP nodes have very short stale-out times (around 10 seconds). Non-PSP nodes have longer times (usually several minutes).

Node “node address” “device name” “ASCII name” removed, NV removed

A node was removed from the association table because the operator used the “association remove” command.

Node “node address” “device name” “ASCII name” removed, deassoc notice from “address”

The node was removed from the association table because another Access Point reported that it now has the node associated locally. This log is produced whenever a node handoff occurs.

RARP set new IP address

A RARP server answered a request for an IP address with an address different from the one currently saved. The currently saved value is overwritten.

Associated to router “node address”

This log is produced when the unit, configured as a repeater, associates to its parent node.

Removed from the Token Ring (Token Ring Only)

This log is produced when the connection to the Token Ring is removed. This could be the result of an operator command or a ring error. If it was the result of an error, the unit will immediately try to reopen the ring.

SNMP: “command text”

A SNMP management station sent the unit a “set” variable request which was successfully executed. The “command text” is a similar menu command that has the same effect as the SNMP request.

SNMP access failure from “community name” “IP address” (node address)

A SNMP management station attempted to access the SNMP agent with an invalid community name or a name that it was not allowed to use.

TFTP is loading “file name” from “ip address”

This log is produced when the BOOTP server gives the Aironet Access Point the name of a configuration file and then the name of a firmware file to load.

Error Logs

“Category” Error: nnn “type” errors

This log is produced when any error occurs that is marked by an asterisk “*” after its count in the statistics displays. These errors are serious enough to affect the operation of the unit. See the sections on each display for an explanation of each error.

Node “node address” “device name” “ascii name” removed

These logs are similar to the information logs except that the node removed is an Access Point. Since these nodes do not normally roam, it may be an indication that contact with a child repeater is lost.

Asoctable is full

The association table is completely full. To troubleshoot, try to force some radio nodes to associate to other Access Points on the LAN using the specified router field in their association table.

Unable to locate IP address “ip address”

The unit was trying to send a packet to an IP address without knowing the hardware node ID. When this occurs, the unit will use the ARP protocol to try to determine the proper address. This log is produced if there was no answer to the ARP request. Usually the unit is trying to find the destination for the SNMP traps.

Severe Error Logs

Ethernet or Token Ring cabling problem

If no traffic has been sent or received on the Ethernet or Token Ring cable in the last 10 seconds, the unit will send a packet to itself to test the connection. If the transmission succeeds, the timer is reset. If it fails, this log is produced and traffic for the connection will be discarded until the test succeeds.

Becoming repeater due to Ethernet or Token Ring cable fault

If “config Ethernet (or Token Ring) fallback” parameter is enabled and a cable fault has been detected on the wired LAN, the unit will become a repeater to try and find another root to associate as well as maintain a path to the wired LAN.

Becoming root due to Ethernet or Token Ring cable connection

If “config Ethernet (or Token Ring) fallback” parameter is enabled and a cable fault was detected and has now been repaired, the unit will revert to being a root to provide the shortest path access to the wired LAN.

Configuration is too large to save

The number of commands in the configuration is too large for the available non-volatile memory. This may be caused by too many non-volatile entries in the association table.

Could not program the flash memory

An error occurred when trying to program a new version of the firmware into flash memory. The unit must be serviced.

Lost our association, max radio retries

The unit, configured as a repeater, lost communications with its parent node after trying to send a packet the maximum number of times. The unit will try to re-associate. The problem may be a parent Access Point failure. All local associations will be dropped.

Lost our association, max radio naks

The unit, configured as a repeater, lost communications with its parent node after trying to send a packet the maximum number of times. Each time the unit sent a packet, it received a response indicating that the parent's receive buffers were full. The unit will try to re-associate. The likely cause is that the parent is handling too much traffic. All local associations will be dropped.

Lost our association, radio restarted

A radio configuration parameter has been changed. All associations will be dropped and the radio will be restarted.

Lost our association, changed repeater mode

A unit has changed from a root to a repeater or vice versa. If the unit is now a root unit, it will wait for nodes to associate to it. If the unit is now a repeater, it will attempt to associate to a parent.

Lost our association, new specified router

The specified router parameter of this repeater has been changed. The unit will drop its current association and try to re-associate.

Lost our association, NAK from router

The unit thought it was associated to its parent, however, the parent is not aware of the association. The unit will attempt to re-associate. The parent may have been rebooted.

No response to radio loopback test

The “config radio extended test” command was set on and no Access Point in range responded to the loopback test. If you know there are units in range, then either the local radio has failed, or if there is only one remote in range, then the remote unit's radio may have failed.

Radio Configuration Error nn

The Aironet Access Point could not program the radio hardware to operate at the correct frequency and bit rate. Have the unit serviced.

Radio loopback test succeeded

After having failed, the radio loopback test heard a response from a remote.

The address PROM is invalid

Each unit contains a Programmable Read-Only Memory (PROM) chip that contains the unit’s hardware address. During power up the unit was not able to read a valid address from the PROM. The unit must be serviced.

Token ring open failed, loopback failed (Token Ring Only)

Before it inserts into a ring, the unit attempts to send a packet to itself, looped back through the wiring concentrator. This message may denote a cabling problem.

Token ring open failed, signal loss (Token Ring Only)

Before the unit inserts into a ring, the unit needs to see certain signals on the interface cable, which were not present or were lost. This message may denote a cabling problem.

Token ring open failed, timeout (Token Ring Only)

The ring insertion procedure took longer than 18 seconds.

Token ring open failed, ring failure (Token Ring Only)

The unit was unable to receive a packet it sent to itself after it inserted into a ring. There may be a problem in the ring at or beyond the wiring concentrator.

Token ring open failed, ring beaconing (Token Ring Only)

A unit on the ring detected a hard error (on the ring) and transmitted a frame to inform all other units.

Token ring open failed, duplicate address (Token Ring Only)

Another station on the ring is using the same node ID as that assigned to the local unit. This could only happen if this or other units in the network have had their node ID's locally assigned with the "config id nid" command.

Token ring open failed, request failed (Token Ring Only)

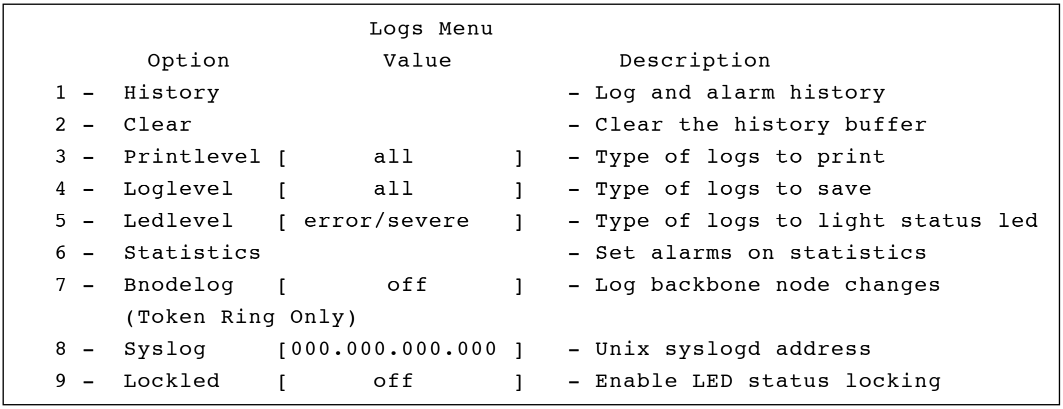
The unit found a parameter server on the ring, but the server did not respond to a request.

Token ring open failed, remove received (Token Ring Only)

Some other unit on the ring sent a remove adapter frame to this unit causing it to remove itself from the ring.

Using the Logs Menu

The event logs are viewed using the Logs Menu shown below. To access this menu, select **Logs** from the Main Menu.



```
                          Logs Menu
         Option            Value            Description
   1 -  History                         - Log and alarm history
   2 -  Clear                           - Clear the history buffer
   3 -  Printlevel [      all       ]   - Type of logs to print
   4 -  Loglevel   [      all       ]   - Type of logs to save
   5 -  Ledlevel   [ error/severe   ]   - Type of logs to light status led
   6 -  Statistics                      - Set alarms on statistics
   7 -  Bnodelog   [       off      ]   - Log backbone node changes
        (Token Ring Only)
   8 -  Syslog     [000.000.000.000 ]   - Unix syslogd address
   9 -  Lockled    [      off       ]   - Enable LED status locking
```

Viewing History Logs (History)

Use the *history* option to view history logs of events that have occurred on the unit and the infrastructure. All logs are stored within the unit in a 10KB memory buffer. The actual number of event logs the unit saves will depend on the size of each log stored in the buffer.

Log entries are always displayed in a least recent to most recent order. If the memory buffer becomes full, the oldest log in the buffer will be replaced by the latest.

Only logs that have occurred since the unit was last powered up or since the memory buffer was cleared will be saved. See “Clearing the History Buffer (Clear)”.

NOTE: If a power failure occurs, the logs contained in the memory will not be saved.

The display will be similar to the following:

```
OLDEST
0:00:00 I Node 004096109e30 APBR2000-E Floor_2_109e30 added locally
0:00:03 I Node 0040961064de AP2000-E F3_1064de added for 004096109e30
30:35:09   NEWEST, cleared at 0:00:00
b[ackward], f[orward], n[ewest], o[ldest], a[ll], C[lear], q[uit] :
```

- **First Line**: “OLDEST” indicates the end of the buffer display. This will appear at the end of the history log.
- **Display Lines**: Displays the time since power-up that the log occurred, the severity level (I-information, E-error, or S-severe) and the actual log text.
- **Last Line**: Indicates the current time and the time the buffer was last cleared by the operator. “NEWEST” indicates the start of the history log.

- **Option Line**: Indicates the movement keys to use when viewing the history logs. Since displaying the entire history will take more than a screen page, use the following keys to navigate through the history log:

  b: Back one page in the log

  f: Forward one page in the log

  n: Moves to the newest log entry

  o: Moves to the oldest log entry

  q: Exit the History Log screen

  a: Dump entire log (usually captured to a file on a PC)

Clearing the History Buffer (Clear)

Use the *clear* option to delete all logs from the history buffer.

Specifying the Type of Logs to Print (Printlevel)

Use the *printlevel* option to specify the type of event logs to appear on the Console screen. You will know immediately when an error or information event has occurred and then take the necessary action required.

There are four levels of logging:

- **Error/Severe**: Displays all error and severe logs.
- **Severe**: Displays severe error logs only.
- **All**: Displays all error, severe and information logs.
- **Off:** No event logs will be displayed.

Specifying the Type of Logs to Save (Loglevel)

Use the *loglevel* option to specify the type of logs you want to save to memory and view on the History Log screen.

There are four levels of logging:

- **Error/Severe**: Displays all error and severe logs.
- **Severe**: Displays severe error logs only.
- **All**: Displays all error, severe, and information logs.
- **Off:** No event logs will be displayed.

See “Specifying the Type of Logs to Print (Printlevel)”.

Specifying the Type of Logs to Light Status Indicator (Ledlevel)

Use the *ledlevel* option to have the indicator status light turn amber when a specific type of error log occurs.

There are four levels of logging:

- **Error/Severe**: Displays all error and severe logs.
- **Severe**: Displays severe error logs only.
- **All**: Displays all error, severe and information logs.
- **Off:** No event logs will be displayed.

See “Specifying the Type of Logs to Print (Printlevel)”.

Setting Statistic Parameters (Statistics)

This command allows you to control how alarms are generated based on any of the available statistics kept by the Access Point. Logs may be:

- Disabled for statistics
- Generated if the statistic changes at all
- Generated if the statistic changes at a greater than specified rate

➔ To Set Statistic Parameters:

1. Select **Statistics**. Type a number or the short form.

```
1. ra Radio
2. re Radio error
3. et Ethernet
4. ee Ethernet Error
Enter one of [a number from 1 to 2, a short form]:
```

2. You will be prompted for the statistics category. Enter the number or the short form. The short form is used to store the command in the configuration.

```
                   Radio

Receive                    Transmit

1 rpa Packets              5 tpa Packets

2 rby Bytes                6 tby Bytes

3 rfi Filtered             7 ter Errors

4 rer Errors

Enter one of [a number from 1 to 7, a short form]
```

3. Type a category number or the short form and press **ENTER**.

4. Choose the particular statistics that you wish to change. If any of the statistics already have an alarm associated, the current setting is displayed after the name.

```
Enter an action, one of [off, any, rate]:
```

5. Enter an action.

- **Off**: Turns off any alarms based on the statistics value.
- **Any**: An alarm will be generated if the statistics change value.
- **Rate**: Prompts for a rate per second change. If the statistic value changes faster than this rate, an alarm is produced.

Using the Print Log (Bnodelog)(Token Ring Only)

Use this option to print a log message whenever a backbone LAN node is added or removed from the association table.

Forwarding Logs to a Unix System (Syslog)

Use the *syslog* option to forward all logs printed on the Console (as controlled by the *printlevel* option) to a Unix host running the **Syslogd deamon** process. Enter the IP address of the Unix host. If the address remains at the default of 0.0.0.0., logs will not be sent.

Packets received by the **Syslogd daemon** process are recorded in the system log file on the Unix host. The logs are displayed on the Console in addition to being forwarded to the Unix host. If the Aironet Access Point should fail for any reason, the logs may still be viewed on the Unix host.

The logs are sent using the syslog facility code “LOG_LOCAL0”. The syslog priority depends on the priority of the log locally.

On the Unix host, the **Syslogd deamon** process will usually add the current time and IP address of the unit that sent the log. The Aironet Access Point will pre-pend its own name to the log before it is sent.

A message similar to the following will appear on the host:

```
Jan 11 10:46:30 192.009.200.206 A630_10172c:

Node 0000c0d1587e 630 added for 004096104546
```

Enabling Indicator Status Locking (Lockled)

Use the *lockled* option to specify whether the status indicator light remains amber or resets itself (after one second) when an event occurs. This option can only be used if the *ledlevel* option set to activate when an event log occurs.

12

CHAPTER 12

Performing Diagnostics

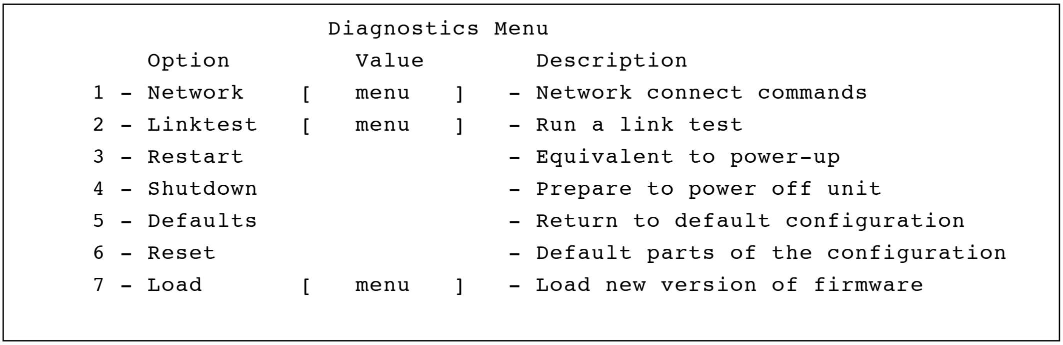
This chapter describes how to use the Diagnostics Menu to maintain the Aironet Access Point.

Here’s what you’ll find in this chapter:

- Using the Diagnostics Menu
- Running a Linktest
- Restarting the Unit
- Preparing the Unit for Power Down
- Returning the Unit to the Default Configuration
- Starting a Telnet Session
- Changing the Escape Sequence
- Physically Locating a Unit
- Sending a Ping Packet
- Loading New Code Versions

Using the Diagnostics Menu

Diagnostics are performed using the Diagnostics Menu. To access this menu, select **Diagnostics** from the Main Menu.



```
                      Diagnostics Menu
        Option         Value        Description
    1 - Network    [    menu   ]   - Network connect commands
    2 - Linktest   [    menu   ]   - Run a link test
    3 - Restart                    - Equivalent to power-up
    4 - Shutdown                   - Prepare to power off unit
    5 - Defaults                   - Return to default configuration
    6 - Reset                      - Default parts of the configuration
    7 - Load       [    menu   ]   - Load new version of firmware
```

Running a Linktest (Linktest)

Use the *linktest* option to test the quality of the radio transmission between the Aironet Access Point and other nodes on the radio network. See “Running a Linktest” in **Chapter 4**.

Restarting the Unit (Restart)

Use the *restart* option to reboot the Aironet Access Point. All associations will be lost and the unit will react as though it had just been powered on.

Preparing the Unit for Shutdown (Shutdown)

Use the *shutdown* option prior to powering off the unit to verify that writes to the flash memory are not in process.

Returning the Unit to the Default Configuration (Defaults)

Use the *defaults* option to return the Aironet Access Point configuration to its default factory settings. The unit will erase the currently saved configuration and execute a restart command.

Resetting the Configuration (Reset)

The *reset* option may be used to reset only parts of the configuration back to the default values. You will prompted for part of the configuration you wish to reset. If you enter **ident_save**, everything but the configuration identifying the unit will be reset to defaults. If you enter **filter_default**, only the filter configuration will be defaulted. You can determine what configuration items are in each set by using the configuration dump command and select a type of **ident**, **radio**, or **filter**.

Using the Network Menu

Network parameters are set up using the Network Menu. To access this menu, select **Diagnostics** from the Main Menu then **Network** from the Diagnostics Menu.

```
                         Network Menu
       Option          Value        Description
   1 - Connect                   - Network connect commands
   2 - Escape   [“ˆXˆYˆZ”]       - Run a link test
   3 - Find                      - Equivalent to power-up
   4 - Ping                      - Prepare to power off unit
```

Starting a Telnet Session (Connect)

The *connect* option is used to start a telnet session with a remote unit on the network to gain access to its Console Menu. The *connect* option can also be used to access any remote node (PC or Server) that supports telnet access.

The connection may be initiated using the remote node’s IP address. The connection is completely routable and the destination may be anywhere in the internet.

If the connection is to be made to another Aironet unit which has not been assigned an IP address, start the connection using the MAC level network address of the unit. This connection uses a proprietary protocol which is not routable. The destination must lie on the local LAN. It is useful for a large number of Access Points to which you do not want to assign individual IP addresses.

When starting a telnet session with the c*onnect* option:

- Make sure the telnet option on the remote is enabled before connecting to a remote Access Point or client. See “Telnet Access” in **Chapter 2**.
- A message is printed on the remote’s Console stating where the connections originated from. The Console is then disabled for the duration of the telnet session to prevent conflicting commands.
- The remote’s Console privilege is set to the highest level that does not have a password.

While the unit is attempting to connect to the remote node, the connection can be terminated by typing “CTRL-C”. This may be required if the incorrect address was entered.

After connecting, you can close a telnet session and return to the local console by:

- Typing the escape sequence of characters as defined by the *escape* option in the Diagnostics Menu. See “Changing the Escape Sequence”.
- If the remote node is an Aironet node, choose the *close* option which is accessible on the Console Port Main Menu during a telnet session only.
- Using the remote node’s logout command.

Changing the Escape Sequence (Escape)

Use the *escape* option to change the sequence of characters that are assigned to close a telnet session to a remote destination. Typically, you would change the sequence if the current sequence has meaning to the remote system.

The sequence may be up to 10 characters in length. To enter non-printable characters in the sequence you may:

- Use the two-character combination of caret (^) and the alphabetic character corresponding to the control character. For example, to enter “control Z”, use the string “^Z”.
- Use a backslash “\” followed by three octal numbers
- Use a dollar sign “$” followed by two hexadecimal numbers

Physically Locating a Unit (Find)

Use the *find* option to flash the indicators (amber) of the Access Point on and off. Find a unit you can telnet to if you are not sure of it’s exact location. Type “CTRL-C” to stop the command.

Sending a Ping Packet (Ping)

Use the *ping* option to test network connectivity from the Access Point to other IP nodes. The *ping* option sends an ICMP echo_request packet to a user-specified remote node. If the remote node receives the packet it will also respond with an ICMP echo_response packet.

The Aironet Access Point will send the echo_response packet and wait 3 seconds for a response. If none is received, another echo packet is sent. This is repeated up to five times. If a response is received and a message is displayed, the command disappears from the screen. Type “CTRL-C” to stop the command.

Loading New Code Versions (Load)

The Aironet Access Point code is stored in a flash memory chip inside the unit. Use the *load* option to load new code versions of the Aironet Access Point's firmware and save it to flash memory.

To load new versions of the firmware, the code must be loaded into main memory first, then programmed into the flash memory. The unit will reboot using the new firmware. The flash memory will retain the new version even if the power is disconnected.

The new firmware can be downloaded into the unit using:

- **FTP**: Load the new firmware into a single unit using either the XModem or FTP protocols. Then use the FTP protocol to upload (send) the code running in the local unit to other remote units on the infrastructure.
- **Distribute**: Load the new firmware into a single unit using either the XModem or FTP protocols. Then use the *distribute* option to simultaneously load all of the other units on the infrastructure, whether they are connected wirelessly or via the wired infrastructure.
- **Bootp**: Load the new firmware and configuration revisions into the units each time they power up.

When you select the *load* option, the Diagnostics Load Menu appears:

```
                        Diagnostics Load Menu
    Option             Value              Description
1 - Xmodem                           - Xmodem load from serial port
2 - Crc-xmodem                       - Xmodem-CRC load from serial port
3 - Ftp              [  menu  ]      - Load using FTP
4 - Distribute       [  menu  ]      - Distribute the firmware
5 - Bootp/DHCP       [   on   ]      - Use BOOTP/DHCP on startup
6 - Class            [ AP4800 ]      - DHCP class id
Enter an option number or name, "=" main menu, <ESC> previous menu
>
```

Downloading Using Xmodem Protocol (Xmodem/Crc-xmodem)

Use the *Xmodem* or *CRC-xmodem* options to load the new firmware version through the Console Port.

Depending on the communications software programs available, choose:

- **Xmodem**: Terminates packets with a “checksum”
- **CRC-xmodem**: Terminates packets with a Cyclic Redundancy Check (CRC).

➔ **To load firmware using Xmodem or CRC-xmodem:**

1. Connect a terminal to the Console Port using a communications software program (Procomm™ or Windows™ Terminal).
2. Select either the *Xmodem* option or *CRC-xmodem* option, depending on your communications software.

The following message appears:

```
Ready for XMODEM download. Use several ^X's to cancel
```

3. Set the communication program to initiate the file transfer to the unit.
4. The unit begins the file download. A message similar to the following appears:

```
XMODEM: received 160450 bytes in 00:03:36; 800 bytes/s
transfer rate
```

After the loaded code for the new firmware is validated, the flash memory is programmed and the unit will restart with the new code.

The firmware consists of the boot block and the application code. During the firmware download, the application code is replaced, but the boot block is not.

When the unit powers up, the boot block checks the integrity of the application code. If it is valid, the boot block will execute the new firmware. If it is invalid, the boot block will display an error message on the Console and the firmware will need to be reloaded.

The only time you should receive an invalid application code is when the flash memory device fails or the power is interrupted while the flash memory is in the process of being programmed.

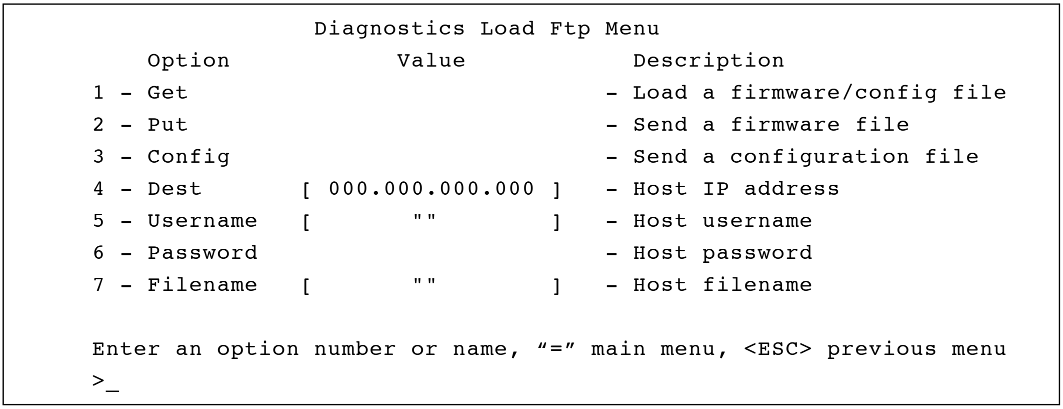
Downloading or Uploading using the File Transfer Protocol (Ftp)

Use the *FTP* option to download or upload firmware. The Aironet Access Point can be an FTP client or FTP server. To upload or download firmware you can initiate a connection from:

- The Aironet Access Point console to a remote PC or host and retrieve a new version of the firmware.
- The Aironet Access Point console to a remote PC or host and send a copy of the running firmware.
- One Access Point console to another allowing units to send or receive firmware running locally.
- A PC or host system to an Aironet Access Point and send a new firmware version.

NOTE: Before you download or upload new code versions, make sure you have set the IP address on all units involved.

When you select the *FTP* option, the Diagnostics Load FTP Menu appears:



```
                  Diagnostics Load Ftp Menu
    Option              Value              Description
1 - Get                                  - Load a firmware/config file
2 - Put                                  - Send a firmware file
3 - Config                               - Send a configuration file
4 - Dest        [ 000.000.000.000 ]      - Host IP address
5 - Username    [        ""       ]      - Host username
6 - Password                             - Host password
7 - Filename    [        ""       ]      - Host filename

Enter an option number or name, “=” main menu, <ESC> previous menu
>_
```

Downloading a New Firmware/Configuration File (Get)

Use the *get* option to download (retrieve) firmware or a configuration file. Once the file has been loaded, the unit will check the first characters of the file. If “! CONFIGURATION” is present, the file contains menu configuration commands. Otherwise the file is considered to be firmware and will be loaded in the flash memory and then executed.

➔ **To Download Firmware using FTP:**

1. Load the file onto a PC, host, or Aironet Access Point you will retrieve from.

2. Select the *dest* option and type in the IP address of the host PC or Aironet Access Point.

3. Select the *username* option and type in the username required to access the firmware file.

   If downloading from another Aironet Access Point, the *username* option must have a value even though the value is not used by the remote Aironet Access Point.

4. Select the *password* option and type the password associated with the username.

   If downloading from another Aironet Access Point, the login password value must match the console write privilege password on the remote Aironet Access Point.

5. Select the *filename* option and type the name of the firmware file you are retrieving (including drive and directory), then press **ENTER**.

   If downloading from another Aironet Access Point, the *filename* option must have a value even though the value is not used by the remote Aironet Access Point.

6. Select the *get* option.

The unit will begin an FTP session to the host PC, retrieve the file, program the flash memory, and reboot. A message will appear:

```
220 sun_host FTP server (SunOS 4.1) ready.
230 User sysop logged in.
200 Type set to I.
200 PORT command successful.
150 Binary data connection for apv33.img (163056 bytes).
226 Binary Transfer complete.
221 Goodbye.
FTP: received 161056 bytes in 00:00:10; 15 Kbytes/s transfer rate

rebooting unit.
```

Uploading a New Firmware Version (Put)

Use the *put* option to upload (send) a copy of the currently running firmware to another system. If the system is a:

- **PC or host**: A copy of the firmware will be stored on the system’s disk, possibly for downloading to other units later.
- **Aironet Access Point**: The remote Aironet Access Point will flash the new code and begin running it immediately. You can use one Aironet Access Point to upgrade another Aironet Access Point.

➔ **To Upload Firmware using FTP:**

1. Select the *dest* option and type the IP address of the remote PC, host or Aironet Access Point you are sending to. Press **ENTER**.

2. Select the *username* option and type the username for the remote PC, host, or Aironet Access Point you are sending to. Press **ENTER**.

   If uploading to another Aironet Access Point, the *username* option must have a value even though the value is not used by the remote Aironet Access Point.

3. Select the *password* option and type the access password for the remote PC, host, or the console. Press **ENTER**.

4. Select the *filename* option type the name of the firmware file you are sending to the PC, host, or Aironet Access Point (including drive and directory). Press **ENTER**.

   If uploading to another Aironet Access Point, the *filename* option must have a value even though the value is not used by the remote Aironet Access Point.

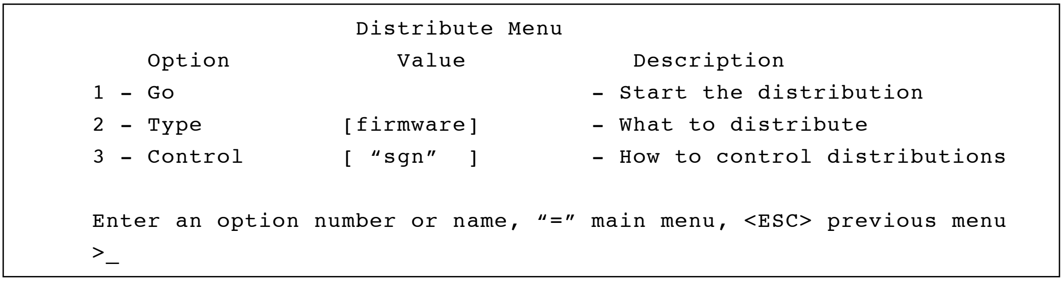
5. Select the *put* option. The unit will begin an FTP session to the remote host PC or Aironet Access Point.

Uploading the Unit's Configuration (Config)

You may use this option to save the configuration on a remote host or PC in a format suitable for later downloading using FTP or BOOTP.

You are first prompted for the name of the file to be created on the remote system. Once the filename is entered the transfer will begin.

Distributing Firmware or Configuration (Distribute)



```
                    Distribute Menu
    Option             Value            Description
1 - Go                              - Start the distribution
2 - Type           [firmware]       - What to distribute
3 - Control        [ “sgn”  ]       - How to control distributions

Enter an option number or name, “=” main menu, <ESC> previous menu
>_
```

Use the *distribute* option to send the firmware or configuration from one Aironet Access Point to all other Aironet Access Points on the infrastructure (whether they are repeaters or are connected to the wired infrastructure). By using the *distribute* option the time needed to perform firmware upgrades or make global changes to the configuration is greatly decreased.

Once a new version of the firmware has been loaded into a single Aironet Access Point, (using Xmodem, CRC-Modem, Ftp, or Bootp) or the configuration has changed, use the *distribute* option to upgrade all other units.

If you are distributing a configuration, examine the parts of the unit’s configuration that will be distributed by executing the command “configuration dump distributable standard”.

The *control* option controls how the remote units respond to a request to send a configuration or firmware.

- **None**: The unit will never respond and cannot be loaded by another unit using the distribute command.
- **Any**: The unit will always respond. It is up to the distributing unit to determine whether to load the local unit.
- **Newer**: The unit will only respond if the version of firmware being distributed has a larger version number than the code currently running. This selection only applies to firmware downloads.
- **None of the Above**: A password that must be entered by the operator of the unit doing the distribution. The local unit will not respond to any distributions that do not supply this password.

If the *distribute* is password protected, only those units that have the same password configured in the control parameter will accept the distribution. The units can be protected from unwanted loads. The password may also be used to divide the units into code load groups such that the loads to one group will not affect the other groups.

If the *distribute* is done without a password, the load will be ignored by remote units with a configured password. If a remote unit does not have a password and firmware is being distributed, it only accepts the load based on the version number and code checksum.

The *type* option controls whether the unit is to distribute its firmware or configuration.

The *go* option starts the distribution. The following message will appear:

```
Finding the other units ....
```

When the command is executed, the local unit will send a special broadcast message to all other units on the infrastructure. The message reports that the unit has a new firmware file with its assigned version number or a configuration file.

The remote units then decide whether to respond based on the value of their control parameter. Any responses are displayed on the local unit.

```
AP4800  004096001d45  has code version 3.2a (checksum
1598)
```

When the local unit receives a response to its request, the remote unit is added to a list of units to be loaded. When the response timeout period has expired, the local unit will begin loading all remote units in parallel using a proprietary protocol. A message similar to the one below will be displayed.

```
Loading 004096001d45
Loading 00409610345f
```

If any remote units timeout during the load, they are removed from the list. Once all units have completed loading, the local unit displays a count of the successful loads. A message similar to the following will be displayed.

```
Completed loading 004096001d45
Completed loading 00409610345f
Loading of 2 Ethernet Access Points completed
```

Downloading Using the Internet Boot Protocol (Bootp/DHCP)

The *Bootp/DHCP* option is enabled by default when the Aironet Access Point is powered on. The process for downloading firmware files using the Bootp/DHCP parameter is:

1. On power up, the Aironet Access Point will issue boot protocol requests to see if there are any Bootp or DHCP servers on the network that have been configured with the unit network address.

2. If no response is found the request is repeated up to 30 times with a 4 second wait after the first request. It then doubles the time between requests for each additional retry. If there is still no response, the unit gives up.

3. If multiple responses are received, the unit will pick a DHCP server over a BOOTP server.

4. If a response is received, the IP address assigned to this unit by the server is compared to the configured value. If they are different, the configured value is changed.

5. The download file is examined. If the file is not empty, it is assumed to be a configuration file in the format produced by the “configuration dump” menu command. A Trivial File Transfer Protocol (TFTP) dialogue is used to retrieve the file from the server.

6. The contents of the configuration file is processed as though the commands have been entered by the operator at the console. The commands in the file will modify the currently running configuration.

NOTE: The current configuration is not set back to the defaults before the file is processed. Therefore, the file contents do not have to be a complete configuration but may contain just the items you wish to change.

7. Once the configuration has been processed, the name stored in the “diagnostics load ftp filename” parameter is assumed to be the name of the firmware file to download. If the parameter is not empty, the unit will use the TFTP protocol to load the file into RAM.

   - If the firmware is different from the currently running version, the unit will program the flash memory with the new code and restart to execute it.

   - If the new firmware is the same, the unit discards the loaded file and continues normal operation.

Configuring DHCP Servers (Class)

Use the *class* option to enter a class ID for a client node. The entered string is placed in the DHCP discover messages sent to the DHCP servers. The server will determine how to respond based on the class ID.

LAN Interfaces Supported

Ethernet

Cable	Specifications	Connector
Thin Ethernet	IEEE 802.3 10Base2	BNC connector
Thick Ethernet	IEEE 802.3 10Base5	DB-15 AUI connector (external Transceiver required)
Twisted Pair Ethernet	IEEE 802.3 10BaseT	RJ-45 connector

Token Ring

Cable	Specifications	Connector
Unshielded Twisted Pair	IEEE 802.5	RJ-45 Connector
Shielded Twisted Pair	IEEE 802.5	DB-9 Connector

Radio Characteristics

Item	Aironet 4500 and 4800 Series Access Point
Frequency	2.400 to 2.497 GHz*
Modulation	Direct Sequence Spread Spectrum
Antenna	Diversity system using (2) dipole antennas (2.2 dBi gain). Optional antennas available.
Power Output	100 mW*
Compliance	Operates license-free under FCC Part 15 and complies as a Class B computing device. Complies with DOC regulations. Complies with ETS 300.328 and MKK standards.

* Depends on regulatory domain

Physical Specifications

Item	Description
Size	20 x 15 x 5 cm (7.8 x 5.9 x 1.9 inches)
Status Indicators	Top Panel - Radio Traffic activity, Ethernet Traffic activity, Status Back Panel (Ethernet Only) -Ethernet Rx and Tx activity, Polarity, Port connections, Collisions
Console Port	DCE with DB-9 female connector
Power Supply	Power Pack. The power pack will be either 120VAC/60Hz or 90-264VAC/47-63Hz to 12-18VDC, whichever is appropriate for country of use.
Weight	0.7 Kg (1 lb. 8 oz.)
Operating environment	-20^{o}C to 50^{o}C (-4^{o}F to 122^{o}F)

Console Port Pin-Out

The Console Port is a DCE using a DB-9 female connector. The following table describes the pinouts on the connector and how you should connect the DB-9 pins to the DB-25 on a terminal. Signal names are in terms of the DTE.

Ethernet Signal	DB-9 Pin Aironet Console Port	DB-25 Pin Computer Serial Port
RxD	2	3
TxD	3	2
GND	5	7
DCD	1	8
DTR	4	20
CTS	8	5
RTS	7	4

Most terminals and communication programs will only require Txd, Rxd and Gnd to communicate with the Aironet Aironet Access Point. Some may also require DCD before the connection on-line can be made. If you use hardware flow control, connect all lines.

Appendix B - Console Menu Tree

The Console system consists of multiple sub-menus that branch off the Main Menu, much like a tree. This Appendix provides you with a detailed listing of all menu, sub-menus and options contained in the Console Port.

Main Menu	
Configuration	General configuration
Radio	Radio network parameters
Ssid	Service set identification
I80211	802.11 parameters
Beacon	Beacon period in Kμsec
Dtim	DTIM interval
Extend	Allow proprietary extensions
Rts	RTS/CTS packet size threshold
Encapsulation	Default encapsulation method
Frequency	Center frequency in MHz
Rates	Allowed bit rates in megabits/second
Basic_rates	Basic rates in megabits/second
Root	Enable root mode
Install	Installation utilities
Linktest	Run a link test
Multicast	Run a multicast test
Unicast	Run a unicast test
Remote	Run a remote test
Destination	Target address
Size	Packet size
Count	Number of packets to send
Errors	Radio error statistics
Autotest	Auto linktest mode
Continuous	Repeat test once started
Strength	Run a signal strength test
Extended	Extended parameters
Parentid	Parent node ID
Parentid_timeout	Time to look for specified parent
Parent_wait	How long to look for previous parent
Time_retry	Number of seconds to retry transmit
Count_retry	Maximum number transmit retries
Refresh	Refresh rate in 1/10 of seconds
Diversity	Enable the diversity antennas
Power	Transmit power level
Fragment	Maximum fragment size

```
Ethernet                      Ethernet configuration
    Active                    Connection active
    Size                      Maximum frame size                     Ethernet Only
    Port                      Port selection
    Fallback                  Become repeater on LAN cable fault
Token Ring                    Token Ring configuration
    Active                    Connection active
    Speed                     Ring speed                             Token Ring Only
    Method                    Routing method
    Fallback                  Become repeater on LAN cable fault
    Extended                  Extended configuration
        Partition             Number bits in bridge numbers
        Earlyrls              Maximum route field length
        Sap                   Set control frame SAPs
    Address                   Config address conversions
        Display               Display the conversion entries
        Add                   Add a conversion entry
        Remove                Remove a conversion entry
Ident                         Identification information
    Name                      Node name
    Nid                       Network address
    Inaddr                    Internet address
    Inmask                    Internet subnet mask
    Routing                   IP routing table configuration
        Display               Display route table entries
        Host                  Add a static host route
        Net                   Add a static network route
        Default               Internet default gateway
        Delete                Delete a static route
    Location                  SNMP system location
    Contact                   SNMP system contact name
Console                       Console set-up
    Type                      Terminal type
    Port                      Port set-up
        Rate                  Console baud rate
        Bits                  Bits per character
        Parity                Console parity
        Flow                  Flow control type
    Rpassword                 Set readonly privilege password
    Wpassword                 Set write privilege password
    Linemode                  Console expects complete lines
    Remote                    Control remote access
        Telnet                Allow telnet connections
        Http                  Allow HTTP connections
        Frame                 Use HTML frames
        Remote Access         Remote access control
```

Display	Display the remote host list
Add	Add a remote host
Remove	Remove a remote host
Snmp	Set snmp values
Enabled	Enable the SNMP agent
Communities	Set community properties
Display	Display communities
Add	Add a community
Remove	Remove a community
Access	Set community access mode
Ipadr	Set allowed NMS IP addresses
Nid	Set allowed NMS node ids
Remote	Allow remote NMS to change community
Trapdest	IP destination for SNMP traps
Trapcomm	Community for SNMP traps
Loglevel	Type of logs to cause a trap
Authtrap	Enable authentication failure trap
More	More items
Dump	Dump configuration to console
Statistics	Display statistics
Throughput	Throughput statistics
Radio	Radio error statistics
Status	Display general status
Watch	Record history of a statistic
History	Display statistic history
Nodes	Node statistics
ARP	ARP table
Display_time	Time to re-display screens
Association	Association table maintenance
Display	Display the table
Summary	Display the table summary
Monitor	Monitor network associations
Map	Show network map
Trace	Trace network associations
Maximum	Maximum allowed child nodes
Autoassoc	Allow automatic table additions
Add	Control node association
Remove	Remove association control
Niddisp	Node Ids display mode
Filter	Control packet filtering
Multicast	Multicast address filtering
Default	Default multicast action
Show	Display the multicast filters
Add	Add a multicast address filter
Remove	Remove a multicast address filter
Radio_mcst	Where to forward multicasts from radio

Node	Node address filtering
Source	Source addresses
Display	Display the node address filters
Ipdisplay	Display the IP address filters
Add	Add a node address filter
Remove	Remove a node address filter
Protocols	Protocol filters
Default	Default action
Unicast	Filter unicast packets
Display	Display the protocol filters
Add	Add a protocol filter
Remove	Remove a protocol filter
Length	Length of packet data to log
Monitor	Protocol monitoring enabled
Show	Show forwarded protocol list
Clear	Clear forwarded protocol list
Direction	Packet direction affected by filters
Logs	Alarm and log control
History	Log and alarm history
Clear	Clear the history buffer
Printlevel	Type of logs to print
Loglevel	Type of logs to save
Ledlevel	Type of logs to light status led
Statistics	Set alarms on statistics
Bnodelog (Token Ring Only)	Log backbone node changes
Syslog	Unix syslogd address
Lockled	Enable LED status locking
Diagnostics	Maintenance and testing commands
Network	Network connect commands
Connect	Start telnet session
Escape	Connection escape sequence
Find	Flash LEDs to find unit
Ping	Send an IP PING packet
Linktest	Run a link test
Restart	Equivalent to power-up
Shutdown	Prepare to power-off unit
Defaults	Return to default configuration
Reset	Default parts of the configuration
Load	Load new version of firmware
Xmodem	Xmodem load from serial port
CRC-Xmodem	Xmodem-CRC load from serial port
Get	Load a firmware/config file
Put	Send a firmware file
Config	Send a configuration file
Dest	Host IP address
Username	Host username
Password	Host password
Filename	Host filename

Ftp	Load using FTP
Distribute	Distribute the firmware
Go	Start the distribution
Type	What to diestribute
Control	How to control distributions
Bootp/DHCP	Use BOOTP/DHCP on startup
Class	DHCP class ID
Privilege	Set privilege level
Help	Introduction

Appendix C - SNMP Variables

The Aironet Access Point supports the Simple Network Management Protocol (SNMP). SNMP provides an industry standard mechanism for the exchange of information in a TCP/IP based internet environment.

The resident SNMP agent is compliant with subsets of the (Management Information Base) MIB-I and MIB-II for TCP/IP based internets as defined in Internet's Request For Changes (RFC) 1156 and 1213. Since the Aironet Access Point does not perform any IP routing or forwarding, certain (groups of) managed objects are not meaningful. For SNMP requests pertaining to such managed objects, the node simply returns a "no such name" error status in the response.

The Object ID (OID) prefix for the Aironet Access Point resides under the Structure of Managed Information (SMI) tree for private enterprises in the Telxon.arlan.devices (551.2.1) branch. The system object identifier for the Aironet Access Point is (1.3.6.1.4.1.551.2.1.76). The resident agent also supports a custom MIB that allows a management station to read/modify most of the parameters that may be set through the Console Menus. For a machine readable version of the custom MIB, contact Aironet Wireless Communications.

C.1 MIB II Variables

The System Group

MIBII.system (1.3.6.1.2.1.1.x)

Object ID	Object Name	Object Type	Access
1	sysDescr	string	read
2	sysObjectID	oid	read
3	sysUpTime	time	read
4	sysContact	string	write
5	sysName	string	write
6	sysLocation	string	write
7	sysServices	integer	read

The Interfaces Group

MIBII.interfaces (1.3.6.1.2.1.2.x)

Object ID	Oject Name	Object Type	Access
1	ifNumber	integer	read
2	ifTable	Sequence of if	entry
2.1	ifEntry	Sequence	entry
2.1.1	ifIndex	integer	read
2.1.2	ifDescr	string	read
2.1.3	ifType	integer	read
2.1.4	ifMtu	integer	read
2.1.5	ifSpeed	gauge	read
2.1.6	ifPhysAddress	string	read
2.1.7	ifAdminStatus	integer	read
2.1.8	ifOperStatus	integer	read
2.1.9	ifLastChange	time	read
2.1.10	ifInOctets	counter	read
2.1.11	ifInUcastPkts	counter	read
2.1.12	ifInNUcastPkts	counter	read
2.1.13	ifInDiscards	counter	read
2.1.14	ifInErrors	counter	read
2.1.15	ifInUnknownProtos	counter	read
2.1.16	ifOutOctets	counter	read
2.1.17	ifOutUcastPkts	counter	read
2.1.18	ifOutNUcastPkts	counter	read
2.1.19	ifOutDiscards	counter	read
2.1.20	ifOutErrors	counter	read
2.1.21	ifOutQLen	gauge	read
2.1.22	ifSpecific	integer	read

The Address Translation Group (deprecated by MIB-II)

MIBII.at (1.3.6.1.2.1.3.x)

Object Id	Object Name	Object Type	Access
1	atTable	Sequence of at	entry
1.1	atEntry	Sequence	entry
1.1.1	atIfIndex	integer	read
1.1.2	atPhysAddress	string	read
1.1.3	atNetAddress	ipaddress	read

The IP Group

MIBII.ip (1.3.6.1.2.1.4.x)

Object Id	Object Name	Object Type	Access
1	ipForwarding	integer	read
2	ipDefaultTTL	integer	write
3	ipInReceives	counter	read
4	ipInHdrErrors	counter	read
5	ipInAddrErrors	counter	read
6	ipForwDatagrams	counter	read
7	ipInUnknownProtos	counter	read
8	ipInDiscards	counter	read
9	ipInDelivers	counter	read
10	ipOutRequests	counter	read
11	ipOutDiscards	counter	read
12	ipOutNoRoutes	counter	read
13	ipReasmTimeout	integer	read
14	ipReasmReqds	counter	read
15	ipReasmOKs	counter	read
16	ipReasmFails	counter	read
17	ipFragOKs	counter	read
18	ipFragFails	counter	read
19	ipFragCreates	counter	read
20	ipAddrTable	Sequence of	ipAddrEntry
20.1	ipAddrEntry	Sequence	ipAddrEntry
20.1.1	ipAdEntAddr	ipaddress	read
20.1.2	ipAdEntIfIndex	integer	read
20.1.3	ipAdEntNetMask	ipaddress	read
20.1.4	ipAdEntBcastAddr	integer	read

The ICMP Group

MIBII.icmp (1.3.6.1.2.1.5.x)

Object Id	Object Name	Object Type	Access
1	icmpInMsgs	counter	read
2	icmpInErrors	counter	read
3	icmpInDestUnreachs	counter	read
4	icmpInTimeExcds	counter	read
5	icmpInParmProbs	counter	read
6	icmpInSrcQuenchs	counter	read
7	icmpInRedirects	counter	read
8	icmpInEchos	counter	read
9	icmpInEchoReps	counter	read
10	icmpInTimestamps	counter	read
11	icmpInTimestampReps	counter	read
12	icmpInAddrMasks	counter	read
13	icmpInAddrMaskReps	counter	read
14	icmpOutMsgs	counter	read
15	icmpOutErrors	counter	read
16	icmpOutDestUnreachs	counter	read
17	icmpOutTimeExcds	counter	read
18	icmpOutParmProbs	counter	read
19	icmpOutSrcQuenchs	counter	read
20	icmpOutRedirects	counter	read
21	icmpOutEchos	counter	read
22	icmpOutEchoReps	counter	read
23	icmpOutTimestamps	counter	read
24	icmpOutTimestampReps	counter	read
25	icmpOutAddrMasks	counter	read
26	icmpOutAddrMaskReps	counter	read

The UDP Group

MIBII.udp (1.3.6.1.2.1.7.x)

Object Id	Object Name	Object Type	Access
1	udpInDatagrams	counter	read
2	udpNoPorts	counter	read
3	udpInErrors	counter	read
4	udpOutDatagrams	counter	read

The Transmission group

MIBII.transmission.dot3 (1.3.6.1.2.1.10.7.x)

Object Id	Object Name	Object Type	Access
1	dot3Table	Sequence of dot3	entry
1.1	dot3Entry	Sequence	entry
1.1.1.1	dot3Index	integer	read
1.1.3.1	dot3MacSubLayerStatus	integer	write
2	dot3StatsTable	Sequence of dot3Stats	entry
2.1	dot3StatsEntry	Sequence	entry
2.1.1.1	dot3StatsIndex	integer	read
2.1.2.1	dot3StatsAlignmentErrors	counter	read
2.1.3.1	dot3StatsFCSErrors	counter	read
2.1.4.1	dot3StatsSingleCollisionFrames	counter	read
2.1.5.1	dot3StatsMultipleCollisionFrames	counter	read
2.1.6.1	dot3StatsSQETestErrors	counter	read
2.1.7.1	dot3StatsDeferredTransmissions	counter	read
2.1.8.1	dot3StatsLateCollisions	counter	read
2.1.9.1	dot3StatsExcessiveCollisions	counter	read
2.1.10.1	dot3StatsInternalMacTransmitErrors	counter	read
2.1.11.1	dot3StatsCarrierSenseErrors	counter	read
2.1.12.1	dot3StatsExcessiveDeferrals	counter	read
2.1.13.1	dot3StatsFrameTooLongs	counter	read
2.1.14.1	dot3StatsInrangeLengthErrors	counter	read
2.1.15.1	dot3StatsOutOfRangeLengthFields	counter	read
2.1.16.1	dot3StatsInternalMacReceiveErrors	counter	read

The SNMP Group

MIBII.snmp (1.3.6.1.2.1.11.x)

Object Id	Object Name	Object Type	Access
1	snmpInPkts	counter	read
2	snmpOutPkts	counter	read
3	snmpInBadVersions	counter	read
4	snmpInBadCommunityNames	counter	read
5	snmpInBadCommunityUses	counter	read
6	snmpInASNParseErrs	counter	read
7	snmpInBadTypes	counter	read
8	snmpInTooBigs	counter	read
9	snmpInNoSuchNames	counter	read
10	snmpInBadValues	counter	read
11	snmpInReadOnlys	counter	read
12	snmpInGenErrs	counter	read
13	snmpInTotalReqVars	counter	read
14	snmpInTotalSetVars	counter	read
15	snmpInGetRequests	counter	read
16	snmpInGetNexts	counter	read
17	snmpInSetRequests	counter	read
18	snmpInGetResponses	counter	read
19	snmpInTraps	counter	read
20	snmpOutTooBigs	counter	read
21	snmpOutNoSuchNames	counter	read
22	snmpOutBadValues	counter	read
23	snmpOutReadOnlys	counter	read
24	snmpOutBadGenErrs	counter	read
25	snmpOutGetRequests	counter	read
26	snmpOutGetNexts	counter	read
27	snmpOutSetRequests	counter	read
28	snmpOutGetResponses	counter	read
29	snmpOutTraps	counter	read
30	snmpEnableAuthenTraps	integer	write

The Token Ring Group

iso.org.dod.internet.experimental.dot5 (1.3.6.1.3.4)

Object Id	Object Name	Object Type	Access
1	dot5Table	Sequence of	dot5Entry
1.1	dot5entry	Sequence	
1.1.1.1	dot5IfIndex	integer	read
1.1.2.1	dot5Commands	integer	write
1.1.3.1	dot5RingStatus	integer	read
1.1.4.1	dot5RingState	integer	read
1.1.5.1	dot5RingOpenStatus	integer	read
1.1.6.1	dot5RingSpeed	integer	read
1.1.7.1	dot5UpStream	integer	read
1.1.8.1	dot5MonParticipate	integer	read
1.1.9.1	dot5Functional	integer	read
2	dot5StatsTable	Sequence of	dot5StatsEntry
2.1	dot5StatsEntry	Sequence	
2.1.1.1	dot5StatsIndex	integer	read
2.1.2.1	dot5StatsLineError	counter	read
2.1.3.1	dot5StatsBurst Errors	counter	read
2.1.4.1	dot5StatsACErrors	counter	read
2.1.5.1	dot5StatsAbortTransErrors	counter	read
2.1.6.1	dot5StatsInternalErrors	counter	read
2.1.7.1	dot5StatsLostFrameErrors	counter	read
2.1.8.1	dot5StatsReceiveCongestions	counter	read
2.1.9.1	dot5StatsFrameCopiedErrors	counter	read
2.1.10.1	dot5StatsTokenErrors	counter	read
2.1.11.1	dot5StatsSoftErrors	counter	read
2.1.12.1	dot5StatsHardErrors	counter	read
2.1.13.1	dot5StatsSignalLoss	counter	read
2.1.14.1	dot5StatsTransmitBeacons	counter	read
2.1.15.1	dot5StatsRecoverys	counter	read
2.1.16.1	dot5StatsLobeWires	counter	read
2.1.17.1	dot5StatsRemove	counter	read
2.1.18.1	dot5StatsSingles	counter	read
2.1.19.1	dot5StatsFreqErrors	counter	read

3.2 The Custom MIB

The Configure Ethernet Group

ACCESSPOINT.configuration.cfgEthernet (1.3.6.1.4.1.551.2.2.1.1.x)

Object ID	Object Name	Object Type	Access
1	cfgEthEnable	integer	write
2	cfgEthSize	integer	write

The Configure ARLAN Group

ACCESSPOINT.configuration.cfgArlan (1.3.6.1.4.1.551.2.2.1.2.x)

Object Id	Object Name	Object Type	Access	Product Series
1	cfgArlRoot	integer	write	
7	cfgArlParent	string	write	
8	cfgArlParentTime	integer	write	
16	cfgArlSsid	String	write	
17	cfgArlHopSet	Integer	write	4500
18	cfgArlHopPattern	Integer	write	4500
19	cfgArlHopDwell	Integer	write	4500
20	cfgArlBeaconInt	Integer	write	4500
21	cfgArlDTIMCnt	Integer	write	4500
22	cfgArl802Extend	Integer	write	4500
23	cfgArlRtsThresh	Integer	write	4500
24	cfgArlFragThresh	Integer	write	4500

The Configure Filtering Group

ACCESSPOINT.configuration.cfgFilter (1.3.6.1.4.1.551.2.2.1.3.x)

Object Id	Object Name	Object Type	Access
1	cfgFiltMcst	integer	write
7	cfgFiltSrc	integer	write

The Configure Console Group

ACCESSPOINT.configuration.cfgConsole (1.3.6.1.4.1.551.2.2.1.4.x)

Object Id	Object Name	Object Type	Access
1	cfgConsPrivilege	integer	write
2	cfgConsReadPwd	string	write
3	cfgConsWritePwd	string	write
4	cfgConsType	integer	write
5	cfgConsBaud	integer	write
6	cfgConsBits	integer	write
7	cfgConsParity	integer	write
9	cfgConsTelnet	integer	write
11	cfgConsFlow	integer	write

The Configure SNMP Group

ACCESSPOINT.configuration.cfgSnmp (1.3.6.1.4.1.551.2.2.1.5.x)

Object Id	Object Name	Object Type	Access
1	cfgSnmpDest	ipaddress	write
2	cfgSnmpAuth	integer	write
3	cfgSnmpTComm	string	write
4	cfgSnmpLog	integer	write
5	cfgSnmpCommTable	Sequence of cfgSnmpCommTableEntry	
5.1	cfgSnmpCommTableEntry	Sequence	
5.1.1	cfgSnmpCommStatus	integer	write
5.1.2	cfgSnmpCommIndex	integer	write
5.1.3	cfgSnmpCommName	string	write
5.1.4	cfgSnmpCommAccess	integer	write
5.1.5	cfgSnmpCommIP1	ipaddress	write
5.1.6	cfgSnmpCommIP2	ipaddress	write
5.1.7	cfgSnmpCommIP3	ipaddress	write
5.1.8	cfgSnmpCommIP4	ipaddress	write
5.1.9	cfgSnmpCommIP5	ipaddress	write
5.1.10	cfgSnmpCommNID1	string	write
5.1.11	cfgSnmpCommNID2	string	write
5.1.12	cfgSnmpCommNID3	string	write
5.1.13	cfgSnmpCommNID4	string	write
5.1.14	cfgSnmpCommNID5	string	write

The Configure Logs Group

ACCESSPOINT.configuration.cfgLogs (1.3.6.1.4.1.551.2.2.1.6.x)

Object Id	Object Name	Object Type	Access
1	cfgLogPrint	integer	write
2	cfgLogSave	integer	write
3	cfgLogLed	integer	write
5	cfgLogClear	integer	write
6	cfgLogStatusLock	integer	write
7	cfgLogBnodeLog	interger	write
8	cfgLogSyslog	ipaddress	write

The Configure Association Table Group

ACCESSPOINT.configuration.cfgAssociation (1.3.6.1.4.1.551.2.2.1.7.x)

Object Id	Object Name	Object Type	Access
1	cfgRegAutoReg	integer	write
2	cfgRegSave	integer	write
3	cfgRegTable	Sequence of cfgRegTableEntry	
3.1	cfgRegTableEntry	Sequence	
3.1.1	cfgRegTabAddress	string	read
3.1.2	cfgRegTabName	string	read
3.1.3	cfgRegTabDevice	string	read
3.1.4	cfgRegTabRouter	string	read
3.1.5	cfgRegTabRadDst	integer	read
3.1.6	cfgRegTabBkbnDst	integer	read
3.1.7	cfgRegTabSrc	integer	read
3.1.8	cfgRegTabRegControl	integer	read
4	cfgRegNvTable	Sequence of cfgRegNvTableEntry	
4.1	cfgRegNvTableEntry	Sequence	
4.1.1	cfgRegNvTabAddress	string	write
4.1.2	cfgRegNvTabStatus	integer	write
4.1.3	cfgRegNvTabRegControl	integer	write
4.1.4	cfgRegNvTabRadDst	integer	write
4.1.5	cfgRegNvTabBkbnDst	integer	write
4.1.6	cfgRegNvTabSrc	integer	write

The Configure Ident Group

ACCESSPOINT.configuration.cfgIdent (1.3.6.1.4.1.551.2.2.1.9.x)

Object Id	Object Name	Object Type	Access
1	cfgIdIpadr	ipaddress	write
2	cfgIdImask	ipaddress	write
3	cfgIdIpGateway	ipaddress	write

The Radio Error Statistics Group

ACCESSPOINT.statistics.statRadio (1.3.6.1.4.1.551.2.2.2.1.x)

Object Id	Object Name	Object Type	Access
1	statRadLocalBufferFull	counter	read
3	statRadDuplicateRcv	counter	read
5	statRadBadCRC	counter	read
12	statRadRetries	counter	read
13	statRadMaxRetries	integer	read
16	statRadTxFull	counter	read

The Logging Group

ACCESSPOINT.logging (1.3.6.1.4.1.551.2.2.3.x)

Object Id	Object Name	Object Type	Access
1	logTable	Sequence of logTableEntry	
1.1	logTableEntry	Sequence	
1.1.1	logTabEntryIndex	integer	read
1.1.2	logTabEntryTicks	time	read
1.1.3	logTabEntryText	string	read
1.1.4	logTabEntryLevel	integer	read

The Admin Group

ACCESSPOINT.admin (1.3.6.1.4.1.551.2.2.4.x)

Object Id	Object Name	Object Type	Access
1	adminRestart	integer	write
4	adminMajVersion	integer	read
5	adminMinVersion	integer	read
6	adminBootp	integer	write
7	adminDistribute	integer	write
8	adminDistributeCnt	integer	read
9	adminPing	integer	write
10	adminPingState	integer	read
11	adminFallback	integer	write
12	adminRcvDistribute	integer	write
13	adminBetaVersion	integer	read

The Admin LinkTest Group

ACCESSPOINT.admin.adminLinktest (1.3.6.1.4.1.551.2.2.4.2.x)

Object Id	Object Name	Object Type	Access
1	adminLtMultiTest	integer	write
2	adminLtDest	string	write
3	adminLtSize	integer	write
4	adminLtCount	integer	write
5	adminLtDstRcv	counter	read
6	adminLtSrcRcv	counter	read
7	adminLtSrcXmt	counter	read
8	adminLtAveTrip	counter	read
9	adminLtMinTrip	counter	read
10	adminLtMaxtrip	counter	read
11	adminLtUniTest	integer	write
12	adminLtAuto	integer	write

The Admin FTP Group

ACCESSPOINT.admin.adminFTP (1.3.6.1.4.1.551.2.2.4.3.x)

Object Id	**Object Name**	**Object Type**	**Access**
1	adminFtpGet	integer	write
2	adminFtpDest	ipaddress	write
3	adminFtpUser	string	write
4	adminFtpPassword	string	write
5	adminFtpFile	string	write
6	adminFtpPut	integer	write

Appendix D - Aironet Technical Support

User's Guide

Use the User's Guide document number 710-004240 to learn more about operating your Aironet unit.

Communications

Use the following information to contact the Aironet Technical Support group:

Telephone	(330) 664-7903
FAX	(330) 664-7990
Email	techsupp@aironet.com

Web Site

For additional product information and technical support, including the capability to download new firmware and drivers, use the Aironet web site at:

http://www.aironet.com

Index