Spectrum24
Access Point AP-3020

Product Reference Guide

PRE-RELEASE

70-20504-02
April 1999

symbol®

www.symbol.com

Copyright

Symbol reserves the right to make changes to any product to improve reliability, function, or design.

No license is granted, either expressly or by implication, estoppel, or otherwise under any Symbol Technologies, Inc., intellectual property rights. An implied license only exists for equipment, circuits, and subsystems contained in Symbol products.

Symbol, the Symbol logo and Spectrum24 are registered trademarks of Symbol Technologies, Inc.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Novell and LAN Workplace are registered trademarks of Novell Inc.

Patents

This product is covered by one or more of the following U.S. and foreign Patents:

U.S. Patent No.4,360,798; 4,369,361; 4,387,297; 4,460,120; 4,496,831; 4,593,186; 4,603,262; 4,607,156; 4,652,750; 4,673,805; 4,736,095; 4,758,717; 4,816,660; 4,845,350; 4,896,026; 4,897,532; 4,923,281; 4,933,538; 4,992,717; 5,015,833; 5,017,765; 5,021,641; 5,029,183; 5,047,617; 5,103,461; 5,113,445; 5,130,520 5,140,144; 5,142,550; 5,149,950; 5,157,687; 5,168,148; 5,168,149; 5,180,904; 5,229,591; 5,230,088; 5,235,167; 5,243,655; 5,247,162; 5,250,791; 5,250,792; 5,262,627; 5,262,628; 5,266,787; 5,278,398; 5,280,162; 5,280,163; 5,280,164; 5,280,498; 5,304,786; 5,304,788; 5,306,900; 5,321,246; 5,324,924; 5,337,361; 5,367,151; 5,373,148; 5,378,882; 5,396,053; 5,396,055; 5,399,846; 5,408,081; 5,410,139; 5,410,140; 5,412,198; 5,418,812; 5,420,411; 5,436,440; 5,444,231; 5,449,891; 5,449,893; 5,468,949; 5,471,042; 5,478,998; 5,479,000; 5,479,002; 5,479,441; 5,504,322; 5,519,577; 5,528,621; 5,532,469; 5,543,610; 5,545,889; 5,552,592; 5,578,810; 5,581,070; 5,589,679; 5,589,680; 5,608,202; 5,612,531; 5,619,028; 5,664,229; 5,668,803; 5,675,139; 5,693,929; 5,698,835; 5,705,800; 5,714,746; 5,723,851; 5,734,152; 5,734,153; 5,745,794; 5,754,587; 5,658,383; D305,885; D341,584; D344,501; D359,483; D362,453; D362,435; D363,700; D363,918; D370,478; D383,124; D391,250.

Invention No. 55,358; 62,539; 69,060; 69,187 (Taiwan); No. 1,601,796; 1,907,875; 1,955,269 (Japan).

European Patent 367,299; 414,281; 367,300; 367,298; UK 2,072,832; France 81/03938; Italy 1,138,713.

Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, N.Y. 11742-1300
Telephone:(800)SCAN234, (516)738-2400, TLX:6711519
www.symbol.com

About This Document

This document covers...and has the following sections:

- ...
- ...
- ...

Reference Documents

This reference guide refers to the following documents:

Part Number	Document Title
70-xxxxx-01	Title

RFCs (Request For Comments) can be found on the Web at: http://www.ctrl-c.lin.se/ftp/DOC/RFC.

Conventions

Keystrokes are indicated as follows:

ENTER	identifies a key.
FUNC, CTRL, C	identifies a key sequence. Press and release each key in turn.
Press A+B	press the indicated keys simultaneously.
Hold A+B	press and hold the indicated keys while performing or waiting for another function. Used in combination with another keystroke.

Typeface conventions used include.

<angles>	indicates mandatory parameters in a given syntax.
[brackets]	for command line, indicates available parameters; in configuration files brackets act as separators for options.
GUI Screen text	indicates the name of a control in a GUI-based application.
Italics	indicates the first time a term is used, a book title, variables, and menu titles.

`Screen` indicates monitor screen dialog. Also indicates user input. A screen is the hardware device on which data appears. A display is data arranged on a screen.

Terminal indicates text shown on a radio terminal screen.

This document uses the following for certain conditions or types of information:

Note

Indicates tips or special requirements.

Caution

Indicates conditions that can cause equipment damage or data loss.

Warning

Indicates a potentially dangerous condition or procedure that only Symbol-trained personnel should attempt to correct or perform.

Contents

Chapter 1 Introduction

Spectrum24 is a frequency-hopping, spread spectrum cellular network that operates between 2.4 and 2.5 *GHz (gigahertz)*. This technology provides a high-capacity network using multiple access points within large or small environments.

Spectrum24 features include:

- bridging architecture to provide communication between radio and wired multiple network segments
- a design based on the IEEE 802.11 standard
- a 2 Mbps data rate for fast operation
- seamless roaming for mobile users with devices such as laptop computers, wireless PCs, scanning terminals and computer devices with PCMCIA slots.

1.1 Ethernet Access Point (AP)

The *Ethernet Access Point (AP)* provides a bridge between Ethernet wired LANs and Spectrum24 wireless networks. It provides transparent access between Ethernet wired networks and radio-equipped *mobile units (MUs)*. MUs include the full line of Symbol Spectrum24 terminals, scanners, third-party devices and other devices.

The AP provides 1 and 2 Mbps data transfer rate on the radio network. It monitors Ethernet traffic and forwards appropriate Ethernet messages to MUs over the Spectrum24 network. It also monitors MU radio traffic and forwards MU packets to the Ethernet LAN.

The AP meets the following:

- the regulatory requirements for Europe and many other areas of the world
- FCC part 15, class A with no external shielding
- FCC part 15 class B, ETS 300-339 compliance, including CE mark.

The AP has the following features:

- built-in diagnostics including a power-up self-check
- a four-way bridging architecture (wireless, Ethernet, PPP, internal stack)
- wireless MAC interface
- 10baseT Ethernet port interface with full-speed filtering
- 100 mW and 500 mW radio versions
- power supply IEC connector and a country-specific AC power cable
- PC/AT Serial Port Interface
- built-in antenna diversity
- multiple antenna options
- support for 127 mobile units
- SNMP support
- wireless AP support
- repeater functions.

An MU communicating with an AP appears on the network as a peer to other network devices. The wireless interface is transparent. The AP receives data from its wired or wireless interfaces and forwards the data to the proper interface.

The AP has connections for the wired network, external antennas and power supply. The AP attaches to a wall or ceiling depending on installation-site requirements.

The AP requires a single antenna for radio transmission and reception. The dual-antenna system allows the AP to select the best radio signal.

1.1.1 New Features

- IEEE 802.1d Spanning Tree Support
- Auto-Fallback to Wireless Mode
- Increased MIB support
- DHCP Support
- HTTP, Web server Support
- Mobile IP Support
- Programmable SNMP Trap Support using SNMP Agents
- Data Encryption
- Wireless Options in Radio Parameters
- ACL (Access Control List)
- AP Auto Upgrade of other APs via messaging
- Multiple Gateways.

1.2 Radio Basics

Spectrum24 uses *electromagnetic waves*, radio signals, to transmit and receive electric signals without wires. Users communicate with the network by establishing radio links between terminals and APs.

Spectrum24 uses *FM (frequency modulation)* to transmit digital data from one device to another. Using FM, a radio signal begins with a carrier signal that provides the base or center frequency. The digital data signal is superimposed on the *carrier signal (modulation)*. The radio signal propagates into the air as electromagnetic waves. A receiving antenna in the path of the waves absorbs the waves as electrical signals. The receiving device demodulates the signal by removing the carrier signal. This demodulation results in the original digital data.

Spectrum24 uses the *environment* (the air and certain objects) as the transmission medium. Spectrum24 radio devices use the 2.4 to 2.5-GHz frequency range, a license-free range throughout much of the world. The actual range is country-dependent.

Spectrum24 devices, like other Ethernet devices, have unique, hardware-encoded *Media Access Control (MAC)* or *IEEE addresses*. MAC addresses determine the device sending or receiving data. The MAC address is a 48-bit number written as six hexadecimal bytes separated by colons. For example:

```
00:A0:F8:24:9A:C8
```

To locate the AP MAC address see the bottom of the unit.

1.2.1 S24 Network Topology

The variations possible in Spectrum24 network topologies depend on the following factors:

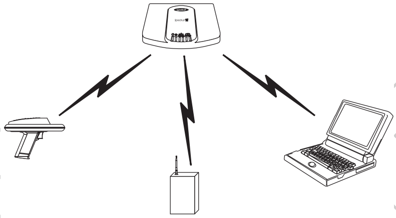
- the AP function in the network
- a 1 or 2 Mbps data transfer rate
- the *wireless AP (WLAP)* interface.

Note

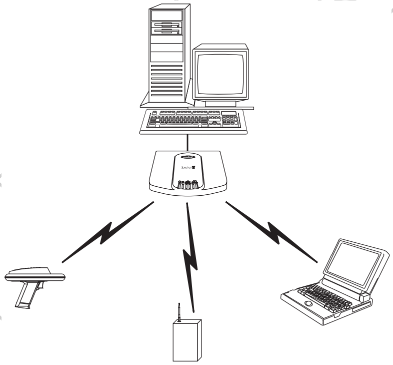
A WLAP communicates only with its root AP through the wireless interface as discussed in The Root AP and Association Process on page 14.

If the AP is not in wireless mode, select from the following topologies:

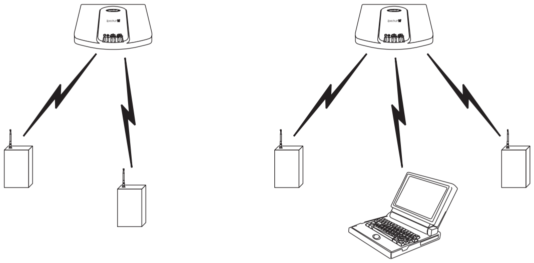
- A single AP used without the wired network provides a single-cell wireless network for peer-to-peer MUs.



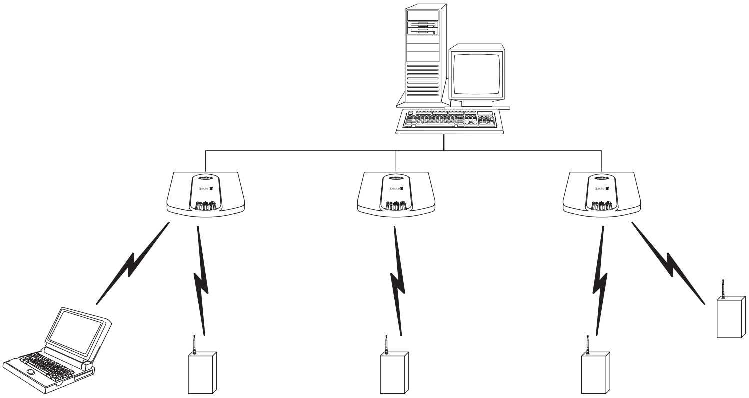
- A single AP can bridge the Ethernet and radio networks.



- Multiple APs can coexist as separate, individual networks at the same site without interference using different Net_IDs.



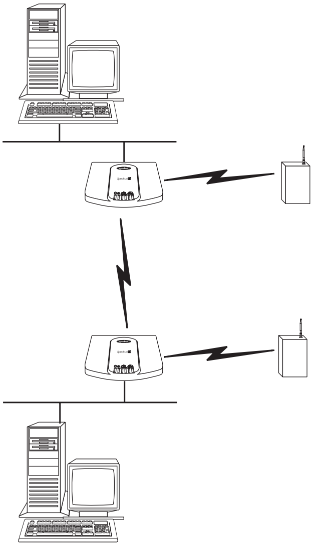
- Multiple APs wired together provide a network with better coverage area and performance.



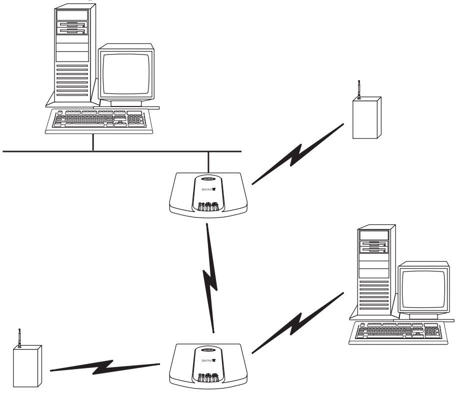
- Multiple 1 Mbps and 2 Mbps APs wired together.

In WLAP mode, a wireless AP-to-AP connection functions:

- as a bridge to connect two Ethernet networks



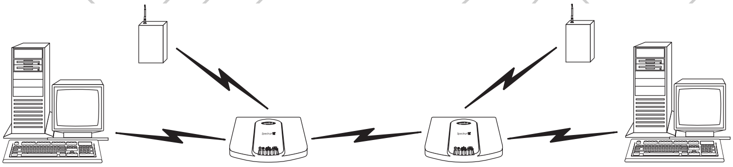
- as a repeater to extend coverage area without additional network cabling



Note

When using a wireless AP-to-AP connection, use the optimal antenna configuration for the site. For example, use a directional antenna when establishing a dedicated wireless bridge or repeater.

- A wireless AP network is possible, depending on the network bandwidth and configuration. Each wireless AP can have connections with up to four other wireless APs.



Using more than two WLAPs to establish a connection slows network performance for all topologies. If not using the AP *Auto Configure* feature, disable *WNMP Functions* and *AP-AP State Xchg* parameters under the *Set System Configuration* screen to increase WLAP performance.

Note

WNMP is a Wireless Network Management Protocol.

1.2.2 Quick Wireless AP Setup

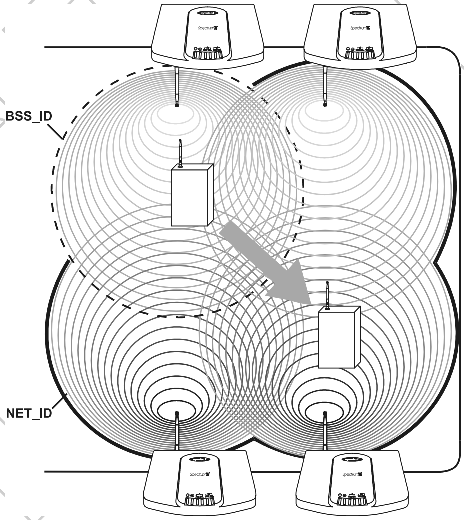
To set up an AP for wireless operation automatically, select the `Enabled` option for the *WLAP Mode* parameter. To set these values, See 2.5 Configuring Radio Parameters on page 43.

Note

The WLAP initialization process length depends on the time specified in the *WLAP Forward Delay* field. See 2.5 Configuring Radio Parameters on page 43.

1.2.3 Cellular Coverage

The AP establishes an average communication range with MUs called *a Basic Service Set (BSS*) or *cell*. When in a particular cell the MU associates and communicates with the AP of that cell. Each cell has a *Basic Service Set Identifier (BSS_ID)*. In 802.11, the AP MAC address represents the BSS_ID. The MU recognizes the AP it associates with using the BSS_ID. Adding APs to a LAN establishes more cells in an environment, making it an RF Network using the same *Net_ID or Extended Service Set (ESS)*.



APs with the same Net_ID (ESS) define the coverage area. The MU searches for APs with a matching Net_ID (ESS) and synchronizes with an AP to establish communications. This allows MUs within the coverage area to move about or *roam*. As the MU roams from cell to cell, it switches APs. The switch occurs when the MU analyzes the reception quality at a location and decides the AP to communicate with based on the best signal strength and lowest MU load distribution.

If the MU does not find an AP with a workable signal, it performs a scan to find any AP. As MUs switch APs, the AP updates the *association table*. Roaming is transparent in high-level applications.

The user can configure the Net_ID (ESS). A valid Net_ID (ESS) is an alphanumeric, case-sensitive identifier up to 32 characters. Ensure all nodes within one LAN use the same Net_ID (ESS) to communicate on the same LAN. Multiple wireless LANs can coexist in a single environment by assigning different Net_IDs (ESS) for APs.

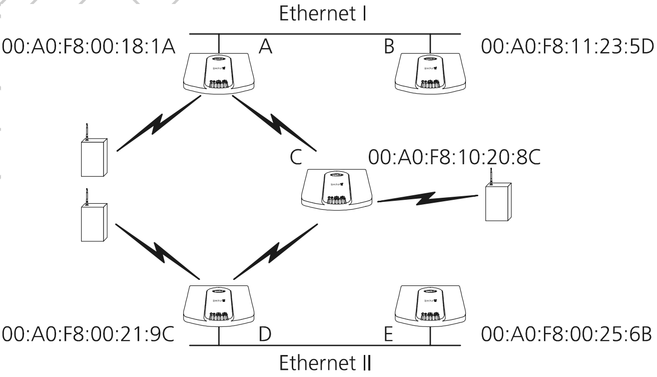
The Root AP and Association Process

By default, APs with *WLAP Mode* enabled and within range of each other automatically associate and configure wireless operation parameters at power up. This association process determines the wireless connection viability and establishes the *Root AP* and subsequently designated WLAPs.

Note

APs communicating wirelessly together require the same Net_ID (ESS) setting.

The root AP maintains the wireless connection among WLAPs by sending out beacons, sending and receiving configuration *BPDU (Bridge Protocol Data Unit)* packets between each designated WLAP. The WLAP with the lowest *WLAP ID* becomes the Root AP. The WLAP ID is a concatenation of the *WLAP Priority* value and the MAC address. Ensure the WLAPs associated with the Root AP use the Root AP hop sequence, *DTIM (Delivery Traffic Indicator Maps)* and *TIM (Traffic Indicator Message)* interval.



In this configuration, the WLAP Priority value is the default 8000 Hex. On concatenating this value to the MAC addresses of the APs, AP A on Ethernet I has the lowest WLAP ID with 800000A0F800181A, making it the Root AP. AP C uses the AP A hop sequence, DTIM and TIM interval.

If AP D on Ethernet II has data for a device on Ethernet I, it requires a bridge or a repeater. In this configuration, AP C functions as a repeater. To ensure transmission to devices on Ethernet I, AP D has to use the AP A hop sequence, DTIM and TIM interval.

Note

To prevent forming a loop, disable WLAP mode on B and E. See 2.5 Configuring Radio Parameters on page 43.

To manually designate AP B as the Root AP, assign it a lower WLAP Priority value. See 2.5 Configuring Radio Parameters on page 43. Assigning a WLAP Priority value of 7000 Hex to the AP B MAC address of 00:A0:F8:11:23:5D causes AP B to become the Root AP by having the lowest WLAP ID of 700000A0F811235D.

802.1d Spanning Tree Support

This protocol creates a *loop-free* topography with exactly ONE path between every LAN. This is the shortest path from the Root AP to each AP and LAN. If an AP or LAN fails, a new route is calculated and added to the tree. All packet forwarding follows the spanning tree. APs have to choose one AP as the Root AP. The same holds true for WLAPs associating with the root AP or another AP connected to the Ethernet LAN to prevent forming loops.

1.2.4 Site Topography

For optimal performance, locate MUs and APs away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators and other industrial equipment.

Signal loss can occur when metal, concrete, walls or floors block transmission. Locate antennas in open areas or add APs as needed to improve coverage.

In an open-air environment the radio range is up to 2000 ft. (606 m). In a typical office or retail environment the radio range is between 180 and 250 ft (54.5 to 75.7 m).

Site Surveys

A site survey analyzes the installation environment and provides users with recommendations for the equipment and its placement.

1.3 Advanced Radio Theory

To improve AP management and performance, users need to understand basic AP functionality and configuration options. The AP includes features for different interface connections and network management.

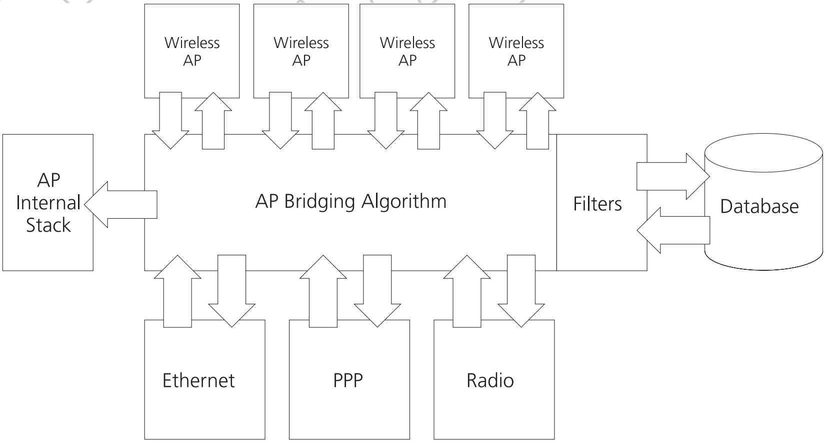
The AP provides MAC *layer bridging* between its interfaces. The AP monitors traffic from its interfaces and, based on frame address, forwards the frames to the proper destination. The AP tracks the frames sources and destinations to provide intelligent bridging as MUs roam or network topologies change. The AP also handles broadcast and multicast message initiations and responds to MU association requests.

1.3.1 MAC Layer Bridging

The AP listens to all packets on all interfaces and builds an address database using the unique IEEE 48-bit address (MAC address). An address in the database includes the interface media that the device uses to associates with the AP. The AP uses the database to forward packets from one interface to another as they arrive. The bridge forwards packets addressed to unknown systems to the Default Interface (either Ethernet or PPP). Users can use the Ethernet interface as a wireless AP interface.

Note

Users have up to four wireless AP interfaces available for the bridging algorithm (v3.10 and above only).



Note

The AP internal stack interface handles all messages directed to the AP.

Each AP stores information on destinations and their interfaces to facilitate *forwarding*. When a user sends an *ARP (Address Resolution Protocol)* request packet, the AP forwards it over all enabled interfaces (Ethernet, PPP, radio and WLAP) except over the interface the ARP request packet was received. On receiving the ARP response packet, the AP database keeps a record of the destination address along with the receiving interface. With this information, the AP forwards any directed packet to the correct destination. The AP forwards packets for unknown destinations to the Ethernet interface.

Note

Only ARP request packets received over radio are echoed-back over radio for other APs to hear.

The AP removes from its database destinations or interfaces not used for a specified time. The AP refreshes its database when it transmits or receives data from these destinations and interfaces.

Filtering and Access Control

The AP provides facilities to limit the MUs that associate with it and the data packets that can forward through it. Filters can provide network security or improve performance by eliminating broadcast/multicast packets from the radio network.

The *ACL (Access Control List)* contains the MAC addresses for MUs allowed to associate with the AP. This provides security by preventing unauthorized access.

The AP supports using a *disallowed address* list of destinations. This feature prevents the AP from communicating with specified destinations. This can include network devices that do not require communication with the AP or its MUs.

Depending on the setting, the AP can keep a list of frame types that it forwards or discards when they reach it. The *Type Filtering* option prevents specific frames (indicated by the 16-bit DIX Ethernet Type field) from being processed by the AP. These include certain broadcast frames from devices unimportant to the wireless LAN but take up bandwidth. Filtering out unnecessary frames can also improve performance.

1.3.2 Auto Fallback to Wireless Mode

The AP supports an Auto Fallback to Wireless when the hardware Ethernet connection fails or becomes broken. The AP resets itself and during initialization attempts to associate with any other WLAP in the network. This feature is available only if the WLAP Mode is enabled and the Ethernet Timeout parameter is set to one. See Configuring System Parameters on page 39 and Wireless Operation Parameters on page 46.

1.3.3 DHCP Support

The AP uses *Dynamic Host Configuration Protocol (DHCP)* to obtain a leased IP address and network configuration information from a remote server. DHCP is based on BOOTP protocol. DHCP can coexist or interoperate with BOOTP. An AP sends out a *DHCP request* searching for a *DHCP server* to acquire the network configuration and firmware filenames. Because BOOTP and DHCP are interoperable, whichever responds first becomes the server allocating the information. The DHCP client automatically sends a DHCP request every XX hours/days to renew the IP address lease as long as the AP is running. (This parameter is programmed at the DHCP server. Example: Windows NT servers typically are set for 3 days.) The AP can optionally download two files when a boot takes place, the firmware file and an HTML file, because firmware versions 4.00-31 and above support Web servers. Users can program the DHCP or BOOTP server to transfer these two files when a DHCP request is made.

When the AP receives a network configuration change or not able to renew the IP address lease the AP sends out an SNMP trap.

1.3.4 Media Types

The AP supports bridging between Ethernet, radio and serial media.

The *Ethernet interface* fully complies with Ethernet Rev. 2 and IEEE 802.3 specifications. The AP supports 10Base-T wired connections and full-speed filtering. The data transfer rate over radio waves is 1 or 2 Mbps. This rate requires adjustment of AP application time-out values for data transfer between the Ethernet and radio interfaces. The Ethernet interface is optional for single-cell or PPP-connected networks.

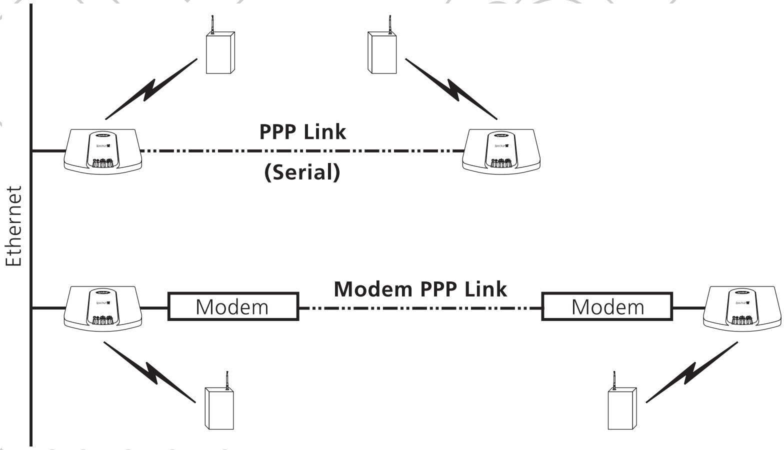
The *radio interface* conforms to IEEE 802.11 specification. The interface operates at 1 and 2 Mbps using frequency hopping, spread spectrum radio technology. The AP supports multiple-cell operations with fast, transparent roaming between cells. With the frequency-hopping system, each cell operates independently. Each cell provides a 1 or 2 Mbps bandwidth. Adding cells to the network provides increased coverage area and total system capacity. The AP supports MUs operating in *Power Save Polling (PSP)* mode or *Continuously Aware Mode (CAM)* without user intervention.

The *DB-9*, 9-pin, *RS-232 serial port* provides a *UI (User Interface)* or a *PPP (Point to Point Protocol)* connection. The UI provides basic management tools for the AP. The PPP provides a link between APs using a serial connection. The serial link supports *short haul (direct serial)* or *long haul (telephone-line)* connections. The AP is a *DTE (Data Terminal Equipment)* device with male pin connectors for the RS-232 port. Connecting the AP to a PC requires a null modem cable and connecting the AP to a modem requires a straight-through cable.

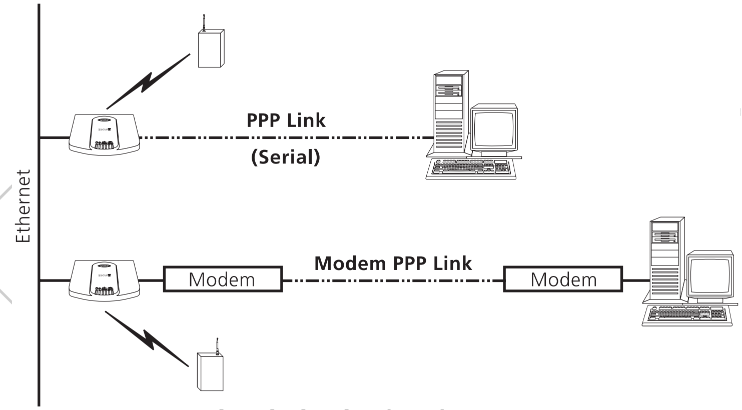
1.3.5 Bridging Support

The AP *PPP (Point to Point Protocol)* interface, accessible from the serial port at the rear of the AP, provides two types of bridging operations:

- Data-link bridging between two APs. A network using a data-link bridge provides radio coverage by using a remote AP in a location geographically distant from the AP connected to the Ethernet network. The remote AP cannot provide an Ethernet connection to other APs. MUs associating with the remote AP transmit and receive from the Ethernet network via the PPP link.



- Internet Protocol bridging between an AP and a computer. To establish an Internet Protocol bridge with an AP, ensure the computer includes the appropriate Telnet software with PPP and TCP/IP protocols. By using Telnet, a computer at a remote location can connect to any AP on an Ethernet network, as long as data transfers through IP packets.



A PPP link provides the option of using a direct serial link or modem to extend wired Ethernet topologies.

Once in PPP mode, the AP automatically attempts to communicate with the other device using the *Data-Link Bridging (DLB)* protocol. An AP using DLB communicates on the MAC level, and receives and transmits Ethernet frames.

If the other device does not support DLB, the AP attempts to communicate using *Internet Protocol Control Protocol (IPCP)*. An AP using IPCP communicates on the IP level, and receives and transmits *IP (Internet Protocol)* packets.

The PPP implementation in the AP uses the *Link Control Protocol (LCP)* and *Network Control Protocol (NCP)* as described in:

- RFC 1171: the Point-to-Point Protocol, July 1990
- RFC 1220: PPP Extensions for Bridging, April 1991
- RFC 1332: The PPP Internet Protocol Control Protocol, May 1992
- RFC 1661: The Point-to-Point Protocol, July 1994.

Note

RFCs are *Requests For Comments* used in Internet Communities.

The AP database dynamically tracks MUs and APs on the PPP interface. Packets forward to the PPP link after the AP determines their destination.

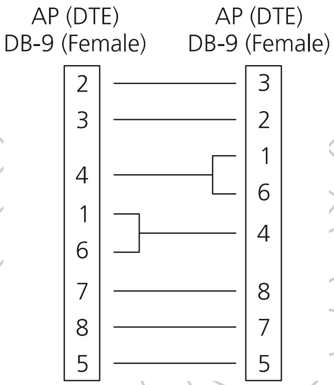
Note

The PPP implementation in the AP uses the NCP as described in *RFC 1220: PPP Extensions for Bridging* to encapsulate packets at the Ethernet level. The PPP provides IP bridging control as defined by *RFC 1172 and MAC-level bridging*. It provides support for PPP negotiations conforming to *RFC 1661*. Users cannot plug a non-AP node directly into the AP serial port, only AP-to-AP PPP links.

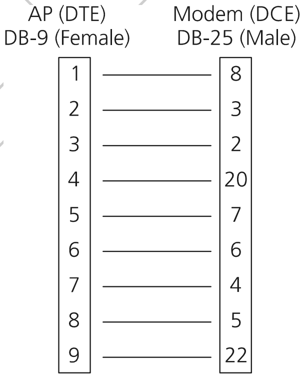
Refer to *RFC 1171: The Point to Point Protocol* and *RFC 1220: PPP Extensions for Bridging* for information.

PPP Connection

Connecting two APs with a direct serial link requires a null-modem serial cable.



Connecting two APs with modem devices requires straight-through cables between the APs and modems. Using modems requires using a telephone line for as long as the link remains active.

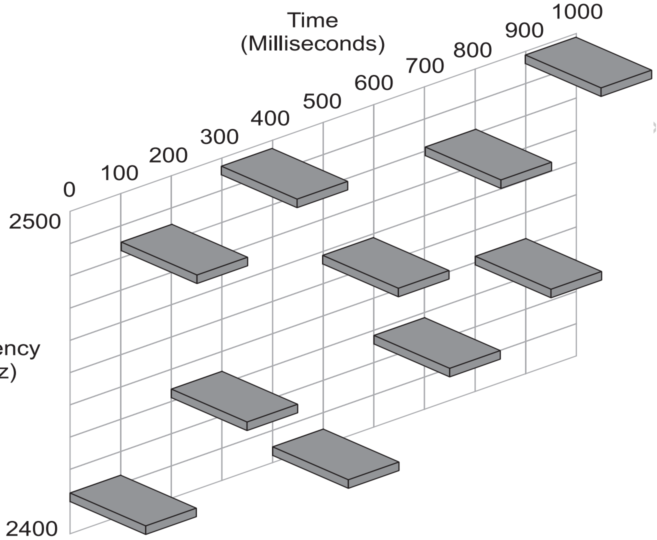


If using a modem connection, one AP represents the originating AP and the other represents the answering AP. When using a PPP link, do not use the serial port to access the UI. Access to the UI requires establishing a Telnet session with the AP.

1.3.6 Frequency Hopping Spread Spectrum

The *Spread spectrum* technique (also known as *broadband*) takes a narrowband signal and spreads the data signal over a broad segment of the radio frequency band or spectrum. Spectrum24 uses the Frequency Hopping Spread Spectrum (FHSS) technology for radio communication. FHSS spreads the signal by transmitting a short burst on one frequency, jumping to another frequency for another short burst and so on. Spectrum24 uses the 2.4 - 2.5 GHz range depending on the country, this range does not require licensing from the FCC. FHSS offers a higher transmission rate than a conventional radio narrowband method.

In FHSS systems, the carrier frequency of the transmitter changes (or hops) in accordance with the pseudo-random code sequence. The code sequence dictates the frequency order selected by the transmitter. The transmitter takes the input data and spreads it in a predefined method. Each receiver has to understand this predefined method and reconstruct the signal before interpreting data. Stations in a cell using FHSS techniques hop or change the carrier frequency at synchronized intervals. Government regulatory agencies and standards, such as ETSI, MKK, the FCC and IEEE 802.11, determine the number of frequency *hops* (79 for the U.S.), the *hopping pattern* (sequence each frequency is used) and *dwell time* (time at each frequency). The FCC requires 75 or more hopping frequencies used and a maximum of 400ms for dwell time per frequency. The transmitter and receiver synchronize to the hop sequence to ensure communication. The time synchronization field included in message packets coordinates the hop timing of all units. The user can program the length each hop lasts. Each hop is a frequency at least 6 MHz away from the previous frequency and has a 1 MHz bandwidth.



FHSS can survive in an adverse environment and coexist with other devices/services in the same band. The average signal strength being relatively low on any given frequency is a result of FHSS. When the signal intelligence is spread out over several MHz in the frequency spectrum, the resulting power spectrum also spreads out (less than 1 watt). This results in the transmitted power spread out over a wide frequency bandwidth and makes detection very difficult (without the code sequence).

Hopping provides enhanced data reception in the presence of interfering signals, like fixed frequency radio networks or microwave ovens. The system also resists interference because it spends a short time on each given frequency. If an interfering source is present (interference at a specific frequency), only a small number of frequency hops are blocked instead of the entire range. With interference occurring on one frequency, the data is retransmitted on a subsequent hop at another frequency. Even if constant interference exists on a given frequency, it affects the radio network for only a short time on that specific frequency. Although APs can share the same hopping sequence, they usually do not synchronize in time. Rarely do they simultaneously arrive at the same frequency, referred to as contention. Interfering signals can reduce overall throughput at some frequencies. This reduces the probability and impact of overlapping frequencies or collisions. Although devices can hop to the same frequency, they eventually hop to different frequencies after the hop time.

With Spectrum24, each AP on the local network negotiates a different hopping sequence at start-up. This allows APs to provide frequency separation and evenly divide the frequency spectrum among the units.

1.3.7 MU Association Process

APs recognize MUs through an association method. The AP keeps a list of MUs it services. MUs associate with the AP based on the following conditions:

- the signal strength between the AP and MU
- the MUs currently associated with the AP
- the MU Supported Rate.

Mobile Unit	**Access Point (Rate Set)**			
transmit rate (supported rates)	1 only	1 reqd, 2 optl default	1 & 2 reqd	2 only
1	1	1	NA	NA
1 & 2 default	1	Dynamic Rate Control	Dynamic Rate Control	2
2	NA	NA	NA	2

Where:

reqd = required

optl = optional

NA = No Association

Dynamic Rate Control= rate chosen for best transmission.

MUs perform preemptive roaming by intermittently scanning for APs and associating with the best available AP. Before roaming and associating with APs, MUs perform full or partial scans to collect AP frequency-hopping statistics like:

- hopping sequences
- the current hopping frequencies
- the time until the end of the hop (*hop interval*).

Scanning is a periodic process where the MU sends out probe messages on all frequencies defined by the country code. The statistics enable an MU to reassociate by synchronizing its frequency to the AP. The MU continues communicating with that AP until it needs to switch cells or roam.

MUs perform full scans at start-up. In a full scan, an MU uses a sequential set of channels as the scan range. For each channel in range, the MU tests for *CCA (Clear Channel Assessment)*. When a transmission-free channel becomes available, the MU broadcasts a probe with the Net_ID and the broadcast BSS_ID. An AP-directed probe response generates an MU ACK (Mobile Unit Acknowledgment) and the addition of the AP to the AP table with a proximity classification. An unsuccessful AP packet transmission generates another MU probe on the same channel. If the MU fails to receive a probe response within the time limits, it repeats the probe process on the next channel in the sequence. This process continues through all channels in the range.

MUs perform partial scans at programmed intervals, when missing expected beacons or after excessive transmission retries. In a partial scan, the MU scans APs classified as proximate on the AP table. For each channel, the MU tests for CCA. The MU broadcasts a probe with the Net_ID and broadcast BSS_ID when the channel is transmission-free. It sends an ACK to a directed probe response from the AP, and updates the AP table. An unsuccessful AP packet transmission causes the MU to broadcast another probe on the same channel. The MU classifies an AP as out-of-range in the AP table if it fails to receive a probe response within the time limits. This process continues through all APs classified as proximate on the AP table.

An MU can roam within the coverage area by switching APs. Roaming is transparent and virtually instantaneous in high-level applications. Roaming occurs when:

- an unassociated MU attempts to associate or reassociate with an available AP
- the supported rate changes or the MU finds a better transmit rate with another AP
- the *RSSI (received signal strength indicator)* of a potential AP exceeds the current AP
- the ratio of good-transmitted packets to attempted-transmitted packets falls below a threshold
- the MU detects an imbalance in the number of MUs associated with available APs and roams to a less loaded AP.

The MU selects the best available AP and adjusts itself to the correct hopping sequence to begin association. After establishing an association between the AP and MU, the AP begins forwarding any frames it receives addressed to the MU. Each frame from the AP contains fields for the current hop frequency and how much time remains in the current hop sequence. The MU uses these fields to resynchronize its hopping to the AP.

1.3.8 Mobile IP (Roaming Across Routers)

The Internet Protocol identifies the MU point of attachment to a network through its IP address. The AP routes packets for the MU according to the location information contained in the IP header. If the MU roams across routers to another subnet, the following situations occur:

- The MU changes its point of attachment without changing its IP address and this causes forthcoming packets to become undeliverable.
- The MU changes its IP address when it moves to a new network and this causes it to lose the connection.

Mobile IP enables an MU to communicate with other hosts using only its home IP address after changing its point-of-attachment to the internet/intranet.

Conceptually, Mobile IP is like giving an individuals local post office a forwarding address when leaving home for an extended period. When mail arrives for the individuals home address it is forwarded by the local post office to the individuals current care-of-address. Using this method, only the local post office requires notification of the individuals current address instead of each correspondent. While the example given represents the general concept of Mobile IP operation and functionality it does not represent the implementation of Mobile IP used.

A tunnel is the path taken by the original packet encapsulated within the payload portion of a second packet to some destination on the network.

A Home Agent is an AP acting as a router on the MUs home network. The home agent intercepts packets sent to the MUs home address and tunnels the message to the MU at its current location. This happens as long as the MU keeps its home agent informed of its current location on some foreign link.

A Foreign Agent is an AP acting as a router at the MUs location on a foreign link. The foreign agent de-tunnels packets for the MU sent by the MUs home agent. The foreign agent also serves as the default router for packets sent out by the MU connected on the same foreign link.

A care-of-address is the IP address used by the MU visiting a foreign link. This address changes each time the MU moves to another foreign link. It can also be viewed as an exit point of a tunnel between the MUs home agent and the MU itself.

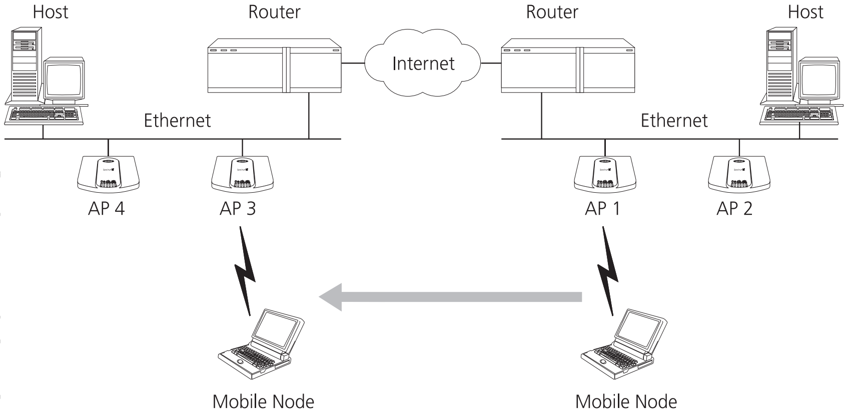
The *S24 Mobile IP (roaming across routers)* feature enables an MU on the Internet to move from one subnet to another while keeping its IP address unchanged.

Note

To configure this feature, See 2.4 Configuring System Parameters on page 39.

The scanning and associating process continues for active MUs. This allows the MUs to find new APs and discard out-of-range or deactivated APs. By always testing the airwaves, the MUs can choose the best network connection available.

The following diagram illustrates Mobile IP (roaming across routers):



Note

Set the MU for mobile IP as specified in the MUs user documentation.

Security has become a concern to mobile users. Enabling the *Mobile-Home MD5 key* option in the *System Configuration* menu generates a 16-byte *checksum authenticator* using an *MD5 algorithm*. The MU and AP share the *checksum,* called a *key,* to authenticate transmitted messages between them. The AP and MU share the key while the MU is visiting a foreign subnet. The MU and AP have to use the same key. If not, the AP refuses to become the *Home Agent* for the MU. The maximum key length is 13 characters. The AP allows all printable characters.

1.3.9 Supporting CAM and PSP Stations

CAM (Continuously Aware Mode) stations leave their radios on continuously and hear every beacon and message transmitted. These systems operate without any adjustments by the AP.

A *beacon* is a uniframe system packet broadcast by the AP to keep the network synchronized. A beacon includes the Net_ID (ESS), the AP address, the Broadcast destination addresses, a time stamp, a *DTIM (Delivery Traffic Indicator Maps)* and the *TIM (Traffic Indicator Message)*.

PSP (Power Save Polling) stations power off their radios for long periods. When an MU in PSP mode associates with an AP, it notifies the AP of its activity status. The AP responds by buffering packets received for the MU. The PSP-mode MU wakes up to listen to the AP beacon every n^{th} *Beacon Interval* where `n` is a PSP-mode value from the 1 to 10-range; the *Beacon Interval* is set on the MU. When the MU wakes up and sees its bit set in the TIM, it issues a poll request to the AP for packets stored for it. The AP sends them to the MU and the MU goes back to sleep. A DTIM field, also called a countdown field, informs MUs of the next window for listening to broadcast and multicast messages. The AP sends the messages following the `nth beacon` where `n` is the DTIM interval defined in the AP. When the AP has buffered broadcast or multicast messages for associated MUs, it sends the next DTIM with a *DTIM Interval* value. This value decreases by '1' with each successive beacon. The AP sends broadcast and multicast messages immediately following the beacon where the DTIM value is '0.' To prevent a PSP-mode MU from sleeping through a DTIM notification, select a PSP mode value less than or equal to the DTIM value. PSP-mode MUs hear the beacons and awaken to receive the broadcast and multicast messages.

A TIM is a compressed virtual bitmap identifying the AP associated MUs in PSP mode that have buffered directed messages. MUs issue a poll request when APs issue a TIM. A beacon with the broadcast-indicator bit set causes the MU to note *DTIM Count* field value. The value informs the MU of the beacons remaining before next DTIM. This ensures the MU turns on the receiver for the DTIM and the following *BC/MC packet transmissions*.

1.3.10 Data Encryption

Mobile nodes and other hosts on any network face possible information theft. This occurs when an unauthorized user eavesdrops on someone else to glean information. The absence of a physical connection makes wireless links particularly vulnerable to this form of theft. Encryption becomes the most efficient method in preventing information theft and improving data security. *Encryption* requires scrambling and coding of information, typically with mathematical formulas called algorithms, before the information is transmitted over a communications link or network. An *algorithm* is a set of instructions or formula for scrambling the data. A *key* is the specific code used by the algorithm to encrypt or decrypt the data. *Decryption* is the decoding and unscrambling of the received encrypted data. The same device, host computer or front-end processor, usually performs both encryption and decryption. The data transmit or receive direction determines whether the encryption or decryption function is performed. This device takes the plain text and scrambles or encrypts it and transmits the data over the network, typically by mathematically combining the key with the plain text as prescribed by the algorithm. At the receiving end another device takes the encrypted text and decrypts, unscrambles, the text resulting in the original plain text. An authorized user can know the algorithm, but cannot interpret the encrypted data without the appropriate key. Only the sender and receiver of the transmitted data know the *secret key*. Symbol uses the *Wired Equivalent Privacy (WEP)* algorithm, specified in IEEE 802.11 section 8, for encryption and decryption. WEP uses the same secret key for both encrypting and decrypting plain text. Typically an external key management service distributes the secret key. Users should change the key often for added security. IEEE 802.11 defines two types of *authentication*, *Open System* and *Shared Key*. *Open system authentication* is a null authentication algorithm. *Shared key authentication* is an algorithm where both the AP and the MU share an *authentication key* to perform a *checksum* on the original message. By default, IEEE 802.11 devices operate in *an open system network* where any wireless device can associate with an AP without authorization. A wireless device with a valid shared key is allowed to associate with the AP. *Authentication management messages* (packets) are unicast, meaning authentication messages transmit from one AP to one MU only, not broadcast or multicast.

1.3.11 HTTP, HTML Web Server Support

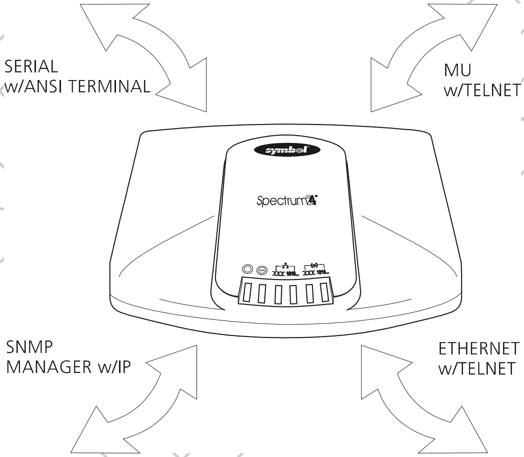
The native language of the Web is Hypertext Transfer Protocol (HTTP). The protocol makes requests from browsers (the user) to servers and responses from servers to browsers. This function provides the user with a web-based format for configuration and firmware download capabilities. Web pages are written in HTML (Hypertext Markup Language.) HTML allows the user to create web pages containing text, graphics and pointers or links to other web pages or elsewhere on the page or document. Pointers are generally known as Uniform Resource Locators (URLs). A URL is essentially the name of the web page. There are three parts to the URL:

- the protocol (sometimes called a scheme)
- the DNS (Domain Name Server) the machine where the page is located
- the local name that identifies the page (usually the filename).

The HTML language describes how to format the document. Much like a copyeditor describes which fonts to use, such as the location, color, header size and text.

1.3.12 Management Options

Managing Spectrum24 includes viewing network statistics and setting configuration options. Statistics track network activity of associated MUs and data transfers on the AP interfaces. Configuration involves setting system operating parameters and filters used in bridging.



The AP requires one of the following to perform a custom installation or maintain the Spectrum24 network:

- SNMP (Simple Network Management Protocol)
- wired or wireless LAN workstation with a Telnet client
- terminal or PC with RS-232 connection and ANSI emulation

Changing one AP does not affect the configuration of other APs on the network. Make configuration changes to APs individually. Each AP requires an individual IP address.

Programmable SNMP Trap Support

The SNMP protocol defines the method for obtaining information about the networks operating characteristics, changing parameters for routers and gateways, and consists of three elements:

- management stations
- management information
- a management protocol (MIB).

Nodes can be hosts, routers, bridges or other devices that can communicate status information. An *SNMP Agent* is a node that runs the SNMP management process to systematically monitor and manage the network. The management station performs network management by running application management software.

An *SNMP trap* is an alert to all configured management stations of some significant event that occurred on the network. The management station queries all stations for the details of each specific event, including what, when, where the event took place and the current status of the node or network. The format or structure is defined in the SNMP protocol. The MIB defines what and who monitors the variables.

Using SNMP

The AP includes *SNMP agent* versions accessible via an SNMP manager application such as, HP Open View or Cabletron Spectrum MIB browser. The SNMP agent supports SNMP versions 1 and 2, MIB II, the 802.11 MIB and one Symbol proprietary *Symbol MIB (Management Information Base)*. The SNMP agent supports read-write, read-only or disabled modes. The AP supports traps that return to the SNMP manager when certain events occur. The *Wireless LAN Installation and Utilities* disk packaged with MUs contains the MIB.

Increased MIB Support

The *MIB (Management Information Base)* defines what the management station needs to understand and which objects the station manages. The MIB has ten categories defined with approximately 175 variables.

Using the UI

The *UI (User Interface)* is a text-based maintenance tool integrated into the AP. It provides statistical displays, AP configuration options and firmware upgrades. Access to the UI requires one of the following:

Telnet Client Gain access to the AP built-in Telnet server from any AP interface including remote Ethernet connections. See Using Telnet on page 29.

Direct Serial Connection Acts as a DTE device to connect directly to a DTE device with a null-modem serial cable. The direct serial access method requires a communication program with ANSI emulation. See Using a Direct Serial Connection on page 30.

Dial Up Access The dial-up access method requires a communication program with ANSI emulation on the remote terminal or PC. The terminal or PC dials to an AP with a modem connection. The AP supports connection to a Hayes-compatible 28,800-baud or faster modem. See Using a Dial-Up Connection on page 31.

SNMP Via a MIB Browser Gain access to the AP SNMP function via a MIB Browser. Typically a Network Manager uses this feature, Symbol does not recommend AP access using this interface method. Refer to the MIB Browser documentation for usage.

Web Browser Gain access to the AP built-in Web server from any AP interface including remote Ethernet connections. See Using a Web Browser on page 33.

Chapter 2 Configuring the AP

Software configuration requires setting up a connection to the AP and gaining access to the UI (User Interface).

Note

The dot in front of certain parameters, functions or options (`.Antenna Selection Primary Only`) indicates these items are updated to all APs with the same Net_ID (ESS) when choosing the `Save ALL APs-[F2]` option.

2.1 Gaining Access to the UI

Setting up access to the UI depends on the connection used. Select the setup that best fits the network environment. If using a PPP connection, access the UI through a Telnet session.

2.1.1 Using Telnet

Using a Telnet session to gain access to the UI requires a remote station to have a TCP/IP stack. The remote station can be on the wired or wireless LAN.

To access the AP from the workstation:

1. From the DOS prompt Telnet to the AP using its IP address:

```
Telnet xxx.xxx.xxx.xxx
```

2. At the prompt enter the password:

```
Symbol
```

Note

The password is case-sensitive.

3. Press the ESC key. The AP displays the *Main Menu*:

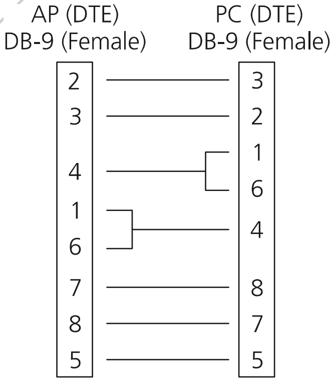
```
Symbol Access Point          MAIN MENU
Show System Summary                 AP Installation
Show Interface Statistics           Special Functions
Show Forwarding Counts              Set System Configuration
Show Mobile Units                   Set RF Configuration
Show Known APs                      Set Serial Port Configuration
Show Ethernet Statistics            Set Access Control List
Show RF Statistics                  Set Address Filtering
Show Misc. Statistics               Set Type Filtering
Show Event History                  Set SNMP Configuration
Enter Admin Mode                    Set Event Logging Configuration
```

- If the session is idle (e.g. no input) for the configured time, the session terminates.
- To manually terminate the session, press CTRL+D.

Set the *System Password* in the *Set System Configuration* screen.

2.1.2 Using a Direct Serial Connection

The AP serial port is a DB-9, 9-pin male connector. The serial port allows PPP connections to another AP, or a UI connection to a configuration PC. Connecting the AP directly to a PC with a 9-pin serial port requires a null modem cable with the following configuration:



The factory-configured AP accepts a direct serial connection to the UI. Configure the AP for the following:

- `Enable` *serial port*.
- Set *Port Use* to `UI`.
- `Disable` *modem connection*.

Note

Configure these settings in the *Set Serial Port Configuration* screen within the UI. See Configuring for Dial-Up to the UI on page 36.

Assuming the UI and serial port are enabled on the AP:

1. Attach a null modem serial cable from the AP to the terminal or PC serial port.
2. From the terminal, start the communication program.
3. Select the correct COM port along with the following parameters.

emulation	ANSI
baud rate	19200 bps
data bits	8
stop bits	1
parity	none
flow control	none

There is no password requirement.

4. Press ESC to refresh the display. The AP displays the *Main Menu*.
5. Exit the communication program to end the session.

2.1.3 Using a Dial-Up Connection

The AP supports a dial-up connection to the UI. This requires accessing the UI from Telnet or a direct serial connection and changing the serial port configuration. Configure the AP for the following:

- Enable *serial port*.
- *Set serial port* for UI.
- Disable any modem connection.
- Set AP to answer mode.

Configure these settings in the *Set Serial Port Configuration* screen within the UI. See Configuring for Dial-Up to the UI on page 36.

2.1.4 Using a Web Browser

Using a Web Browser to gain access to the UI requires the workstation to have a TCP/IP stack and access to a Web browser. The remote station can be on the wired or wireless LAN.

Note

To use this feature the Web Browser, such as Internet Explorer 4.0 and higher or Netscape, requires JavaScript.

To insure the Web Server option is enabled:

1. Access the UI using a Serial or Telnet connection.
2. Select the *System Configuration* screen.
3. Verify the Web Server option on the *System Configuration* screen is enabled.
4. Save the configuration by selecting Save-[F1].

Reset the AP for changes to take effect.

1. Select the *Special Finctions* screen.
2. Select Reset AP.
3. At the comfirmation prompt, select Yes.

To enable help file access change the Help URL parameter:

1. Select the *Special Functions* screen.
2. Select the `Alter Filename(s)/HELP URL/TFTP Server/DHCP` by pressing the e key.
3. Press ENTER.
4. Use the DOWN ARROW key to select the `.HELP URL` option.
5. Type the IP address/URL (Universal Request Locator) or the directory/ folder of the Web server for the Help file location.
6. Press ENTER.
7. Use the DOWN ARROW key to select `OK-[CR]` and press ENTER.
8. Save the new setting by selecting the `Save Configuration` option.
9. At the comfirmation prompt, select `Yes`.
10. The *Main Menu* screen is displayed.

Reset the AP for changes to take effect.

1. Select the *Special Finctions* screen.
2. Select `Reset AP`.
3. At the comfirmation prompt, select `Yes`.

Setup Web Server Help File Access

A Web server is required to access the help file from the *Spectrum24 Access Point Configuration Management System* web pages. To access the help file from a Web server create a directory/folder on the server disk for the help file to reside. Copy the *.gif and *.htm files to this direstory/folder.

Warning

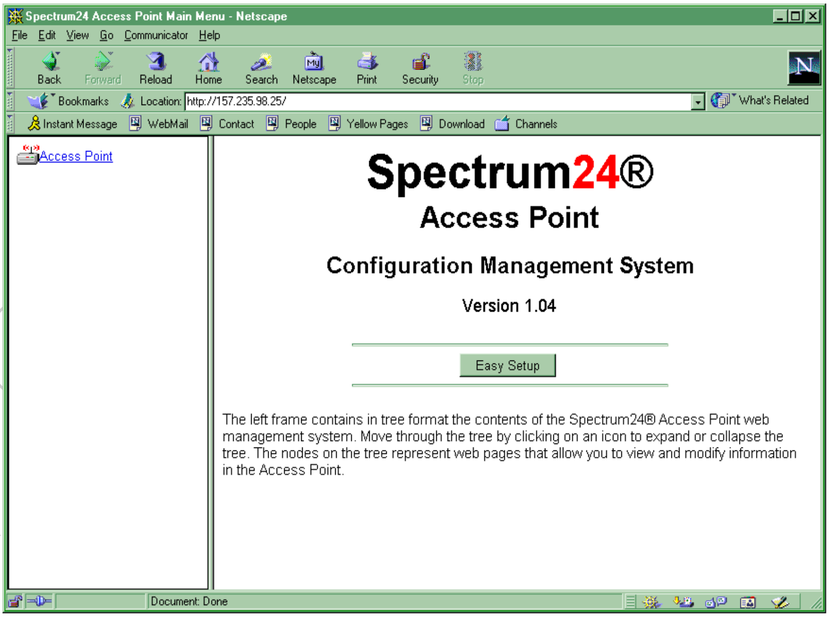
This prcedure is for Network or System Administration personnel only.

Note

This installation process is for Windows NT 4.0.

1. From the desktop windows Task Bar select Start.
2. From the pulldown menu select Programs.
3. From this menu select Microsoft Internet Server.
4. From this menu select Internet Service Manger.
5. The Internet Service Manager window is displayed.
6. Note: insure <servername> (ntserver_170) www is running.
7. Select Properties
8. Select Service Properties
9. The www Service Properties for <servername> windows opens.
10. Select the Directories Tab.
11. Select the Add button.
12. The Directory Properties window opens.
13. Type the Directory/Floder path as indicated.
14. Select the Virtual Directory button.
15. Type the folder alias and select OK.
16. Enable the Defalut document button.
17. Type S24apHelp.htm and select apply.
18. Select OK to exit the window.
19. Start the Web browser.

20. Enter the IP Address for the associated AP to access the AP via the Web browser.


Spectrum24 Access Point Main Menu - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://157.235.98.25/
What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
Access Point
Easy Setup
Document: Done

Spectrum24®

Access Point

Configuration Management System

Version 1.04

The left frame contains in tree format the contents of the Spectrum24® Access Point web management system. Move through the tree by clicking on an icon to expand or collapse the tree. The nodes on the tree represent web pages that allow you to view and modify information in the Access Point.

21. To access help from any *Spectrum24 Access Point Configuration Management System* web page select the Help button always located in the right frames top right corner on each page.

Setup Local Workstation Help File Access

To access the help file from a local workstation the Help file needs to be loaded on the hard disk.

To install the Help file run the InstallShield program.

1. From the floppy disk or Symbol Web site, http://www.symbol.com/ , click on the file UAPHTMLHelp_Install.exe Icon.
2. The **Unpacking UAP HTML Help** window appears indicating the file is unpacking and the installation help program is preparing to start.

3. The UAP HTML Help Installation Setup screen is displayed.
4. Follow the on-screen instructions to install the Help file on the local workstation hard disk.

To access the Help file located on the local workstation:

1. From the Windows Task bar click the Start button.
2. From the Start pulldown menu click Programs
3. From the Programs pulldown menu click *Symbol* Technologies or the directory name chosen during the install process.
4. Click UAP HTML Help to launch the help file program.

To exit the Help file:

1. From the window menu bar click File.
2. From the pulldown menu click Close/Exit.

Accessing Web Browser UI

To access the AP UI via a Web Browser from a workstation:

1. From the NCPA properties window set the IP address of the workstation and the subnet mask. The system tells the user to reboot for property changes to take effect.

Note

The workstation, in this case, is the workstation or laptop using the Web browser to access the UI.

2. To verify the connection, ping the AP. At the default DOS prompt, type:

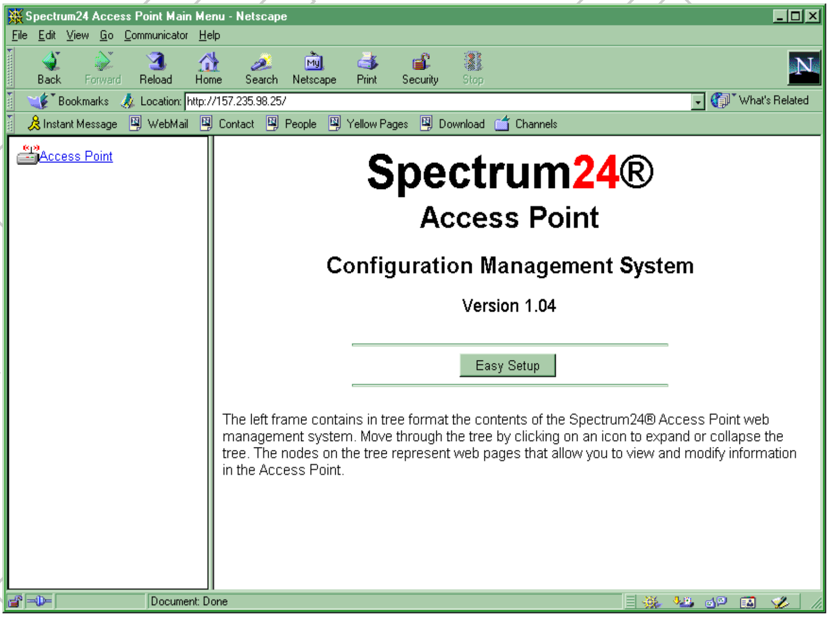
```
Ping -t xxx.xxx.xxx.xxx
```

   – If the ping receives no response, verify that the hardware connections, IP address, gateway address and subnet mask are correct. If correct, contact the site System Administrator for network assistance.

3. Type the AP IP address in the *Address field* of a Web browser such as Internet Explorer 4.0 and higher or Netscape.

```
http://xxx.xxx.xxx.xxx
```

The Main Page for the Spectrum24 Access Point Configuration Management System displays:


Spectrum24 Access Point Main Menu - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://157.235.98.25/ What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
Access Point
Easy Setup
Document: Done

Spectrum24®
Access Point
Configuration Management System
Version 1.04

The left frame contains in tree format the contents of the Spectrum24® Access Point web management system. Move through the tree by clicking on an icon to expand or collapse the tree. The nodes on the tree represent web pages that allow you to view and modify information in the Access Point.

Note

The Web pages look different than the Telnet, Direct Serial or Dial-Up Connections. Access the different pages using the nodes located in the left frame. Refer to the online help file for Web page navigation, page contents and parameter use.

4. For access to the *Easy Setup* and *Configuration* pages this popup dialogue box appears:

5. Enter the AP name.

```
Symbol Access Point
```

6. Enter the password:

```
Symbol
```

Note

The AP name and password are case-sensitive.

To manually terminate the session, exit the browser.

Note

To view configuration, function, option changes on the Web page(s) turn off the caching function for the browser used. If this property/option is not turned off the browser returns the previous view of the page without the changes. To insure the latest version of a web page is viewed set this option in the browser. For Netscape from the menu bar select Edit, Properties, Advanced, Cache. Document in cache is compared to document on network: Every time. For Internet Explorer form the menu bar select View, Internet Options, Temporary Internet files, Settings. Check for newer versions of stored pages: Every visit to the page.

Set the *System Password* under the *Configuration* folder, on the *Security* page.

2.2 Navigating the UI

The AP displays a *Main Menu* when gaining access to the UI:

```
Symbol Access Point          MAIN MENU
Show System Summary                 AP Installation
Show Interface Statistics           Special Functions
Show Forwarding Counts              Set System Configuration
Show Mobile Units                   Set RF Configuration
Show Known APs                      Set Serial Port Configuration
Show Ethernet Statistics            Set Access Control List
Show RF Statistics                  Set Address Filtering
Show Misc. Statistics               Set Type Filtering
Show Event History                  Set SNMP Configuration
Enter Admin Mode                    Set Event Logging Configuration
```

The top line displays the *System Name* for the AP (default is *Symbol Access Point*) and the name of the configuration screen.

The UI uses the following keystrokes to navigate through the menus and screens depending on the terminal emulation. For terminal emulation programs that do not support using arrow keys or function keys, use the control-character equivalents:

UP ARROW	CTRL + O
DOWN ARROW	CTRL + I
LEFT ARROW	CTRL + U
RIGHT ARROW	CTRL + P
F1	CTRL + Q
F2	CTRL + W
F3	CTRL + E
F4	CTRL + R

The following conventions also apply when navigating through screens and menus:

- To select menu items, press the key corresponding to the bold letter for the item (case-sensitive hot key). Press ENTER to select the item.
- Press TAB to scroll through menu items.
- To change menu items, note the bottom line on the screen for configuration options. For multiple choice options, press the bold letter to select. To change values, type in the value and press ENTER. If the value is invalid, the AP beeps and restores the original value. Press TAB to scroll to next menu item.
- The bottom line on the menu enables menu/screen changes to take effect. Press TAB to scroll to the item and press ENTER to select.
- When changing values such as *System Name* or *System Password*, accept values by scrolling to the next field or pressing ENTER.
- Some screens use function keys to initiate commands. For example,
- Statistic screens include `refresh (F1)` and `Timed (F2)` commands to update the display.
- Some options listed at the bottom of screens indicate possible commands for a selected item. For example, in the *Known APs* screen, highlighting an AP on the list and pressing F1 brings up the Ping function to Ping that AP.
- To exit from submenus, press ESC.

Administration screens include options for saving or clearing data that appear on the bottom line of the screen. Confirmation prompts include the following:

OK — Registers settings but does not save them in *NVM (nonvolatile memory*). A reset command returns to previously saved settings.

Save — Saves all settings (including ones not on that screen) to NVM. This is the same as *Save Configuration* in the *Special Functions* screen.

Save ALL APs — To save the *AP installation* configuration information to all APs with the same Net_ID. This option saves the configuration changes for the current AP on the *Known APs* table to update their configuration and reset after the configuration has been modified.

Cancel — Does not register settings changed in a screen.

2.2.1 Entering Admin Mode

The UI defaults to *User* mode that allows read-only access to the APs functions (e.g., view statistics). Switching to *Admin* mode provides access to configuration menus and allows the user to configure the AP.

Entering *Admin* mode requires the administration password.

1. Select *Enter Admin Mode* from the *Main Menu*. The AP prompts for the administration password:

```
Enter System Password:
```

2. Enter the default password:

```
Symbol
```

Note

The password is case sensitive.

- If the password is correct, the AP displays the Main Menu with the Enter Admin Mode menu item changed to Exit Admin Mode.
- If the password is incorrect, the AP continues to display the Main Menu with the Enter Admin Mode menu item.

Note

Set the *System password* in the *Set System Configuration* screen.

2.2.2 Changing the Access to the UI

To prevent unauthorized Telnet access, change the configuration access to the UI. This includes enabling or disabling the *Telnet Logins* or changing the *System Password*.

To change Telnet access to the AP:

1. Select *Set System Configuration* from the Main Menu.
2. Select *Telnet Logins*.
3. Press the SPACE BAR or LEFT/RIGHT-ARROW keys to toggle between Enabled and Disabled.
4. Use the TAB key to highlight the SAVE-[F1] function at the bottom of the screen, press ENTER to confirm save.

To change the *System Password*:

1. Select *Set System Configuration* from the *Main Menu*.
2. Press TAB to select *System Password*.
3. Type in the new password and press ENTER.
4. Use the TAB key to highlight the SAVE-[F1] function at the bottom of the screen, press ENTER to confirm save.

2.2.3 Configuring for Dial-Up to the UI

A dial-up connection to gain access to the UI requires a straight-through cable between the modem and the AP. The remote PC requires a modem and a communication program (e.g. Microsoft Windows Terminal program).

Note

See *Appendix B: Supported Modems* for modems supported by the AP.

Configuring Serial Port

To enable and configure the serial port connection on the AP:

1. Select *Set Serial Port Configuration* from the *Main Menu*.
2. Set the *Port Use* parameter to `PPP`.
3. Set the *Modem Connected* parameter to `Yes`.

Configure the other settings as required on the AP.

Answer Wait Time The time waiting for a remote connection before dropping the attempt. The default is `60` seconds from a 5 to 255-second range.

Modem Speaker AP sends a command to the modem to turn on/off the modem speaker. The default is `On`.

Inactivity Timeout The inactivity time on the UI that causes the AP to terminate the connection while using a modem. The default is `5` minutes from a 0 to 255-minute range. The 0 value indicates no timeout.

Configuring the Dial-Up System

Assuming the PPP, serial port and answer mode are enabled on the AP:

1. Attach the straight-through serial cable from the AP to the modem.
2. Verify modem connects to the telephone line and has power. Refer to modem documentation.
3. From the remote terminal, start the communication program.
4. Select the correct serial port along with the following parameters.

emulation	ANSI
baud rate	19200 bps
data bits	8
stop bits	1
parity	none
flow control	none

5. Dial out to the AP with the correct telephone number.
   No password required.
6. Press ESC to refresh the display. The AP displays the *Main Menu*.

Hanging Up

To hang up from the UI while connected:

1. Select the *Special Functions* Menu from the *Main Menu*.
2. Select *Modem Hangup*.

2.2.4 Navigating the UI Via a Web Browser

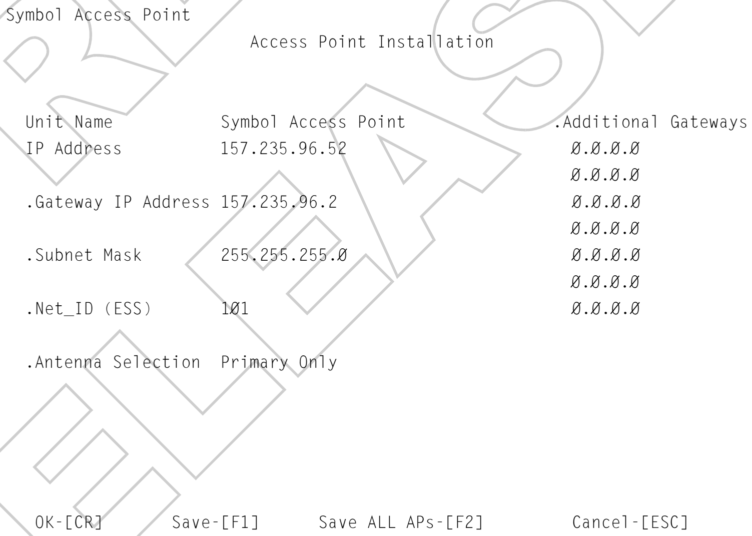
Refer to the online help file for the Web Browser navigation methods and basic functionality.

2.3 Access Point Installation

The AP UI includes an *AP Installation* screen supporting additional configuration to set basic parameters for a Spectrum24 network. These parameters include designating a gateway address that provides the ability to forward messages across routers on the wired Ethernet.

To install an AP:

1. Enter *Admin Mode*.
2. Select *AP Installation* from the *Main Menu* to display:



```
 Symbol Access Point
                          Access Point Installation


   Unit Name           Symbol Access Point              .Additional Gateways
   IP Address          157.235.96.52                      Ø.Ø.Ø.Ø
                                                          Ø.Ø.Ø.Ø
   .Gateway IP Address 157.235.96.2                       Ø.Ø.Ø.Ø
                                                          Ø.Ø.Ø.Ø
   .Subnet Mask        255.255.255.Ø                      Ø.Ø.Ø.Ø
                                                          Ø.Ø.Ø.Ø
   .Net_ID (ESS)       1Ø1                                Ø.Ø.Ø.Ø

   .Antenna Selection  Primary Only






    OK-[CR]       Save-[F1]      Save ALL APs-[F2]         Cancel-[ESC]
```

Where:

Unit Name the AP name

IP Address the network-assigned Internet Protocol address of the AP

Gateway IP Address IP address of a router the AP uses on the Ethernet default gateway

Subnet Mask The first two or three sets of numbers in the four sets of numbers making up the IP address of any device on a network represents the subnet mask values. The first two sets of numbers specify the network domain, the next set specifies the subset of hosts within a larger network and the final set specifies an individual computer. These values help divide a network into sub networks and simplify routing and data transmission.

Net_ID (ESS) the unique 32-character, alphanumeric, case-sensitive network identifier of the AP

Antenna Selection enables selection of antenna diversity

Additional Gateways The IP address of the additional gateways used. Access up to eight gateways.

3. Verify the values set reflect the network environment. Change them as needed.
4. In the *Antenna Selection* field, use SPACE BAR or LEFT/RIGHT-ARROW keys to toggle between `Primary Only` and `Primary and Secondary`.
5. To register settings select `OK` or `Save` to write changes to NVM. Selecting `Save` displays a confirmation prompt.
6. To save the *AP installation* configuration information to all APs with the same Net_ID select `Save ALL APs-[F2]`. This option saves the configuration changes for the current AP on the *Known APs* table to update their configuration and reset after the configuration has been modified.
7. To disregard any changes made to this screen and return to the previous menu, select `Cancel-[ESC]`.

2.4 Configuring System Parameters

The AP provides configuration options for how the unit operates including security access and interface control. Some parameters do not require modification.

1. Select *Set System Configuration* from the *Main Menu* to display:

```
Symbol Access Point
                             System Configuration

 Hopping Set            1                .Access Control     Disabled
 Hopping Sequence      15                .Type Filtering     Discard

 .Ethernet Timeout       0               WNMP Functions      Enabled
                                         .AP-AP State Xchg      1
 .Telnet Logins        Disabled
 .System Password      Symbol            Ethernet Interface  On
                                         PPP Interface       Off
 .Agent Ad Interval      0               RF Interface        On
 .S24 Mobile IP        Disabled
 .Mobile-Home MD5 key  Symbol            Default Interface   Ethernet

 .AP Auto Configure    Disabled

 .Web Server           Enabled



    OK-[CR]       Save-[F1]      Save ALL APs-[F2]         Cancel-[ESC]


   Hopping Set (1-3)   Save, then reset AP to take effect.
```

2. Configure the AP system settings as required:

Hopping Set — The IEEE 802.11 standard requires three hop sets identified by the numerals 1 - 3. The U.S. for example, has 3 hop sets with 26 hopping patterns available for each hop set. The default is 1. Reset the AP for the change to take effect.

Hopping Sequence — AP hopping sequence or pattern depends on the country. The U.S. for example, has 78 hopping patterns. Reset the AP for the change to take effect.

3 sets of	*1 through 26*	Standard
3 sets of	*1 through 11*	Israel and France
3 sets of	*1 through 9*	Spain
3 sets of	*1 through 4*	Japan and Korea
3 sets of	*1 through 6*	Belgium (outdoor)
3 sets of	*1 through 9*	Mexico

Ethernet Timeout Disables the radio interface if no activity is detected on the Ethernet line after the seconds indicated (30-255). The AP disassociates MUs and prevents further associations until it detects Ethernet activity again. The default value `0` disables this feature. The `1` value detects if the 10Base-T line goes down.

If the value is set to 2, the WLAP sends a *WLAP Alive BPDU* on the Ethernet line every *WLAP Hello Time* seconds to allow WLAPs on the Ethernet line to detect its existence.

If the value is set to 3, the WLAP tracks the WLAP Alive BPDU. If the BPDU is missing for WLAP Hello Time seconds, the WLAP state changes to WLAP Lost on Ethernet. Once the WLAP Alive BPDU is detected, the WLAP resets and starts over.

Note: when the Ethernet connection is broken:

- If the WLAP mode is disabled, the AP clears the MU table and disables the RF interface until the Ethernet connection comes up.

- If the WLAP mode is enabled, the AP sets the timeout value to zero (0), resets itself and attempts to associate with another WLAP in the network.

Telnet Logins Specifies if the AP accepts or rejects Telnet Logins. The default value is Enabled.

System Password For administrative access, select any alphanumeric, case-sensitive entry up to 13 characters for a password. The default System Password is Symbol.

Agent Ad Interval Specifies the interval in seconds between the mobility agent advertisement transmission.

S24 Mobile IP If enabled, this feature allows MUs to roam across routers.

Mobile-Home MD5 key Secret key used for Mobile-Home registration and authentication.

AP Auto Configure If enabled, this feature allows APs to automatically resolve hop sequence conflicts.

Web Server Enables the use of a Web based browser to access the UI instead of the HyperTerminal or Telnet applications. An AP Reset is required for this feature to take effect.

Access Control Specifies enabling or disabling the access control feature. If enabled, the ACL (Access Control List) specifies the MAC addresses of MUs that can associate with this AP. The default is Disabled.

Type Filtering Specifies filter type for packets received either Forward/Discard or Disabled. The default value is Disabled.

WNMP Functions Specifies if this AP can perform WNMP functions. The default value is Enabled.

AP-AP State Xchg Specifies AP-to-AP communication exchanged. If Disabled prevents AP Auto Configure and AP load leveling function.

3. To enable or disable interfaces on the AP, modify the following parameters:

   Ethernet Interface Enables or disables wired Ethernet. The default value is On.

   PPP Interface Enables or disables serial PPP. The default value is Off.

   RF Interface Enables or disables radio. The default value is On.

   Default Interface Specifies the default interface (Ethernet or PPP) that the AP forwards a frame to if the AP cannot find the address in its forwarding database. The default interface is Ethernet.

4. Verify the values set reflect the network environment. Change them as needed.

5. To register settings select `OK` or `Save` to write changes to NVM. Selecting `Save` displays a confirmation prompt.

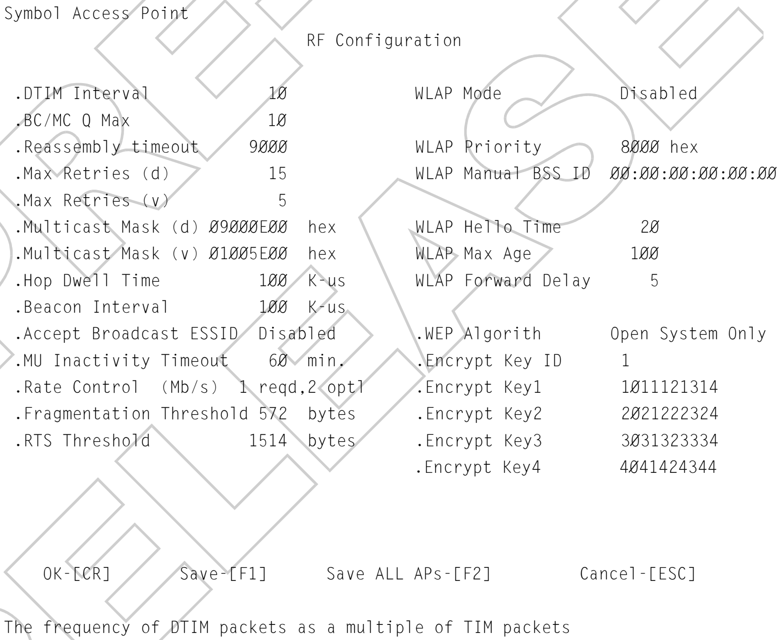
6. To save the *System Configuration* information to all APs with the same Net_ID, select `Save ALL APs-[F2]`. This option saves the configuration changes for the current AP, and sends two WNMP messages to all other APs on the *Known APs* table to update their configuration and reset after the configuration has been modified.

7. To disregard any changes made to this screen and return to the previous menu, select `Cancel-[ESC]`.

2.5 Configuring Radio Parameters

The AP auto configures most radio parameters, including the hop sequence. Only advanced users, Symbol trained users or Symbol representatives should configure radio parameters for the AP. Options in the *RF Configuration* screen fine-tune the radio and WLAP functions.

1. Select *Set RF Configuration* from the *Main Menu* to display:



```
Symbol Access Point
                               RF Configuration

 .DTIM Interval            10             WLAP Mode            Disabled
 .BC/MC Q Max              10
 .Reassembly timeout     9000             WLAP Priority        8000 hex
 .Max Retries (d)          15             WLAP Manual BSS ID  00:00:00:00:00:00
 .Max Retries (v)           5
 .Multicast Mask (d) 09000E00  hex        WLAP Hello Time        20
 .Multicast Mask (v) 01005E00  hex        WLAP Max Age          100
 .Hop Dwell Time          100  K-us       WLAP Forward Delay      5
 .Beacon Interval         100  K-us
 .Accept Broadcast ESSID  Disabled        .WEP Algorith       Open System Only
 .MU Inactivity Timeout    60  min.       .Encrypt Key ID      1
 .Rate Control  (Mb/s)  1 reqd,2 optl     .Encrypt Key1        1011121314
 .Fragmentation Threshold 572  bytes      .Encrypt Key2        2021222324
 .RTS Threshold          1514  bytes      .Encrypt Key3        3031323334
                                          .Encrypt Key4        4041424344



    OK-[CR]       Save-[F1]      Save ALL APs-[F2]        Cancel-[ESC]

The frequency of DTIM packets as a multiple of TIM packets
```

2. Configure the settings as required:

   DTIM Interval — DTIM packet frequency as a multiple of beacon packets. The DTIM Interval indicates how many beacons equal one cycle. Do not modify.

   BC/MC Q Max — Determines the memory allocated for the queue used in the AP to temporarily hold broadcast/multicast messages. Unit measure is in packets and corresponds to maximum-sized Ethernet packets. The default is `10`.

   Reassembly timeout — Sets the time in `0.5` ms units before a timeout occurs during a packet reassembly. Packet reassembly occurs when a large Ethernet packet is fragmented into smaller wireless network packets. The default is `9000`.

   Max Retries (d) — The maximum allowed retries before aborting a single transmission. The default is `15`. Should not modify.

   Max Retries (v) — The maximum allowed retries before aborting a single transmission. The default is `5`. Do not modify.

   Multicast Mask (d) — Supports broadcast download protocols for Point-of-Sale terminals that load a new operating image over the network instead of using a local nonvolatile drive. The multicast mask is the RF data packets with the top 32 bits of the MAC address and allows for a series of MAC addresses to receive multicast messages. The AP transmits these messages immediately and does not queue them for processing at DTIM intervals.

Multicast Mask (v) Supports broadcast download protocols for Point-of-Sale terminals that load a new operating image over the network instead of using a local nonvolatile drive. The multicast mask is the RF voice packets with the top 32 bits of the MAC address and allows for a series of MAC addresses to receive multicast messages. The AP transmits these messages immediately and does not queue them for processing at DTIM intervals.

Hop Dwell Time The time spent on a single channel between hops in kilo-microseconds (1024 microseconds). The default is 100. Avoid changing this parameter because it can adversely affect the performance of PSP-mode terminals.

Beacon Interval The time between beacons in kilo-microseconds. The default is 100.

Avoid changing this parameter because it can adversely affect PSP-mode terminal performance.

Accept Broadcast ESSID Allows the AP to respond to any station sending probe packets with the industry-standard broadcast ESS. If Enabled, this feature allows industry-standard devices interoperability. The AP probe response includes the ESSID and information about the network. By default, this feature is Disabled and the AP responds only to stations that know the ESSID. This helps preserve network security. MUs require using Broadcast ESS to use this function.

MU inactivity Timeout Allows industry-standard devices interoperability by specifying the time the AP allows for MU inactivity. A Spectrum24 AP recognizes MU activity through data packet transmission and reception, and through scanning. Spectrum24 MUs conduct active scanning. Other industry-standard MUs might conduct passive scans and a Spectrum24 AP can classify them as inactive.

Rate Control(Mb/s) Defines the data transmission rate:

1 reqd, 2 optl - allows the AP to automatically select the best transmit rate allowed by the conditions. All management and broadcast traffic is transmitted at 1 Mbps. This mode allows a mixtureof 1 Mbps and 2 Mbps radios in the same network.

2 only - forces the AP to always transmit at 2 Mbps and does not allow 1 Mbps stations to associate with it.

1 only - forces the AP to always transmit at 1 Mbps even if a station can transmit at a higher rate.

1 & 2 reqd - allows the AP to automatically select the best transmit rate allowed by the conditions and allows the AP to ACK received 2Mb packets at 2 Mbps. Also allows sending Broadcast traffic matching the Broadcast Mask at 2 Mbps.

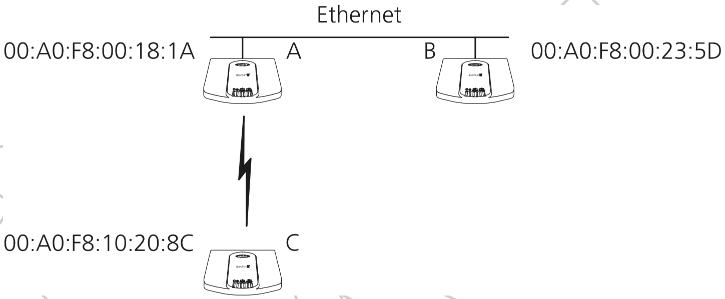
Fragmentation Threshold Defines the maximum size for directed data packets transmitted over the radio. Larger frames are fragmented into several packets this size or smaller before transmission over the radio. The receiving station reassembles the transmitted fragments. This parameter has no impact on the APs ability to receive packets. The AP can receive any packet size up to the maximum Ethernet packet size specified in IEEE 802.11.

RTS Threshold Request to send threshold (256 – 1514). Allows the AP to use RTS (Request To Send) on frames longer than the specified length. The default is 1514 Bytes.

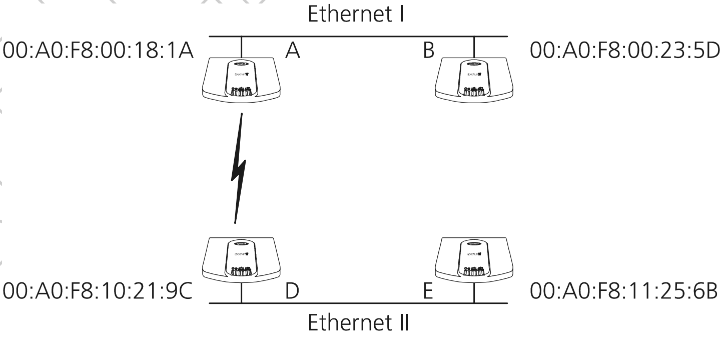
3. Verify the values set reflect the network environment. Change them as needed.
4. To register settings select `OK` or `Save` to write changes to NVM. Selecting `Save` displays a confirmation prompt.
5. To save the *RF Configuration* information to all APs with the same Net_ID, select `Save ALL APs-[F2]`. This option saves the configuration changes for the current AP, and sends two WNMP messages to all other APs on the *Known APs* table to update their configuration and reset after the configuration has been modified.
6. To disregard any changes made to this screen and return to the previous menu select `Cancel-[ESC]`.

2.5.1 Wireless Operation Parameters

The AP supports up to four WLAP interfaces. See 4.8 LED Indicators on page 102 for indication of AP status. If there are more than two WLAPs connected for repeater or bridge configuration, Symbol recommends the WLAPs with the lowest WLAP IDs be placed on the wired network.



If an AP is bridging between wired LANs, Symbol recommends one LAN contain the lower WLAP IDs. Symbol does not recommend low WLAP IDs between wired networks, this can cause root association confusion between the APs.



To configure the AP for wireless operation:

1. Select *Set RF Configuration* from the *Main Menu*.
2. Configure the settings as required:

WLAP Mode

Specifies the APs wireless-AP operation status.

Enabled, the AP sets up automatically for wireless operation.

Disabled, the AP requires user setup for wireless operation. Default setting.

Link Required, at power up the Root AP requires an Ethernet connection, the WLAP requires association with the Root AP.

Note: If these requirements are not met, the Root AP and the WLAP continuously probe for these links.

WLAP Priority

Allows a user to determine the Root and the Designated WLAP in wireless operation. Concatenate the priority value as the most significant portion of the MAC address. An AP with a lower numerical value for priority is more likely to become the root. The default is 8000 hex from the 0 - 0xFFFF range.

WLAP Manual BSS ID

Specifies the BSS_ID of a particular WLAP and forces the current AP to associate only with that WLAP.

If setting the *WLAP Manual BSS_ID* to the current BSS_ID, the current AP jumps into Functional State immediately and waits for an Association Request from the other WLAP. See 3.8 Radio Statistics on page 84. This feature speeds up the association process and minimizes confusion when more than two WLAPs try to associate with each other.

WLAP Hello Time

Sets the time lapse, in seconds, between *Config BPDU* packets sent to the Root AP by a designated WLAP. The default is 20 seconds. If the Root AP fails to hear from the designated WLAP within the *WLAP Max Age* time, it removes the designated WLAP from its interface table.

The *WLAP Hello Time* of the Root AP overwrites the WLAP Hello Time of designated WLAPs. The WLAP Hello Time does not refer to the time lapse between beacons sent by the Root AP. If a designated WLAP fails to receive a beacon, it knows that its Root WLAP has lost the Root status.

WLAP Max Age

Defines time (in seconds) before discarding aged configuration messages. This causes a disconnection between the two WLAPs. The recommended value is a multiple of the WLAP Hello Time. The default is 100 seconds.

The WLAP Max Age of the Root AP overwrites the WLAP Max Age of designated WLAPs.

WLAP Forward Delay

Specifies the time (in seconds) to prevent an AP from forwarding data packets to and from an interface during initialization. The WLAPs involved and the wireless operation state (See 3.8 Radio Statistics on page 84) affect the WLAP Forward Delay time. This delay ensures that all WLAP nodes are heard. The default is five seconds per wireless operation state.

The WLAP Forward Delay of the Root AP overwrites the WLAP Forward Delay of designated WLAPs.

WEP Algorithm

Specifies an Encryption algorithm of the AP.

Open System Only: Encryption is not enabled.

Shared Key Only: Encryption is enabled using a shared key between the AP and its associated MUs. Non-Encryption enabled MUs or MUs with a different key/key order cannot communicate with this option selected.

Open & Shared: MUs with or without encryption enabled can communicate with the AP.

Access the System Summary Screen to find the APs encryption capability. Encryption is enabled at the factory.

Note: When using the Shared Key option, the MU and AP are required to use the same key with the same value.

Encrypt Key ID

Indicates the key used to transmit data packets.

Encryption Key (1 – 4)

Four separate Encryption Keys maximum. Each key enables encryption between the AP and an associated MU with the same encryption Key and value.

Note: Keys are required to be in the same order with the same value per key for the AP and MU to authenticate data transmission using encryption. Example: AP uses `Key 1` with a value of `1011121314`. The associated MU requires the same `Key 1` with a value of `1011121314`.

2.6 Configuring PPP

To use a PPP connection, choose the hardware connection (direct or modem) and verify the enable status of serial port (default) in the System Configuration menu.

2.6.1 PPP Direct

A direct null modem serial cable connection between two APs.

From the UI:

1. Select *Set Serial Port Configuration* from the *Main Menu* to display:

```
Symbol Access Point

                       Serial Port Configuration


        Port Use        UI                    Answer Wait Time      6Ø
        Connect Mode    Answer                Inactivity Timeout     5
        Modem Connected No                    PPP Timeout            3
        Dialout Mode    Auto                  PPP Terminates        1Ø
        Modem Speaker   On
        Dialout Number  1234567




             OK-[CR]            Save-[F1]            Cancel-[ESC]

  (Use the space bar or left/right cursor keys to change)
```

2. Set the *Port Use* parameter to `PPP`.
3. Verify that the *Modem Connected* parameter setting is `No`.
4. Set the *Connect Mode* parameter to `Answer`.
5. Repeat for the other AP. Set the other APs *Connect Mode* to `Originate`.

2.6.2 Establishing Connection

To establish the PPP port connection on both APs:

1. Select *Set System Configuration* from the *Main Menu*.
2. Set the *PPP Interface* to `ON`.
3. Use the SPACE BAR or LEFT/RIGHT-arrow keys to change and press ENTER to confirm.

2.6.3 PPP with Modems

The PPP interface provides a connection using modems over a telephone line. Connect modems to the APs with straight-through serial cables. Designate one AP as the *Originating* AP and the other as the *Answering* AP. Configure the Originating AP with dial-out information to the answering AP. The answering AP waits for the originating AP to dial in to it. See *Appendix B: Supported Modems* for modems supported by the AP.

Dial out manually through the *Special Functions* menu or dial out automatically on boot.

2.6.4 Originating AP

From the originating APs UI:

1. Select Set Serial Port Configuration from the Main Menu.
2. Set the *Port Use* parameter to `PPP`.
3. Set the *Modem Connected* parameter to `Yes`.
4. Set the *Connect Mode* to `Originate`.
5. Select *Dialout Number* and enter the dialout telephone number of the answering AP (maximum 31 characters). This string matches what follows a typical Hayes Smartmodem ATDT command. Possible characters include pauses, numbers and letters. Refer to the modem documentation.
6. Set the *Dialout Mode* to `Auto`.

7. Configure the other settings as required:

   Answer Wait Time Time in seconds waiting for a remote connection before dropping attempt. The default is `60` from a `5` to `255`-second range.

   Modem Speaker Sends a command to the modem to turn on or off the modem speaker. The default is `On`.

   PPP Timeout Controls the timeout between issuing a PPP packet and expecting a reply. This is necessary if the serial connection has long delay periods. The `0` value indicates no timeout. The default is `3` from a `0` to `255-`second range.

   PPP Terminates Controls the PPP terminate requests the AP issues when a PPP-linked AP does not respond to a terminate request. The AP closes the PPP connection after making the maximum requests. The default is `10` from a `0` to `255`-terminate request range.

2.6.5 Answering AP

From the answering APs UI:

1. Select *Set Serial Port Configuration* from the *Main Menu*.
2. Set the *Port Use* parameter to `PPP`.
3. Set the *Modem Connected* parameter to `Yes`.
4. Set the *Connect Mode* to `Answer`.
5. Configure the other required settings as on the originating AP.

2.6.6 Initiating Modem Connection

To manually initiate dial-out from the originating AP to the answering AP:

1. Select the *Special Functions* Menu from the *Main Menu*.
2. Select *Modem Dialout*.

The AP dials out and attempts to make connection according to parameters set in *Serial Port Configuration*. If dial-out fails, the AP switches to manual dial-out.

Note

For automatic dial-out, reset the AP.

To hang up:

1. Select the *Special Functions* Menu from the *Main Menu*.
2. Select *Modem Hangup*.

2.7 Configuring the SNMP Agent

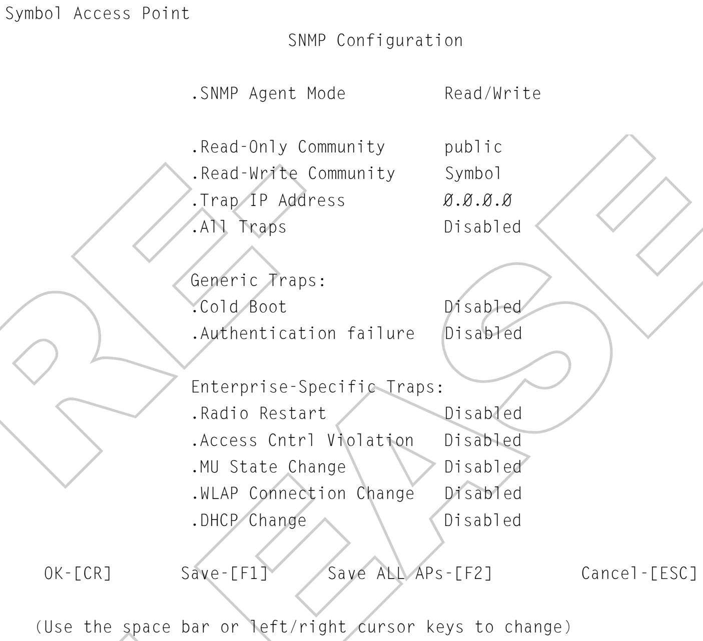
An SNMP manager application gains access to the AP SNMP agent if it has the AP IP address. The agent configures as *read-only, read-write* or *disabled* to provide security when using SNMP. The AP sends specific traps for some conditions. Ensure the SNMP trap manager recognizes how to manage these traps.

Note

Refer to the Symbol MIB on the *Wireless LAN Installation and Utilities* disk for specific entries.

The AP supports SNMP V1, MIB-II and the SYMBOL.MIB.

1. Select *Set SNMP Configuration* from the *Main Menu* to AP display:



```
Symbol Access Point
                             SNMP Configuration

                   .SNMP Agent Mode          Read/Write

                   .Read-Only Community      public
                   .Read-Write Community     Symbol
                   .Trap IP Address          Ø.Ø.Ø.Ø
                   .All Traps                Disabled

                   Generic Traps:
                   .Cold Boot                Disabled
                   .Authentication failure   Disabled

                   Enterprise-Specific Traps:
                   .Radio Restart            Disabled
                   .Access Cntrl Violation   Disabled
                   .MU State Change          Disabled
                   .WLAP Connection Change   Disabled
                   .DHCP Change              Disabled

    OK-[CR]       Save-[F1]      Save ALL APs-[F2]        Cancel-[ESC]

   (Use the space bar or left/right cursor keys to change)
```

2. Configure the settings as required:

SNMP Agent Mode — defines the SNMP agent mode:

Disabled disables SNMP functions.

Readonly allows get and trap operations.

Read/Write (default) allows get, set and trap operations.

Read-Only Community — User-defined password string up to 31 characters identifying users with read-only privileges.

Read-Write Community — User-defined password up to 13 characters for users with read/write privileges. Ensure the password used matches the System Password used to gain access to the System Configuration screen.

Trap IP Address — trap manager IP address

All Traps — Enables or disables all trap operations. The default value is Disabled.

Cold Boot — Send a trap to manager when the AP cold boots. The default value is Disabled.

Authentication failure — Indicates that community strings other than those specified for the Read-Only and Read-Write Community were submitted. The default value is Disabled.

Radio Restart — Send a trap to manager for radio restart. The default is value Disabled.

Access Cntrl Violation — Send a trap to manager when an ACL violation occurs. The default value is Disabled.

MU State Change — if enabled, this trap generates the following enterprise-specific traps:

- MU Associated
- MU Unassociated
- MU state changed from PSP mode to CAM mode
- MU state changed from CAM mode to PSP mode.

WLAP Connection Change if enabled, this trap generates the following enterprise-specific traps:

- Root WLAP Up
  Indicates that the Root WLAP connection is setup and ready to forward data.
- Root WLAP Lost
  If the current WLAP fails to receive a Beacon packet from its Root WLAP within one second, it considers the Root WLAP lost. The WLAP eventually resets itself to reestablish the network topology.
- Designated WLAP Up
  Indicates that the Designated WLAP connection is setup and ready to forward data.
- Designated WLAP Lost
  If the current WLAP fails to receive a Config BPDU packet from its Designated WLAP for MAX AGE time, it considers the Designated WLAP lost.

DHCP Change If enabled, this trap generates the following enterprise-specific traps:

- Gateway Address change
  Indicates the gateway address for the router has changed.
- IP Address Change
  Indicates the IP address for the AP has changed.
- IP Address Lease is up
  Informs the user the IP address leased from the DHCP server is about to expire.

3. Verify that the values set reflect the network environment. Change them as needed.
4. To register settings select `OK` or `Save` to write changes to NVM. Selecting `Save` displays a confirmation prompt.

5. To save the *SNMP Configuration* information to all APs with the same Net_ID, select `Save ALL APs-[F2]`. This option saves the configuration changes for the current AP, and sends two WNMP messages to all other APs on the *Known APs* table to update their configuration and reset after the configuration has been modified.
6. To disregard any changes made to this screen and return to the previous menu, select `Cancel-[ESC]`.

2.8 Configuring the ACL

The ACL supports adding MU entries by individual MAC address or by a range of MAC addresses.

1. Select the *Set Access Control List* option from the *Main Menu* to display:

```
Address Type?   range individual
```

2. Use the UP/DOWN-ARROW keys to toggle between `range` and `individual`.

2.8.1 Range of MUs

To select a range of MAC addresses:

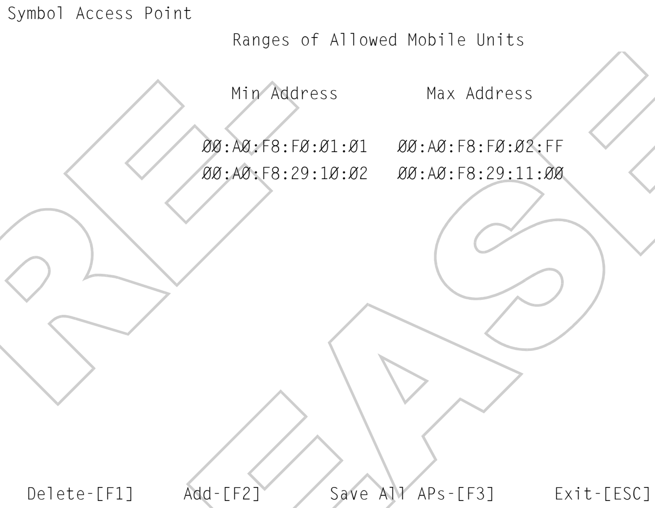
1. Type in the minimum MAC address as the top value:

```
ØØ:ØA:F8:FØ:Ø1:Ø1

ØØ:ØØ:ØØ:ØØ:ØØ:ØØ
```

2. Press ENTER to accept the value; use the DOWN-ARROW key to select the maximum value.
3. Type in the maximum MAC address in the bottom value:

```
ØØ:ØA:F8:FØ:Ø1:Ø1

ØØ:ØA:F8:FØ:Ø2:FF
```

4. Press ENTER to accept the value; use the DOWN-ARROW key to select OK.
5. Press ENTER. The UI displays:



```
Symbol Access Point
                         Ranges of Allowed Mobile Units

                         Min Address          Max Address

                      ØØ:AØ:F8:FØ:Ø1:Ø1   ØØ:AØ:F8:FØ:Ø2:FF
                      ØØ:AØ:F8:29:1Ø:Ø2   ØØ:AØ:F8:29:11:ØØ









  Delete-[F1]     Add-[F2]       Save All APs-[F3]      Exit-[ESC]
```

6. Verify the values set reflect the network environment. Change them as needed.
7. To delete a range of Mobile Units select `Delete-[F1]`.
8. To add a range of Mobile Units select `Add-[F2]`.
9. To save the *Ranges of Allowed Mobile Units* information to all APs with the same Net_ID, select `Save ALL APs-[F3]`. This option saves the configuration changes for the current AP, and sends two WNMP messages to all other APs on the *Known APs* table to update their configuration and reset after the configuration has been modified.
10. To return to the previous menu select `Exit-[ESC]`.

When users enable the *Access Control* option, all MUs within the range specified can associate with the AP. Specify additional ranges as needed or add to the ACL using individual address entries.

2.8.2 Adding Allowed MUs

The *Access Control List* screen provides a facility to add MUs to the ACL.

1. Select the *Set Access Control List* option from the *Main Menu* to display:

   ```
   Address Type?   range individual
   ```

2. Use the UP/DOWN-ARROW keys to toggle between `range` and `individual`. Select `individual`.
3. Press Add - [F2]. The AP prompts for a MAC address.

   ```
   00:00:00:00:00:00
   ```

4. Enter the MAC address.

Note

Users can enter MAC addresses without colons.

5. To save the *AP installation* configuration information to all APs with the same Net_ID, select `Save ALL APs-[F3]`. This option saves the configuration changes for the current AP, and sends two WNMP messages to all other APs on the *Known APs* table to update their configuration and reset after the configuration has been modified.

2.8.3 Removing Allowed MUs

The *Allowed Mobile Units* screen provides a facility to remove MUs from the ACL.

1. Highlight the entry using the UP/DOWN-ARROW keys.
2. Press Delete - [F1].

2.8.4 Enable/Disable the ACL

To switch between enable or disable locate the ACL in the *System Configuration* screen.

1. Select *Set System Configuration* from the *Main Menu*.
2. Press TAB to select `Access Control`.
3. Press SPACE BAR to `Enable`.
4. Select Save to save changes.

2.8.5 Removing All Allowed MUs

The AP provides a facility to remove all MUs from the ACL.

1. Select *Special Functions* from the *Main Menu*.
2. Select *Clear ACL*.

2.8.6 Load ACL from MU List

This option from the *Special Functions* menu takes all associated MUs and creates an ACL from them. This builds an ACL without having to manually enter addresses. Edit the ACL using the add and delete functions.

1. Select *Special Functions* from the *Main Menu*.
2. Select *Load ACL* from MU List to add addresses of associated MUs to the ACL.

2.9 Configuring Address Filtering

The AP can keep a list of MAC addresses of MUs not allowed to associate with it. The *Disallowed Addresses* provides security by preventing unauthorized access by known devices. Use it for preferred association of MUs to APs.

- Select *Set Address Filtering* from the *Main Menu* to display:

```
Symbol Access Point
                             Disallowed Addresses

ØØ:AØ:F8:FØ:ØØ:ØA             ØØ:AØ:F8:FØ:48:Ø1
ØØ:AØ:F8:FØ:ØØ:Ø1             ØØ:AØ:F8:FØ:ØØ:Ø2
ØØ:AØ:F8:FE:1Ø:Ø1
ØØ:AØ:F8:FØ:Ø3:ØA
ØØ:AØ:F8:FØ:Ø3:A1
ØØ:AØ:F8:BØ:AØ:Ø9
ØØ:AØ:F8:F1:A2:Ø8
ØØ:AØ:F8:FØ:Ø8:Ø8
ØØ:AØ:F8:F2:Ø6:Ø1
ØØ:AØ:F8:F2:ØB:Ø2
ØØ:AØ:F8:F2:ØC:Ø4
ØØ:AØ:F8:FØ:Ø4:Ø1
ØØ:AØ:F8:F4:Ø3:Ø2
ØØ:AØ:F8:FØ:Ø7:ØC
ØØ:AØ:F8:FØ:ØC:Ø7
ØØ:AØ:F8:F1:21:3Ø
ØØ:AØ:F8:FØ:2Ø:A1
ØØ:AØ:F8:FØ:AØ:Ø3
ØØ:AØ:F8:FØ:Ø9:ØB

 Delete-[F1]       Add-[F2]       Save All APs-[F3]      Exit-[ESC]
```

2.9.1 Adding Disallowed MUs

The *Disallowed Addresses* screen provides a facility to add MUs to the list:

1. Select Add -[F2]. The AP prompts for a MAC address.

```
00:00:00:00:00:00
```

2. Enter the MAC address.

Note

Users can enter MAC addresses without colons.

2.9.2 Removing Disallowed MUs

The *Disallowed Addresses* screen provides a facility to individually remove MUs from the list:

1. Highlight the MAC address using the UP/DOWN-ARROW keys.
2. Select Delete-[F1] to delete the MAC address.

2.10 Configuring Type Filtering

Packet types supported for the type filtering function include the 16-bit DIX Ethernet types. The list can include up to 16 types.

2.10.1 Adding Filter Types

The Type Filtering screen provides a facility to add types to the list.

1. Select Add-[F2].
2. Enter the packet type.

2.10.2 Removing Filter Types

The *Type Filtering* screen provides a facility to remove types from the list.

1. Highlight the packet type using the UP/DOWN-ARROW keys.
2. Select `Delete`.

2.10.3 Controlling Type Filters

Set the type filters to forward or discard the types listed. To control the type filtering mode:

1. Select *Set System Configuration* from the *Main Menu*.
2. Select *Type Filtering*.
3. Press the SPACE BAR to toggle between the `Forward, Discard` or `Disable` type filtering and press `ENTER` to confirm the choice.
4. To save the *Type Filtering Setup* information to all APs with the same Net_ID select `Save ALL APs-[F2]`.

2.11 Clearing MUs from the AP

Clear the MU association table for diagnostic purposes. This is necessary if the AP has many MU associations no longer in use. Use this option to ensure that MUs associating with the AP are active.

To clear MUs associated with the AP:

1. Select *Special Functions* from the *Main Menu*.
2. Select *Clear MU Table*. The AP removes MUs associated with it. MUs cleared from one AP try to reassociate with the AP or another nearby AP.

2.12 Setting Logging Options

The event log kept by the AP depends on settings for logging options. This allows the administrator to log important events. This option keeps the log concise through the 128-entry circular buffer.

1. Select *Set Event Logging Configuration* from the *Main Menu* to display:

```
Symbol Access Point

                           Event Logging Configuration


                        .Any Event Logging          Enabled

                        .Security Violations        Enabled
                        .MU State Changes           Enabled
                        .WNMP Events                Disabled
                        .Serial Port Events         Enabled
                        .AP-AP Msgs                 Enabled
                        .Telnet Logins              Enabled
                        .System Events              Enabled
                        .Ethernet Events            Disabled





    OK-[CR]       Save-[F1]       Save ALL APs-[F2]         Cancel-[ESC]
```

2. Set *Any Event Logging* to `Enabled` to log all events. Specify the events that do not require logging when disabling *Any Event Logging*. Use SPACE BAR or LEFT/RIGHT-ARROW keys to toggle between *Enabled* and *Disabled*:

Any Event Logging Logs all events listed in the screen.

Security Violations ACL filter or administrative password access violations.

MU State Changes Allows logging all MU state changes.

WNMP Events WNMP events such as MUs using WNMP.

Serial Port Events Serial port activity.

AP-AP Msgs AP to AP communication.

Telnet Logins Telnet sessions for monitoring and administration purposes.

System Events Internal use only.

Ethernet Events Ethernet events such as packet transmissions and errors.

3. Verify the values set reflect the network environment. Change them as needed.
4. To register settings select `OK` or `Save` to write changes to NVM. Selecting `Save` displays a confirmation prompt.
5. To save the *Event Logging Configuration* information to all APs with the same Net_ID, select `Save ALL APs-[F2]`. This option saves the configuration changes for the current AP, and sends two WNMP messages to all other APs on the *Known APs* table to update their configuration and reset after the configuration has been modified.
6. To disregard any changes made to this screen and return to the previous menu select `Cancel-[ESC]`.

2.13 Manually Updating AP Firmware

Options for manually updating the firmware:

- A TFTP host
- Any computer using the Xmodem file transfer protocol.

The files required for firmware updates are UAP_FW.BIN and UAP_HTML.BIN.

2.13.1 Updating using TFTP

The Ethernet TFTP upgrade method requires a connection between the AP and PC on the same Ethernet segment. Verify the PC has a TFTP server running on it. Running the server requires third party software like FTP PC/TCP for DOS or OnNet™ for Windows. The wireless TFTP upgrade method requires a connection between the AP and a TFTP server. The TFTP server can be running on a Symbol Spectrum24 device.

Updating the firmware requires a TFTP server running in the background.

To update the AP firmware:

1. Copy the Firmware files UAP_FW.BIN and UAP_HTML.BIN on the terminal or PC hard disk.
2. Telnet to the AP using its IP address.
3. At the prompt enter the password:

```
Symbol
```

Note

The password is case-sensitive. Set the *System Password* in the *Set System Configuration* screen.

The AP displays the *Main Menu*.

4. Select *Special Functions* from the *Main Menu*.
5. Select *Alter Filename(s)/HELP URL/TFTP* and press ENTER.
6. Enter the firmware filename in the *Download Filename* field:

Note

Change this only if the user or system/network administrator requires a new filename. The defaults are UAP_FW.BIN and UAP_HTML.BIN.

`uap_fw.bin` or `uap_html.bin`

Caution

Ensure the file name is UAP_FW.BIN or UAP_HTML.BIN unless the user changed the filename.

Note

Verify the path for the file name is accurate. (See step one)

7. Enter the TFTP Server IP address in the *TFTP Server* field.
8. Press ENTER.
9. Select *Save Configuration* to save settings.
10. Select *Special Functions* from the *Main Menu*.
11. Select *Use TFTP to Update Access Point's* and press ENTER.
12. “Are you sure (Y/N)?” Type “`y`”.

Note

The Telnet session ends when the user answers “`y`” at the prompt.

- The WIRED LAN ACTIVITY indicator on the AP does NOT flash.

Note

To view the file transfer log, switch to the TFTP application.

The AP resets when the file transfer and flash programming completes.

13. Telnet to the AP using its IP address.
14. At the prompt enter the password:

```
Symbol
```

Note

The password is case-sensitive.

The AP displays the *Main Menu*.

15. Verify that the version number is correct on the *System Summary* screen.
16. Press CTRL+D to end Telnet session.
17. Repeat process for other APs in the network.

2.13.2 Updating using Xmodem

The Xmodem upgrade method requires a direct connection between the AP and PC using a Null modem serial cable and using software like HyperTerminal for Windows 95 or Terminal mode for Windows 3.11. Xmodem supports file transfers between terminal emulation programs and the AP UI.

Note

Xmodem transfers require more time than TFTP transfers.

To update the AP firmware:

1. Copy the firmware files UAP_FW.BIN and UAP_HTML.BIN on to the terminal or PC hard disk.
2. Attach a null modem serial cable from the AP to the terminal or PC serial port.
3. On the PC, start the communication program.
4. Name your session Spectrum24 AP and select OK.

Note

The procedure described below is for Windows 98.

5. Select the correct communication port, typically Direct to Com1, along with the following parameters:

emulation	ANSI
baud rate	19200 bps
data bits	8
stop bits	1
parity	none
flow control	none

6. Select OK.
7. Press ENTER to display the *Main Menu*.
8. Select *Enter Admin Mode* and enter the password:

```
Symbol
```

Note

The password is case-sensitive.

9. Enter the *Special Functions* screen.
10. Under the function heading *Use XMODEM to Update Access Point's*, select `Firmware`, `HTML` or `Both`.
11. Press ENTER.

Note

Selecting `Both` downloads the files UAP_FW.bin and HTML.bin. Insure both file are located in the same directory before the download begins.

12. At the confirmation prompt, press `Y` to display:

```
Downloading firmware using XMODEM.

Send firmware with XMODEM now ...
```

Where UAP_FW.BIN or UAP_HTML.BIN are the firmware files.

Caution

When using Xmodem, verify the file is correct before a send. An incorrect file can render the AP inoperable.

13. In the emulation program, such as HyperTerminal, menu bar, select Transfer.
14. Select the **Send File** command.
15. Select the Browse button and locate the file(s), UAP_FW.BIN or UAP_HTML.BIN.
16. Select XModem protocol from the drop down list.
17. Select the Send `button`.
18. The terminal or PC displays the transfer process through a progress bar.

The AP automatically resets when the file transfer completes.

19. Exit the communication program to cancel the session.
20. Repeat this process for other APs in the network.

2.14 Auto Upgrade all APs Via Messaging

The Update ALL Access Points option up/downgrades the firmware of all associated APs with the same Net_ID. Users can find the specific APs that have firmware up/downgraded on the *Known APs* screen. The time interval between the WNMP update firmware commands for updating each AP is 2 seconds. This interval prevents more than one AP at a time from accessing the TFTP server and causing network congestion. The Ethernet TFTP upgrade method requires a connection between the AP and PC on the same Ethernet segment. Verify the PC has a TFTP server running on it. Running the server requires third party software like FTP PC/TCP for DOS or OnNet™ for Windows. The wireless TFTP upgrade method requires a connection between the AP and a TFTP server. The TFTP server can be running on a Symbol Spectrum24 device.

Updating the firmware requires a TFTP server running in the background.

To update the AP firmware:

1. Copy the Firmware files UAP_FW.BIN and UAP_HTML.BIN on the terminal or PC hard disk.
2. Telnet to the AP using its IP address.
3. At the prompt enter the password:

```
Symbol
```

Note

The password is case-sensitive. Set the *System Password* in the *Set System Configuration* screen.

The AP displays the *Main Menu*.

4. Select *Special Functions* from the *Main Menu*.
5. Select *Alter Filename(s)/HELP URL/TFTP Server* and press ENTER.
6. Enter the firmware filename in the *Download Filename* field:

Note

Change this only if the user or system/network administrator requires a new filename. The defaults are UAP_FW.BIN and UAP_HTML.BIN.

`uap_fw.bin` or `uap_html.bin`

Caution

Ensure the file name is UAP_FW.BIN or UAP_HTML.BIN unless the user changed the filename.

Note

Verify the path for the file name is accurate. (See step one)

7. Enter the TFTP Server IP address in the *TFTP Server* field.
8. Press ENTER.
9. Select *Save Configuration* to save settings.
10. Select *Special Functions* from the *Main Menu*.
11. Select *Use TFTP to update ALL Access Point's* and press ENTER.
12. "Are you sure (Y/N)?"   Type "`y`".

Note

The Telnet session ends when the user answers "`y`" at the prompt.

– The WIRED LAN ACTIVITY indicator on the AP does NOT flash.

Note

To view the file transfer log, switch to the TFTP application.

The AP resets when the file transfer and flash programming completes.

13. Telnet to the AP using its IP address.
14. At the prompt enter the password:

```
Symbol
```

Note

The password is case-sensitive.

The AP displays the *Main Menu*.

15. Verify that the version number is correct on the *System Summary* screen.
16. Press CTRL+D to end Telnet session.

2.15 Performing Pings

A ping sends a packet to an MU or AP and waits for a response. Use pings to evaluate communication between two stations. The other station can exist on any AP interface.

Note

This ping operates at the MAC level and not at the *ICMP (Internet Control Message Protocol)* level.

No pings received or fewer pings received than sent can indicate a communication problem between the AP and the other station.

To ping another station:

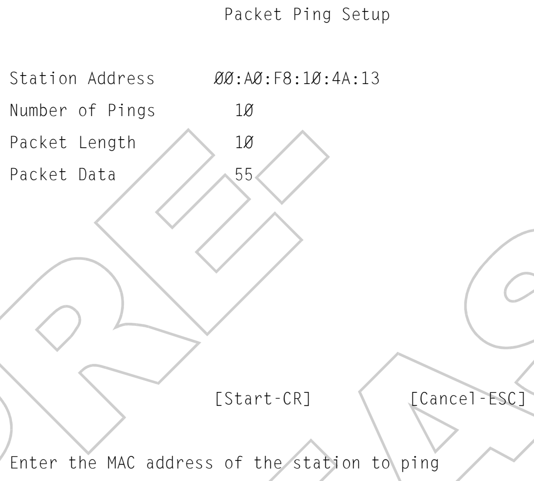
1. Select the *Show Mobile Units* screen from the *Main Menu* to display:

```
Symbol Access Point
                             MAIN MENU
   Show System Summary                 AP Installation
   Show Interface Statistics           Special Functions
   Show Forwarding Counts              Set System Configuration
   Show Mobile Units                   Set RF Configuration
   Show Known APs                      Set Serial Port Configuration
   Show Ethernet Statistics            Set Access Control List
   Show RF Statistics                  Set Address Filtering
   Show Misc. Statistics               Set Type Filtering
   Show Event History                  Set SNMP Configuration
   Enter Admin Mode                    Set Event Logging Configuration
   Regular   Home Agent   Foreign Agent
```

2. Select *Regular* from the *Show Mobile Units* screen to display:

```
Symbol Access Point
                             Mobile Units

 00:A0:F8:29:C9:E2: C:R2:E
 00:A0:F8:10:4B:AB: P:R2:V
 00:a0:F8:10:4A:13: P:R1:
 00:A0:F8:10:3C:85: C:R2:





Symbol Access Point
                             Mobile Units

 00:A0:F8:29:C9:E2: C:R2:E
 00:A0:F8:10:4B:AB: P:R2:V
 00:a0:F8:10:4A:13: P:R1:
 00:A0:F8:10:3C:85: C:R2:





Symbol Access Point
                             Mobile Units

 00:A0:F8:29:C9:E2: C:R2:E
 00:A0:F8:10:4B:AB: P:R2:V
 00:a0:F8:10:4A:13: P:R1:
 00:A0:F8:10:3C:85: C:R2:






    Information-[CR]    Ping-[F1]    Timed-[F2]    Next-[F3]    Exit-[ESC]
```

Press TAB to highlight the MAC address of the station to ping and select `Ping-[F1]` by pressing [F1] to display the *Packet Ping Setup* screen:



```
                      Packet Ping Setup


   Station Address      00:A0:F8:10:4A:13
   Number of Pings        10
   Packet Length          10
   Packet Data            55











                     [Start-CR]          [Cancel-ESC]


   Enter the MAC address of the station to ping
```

3. Enter the number of Pings (1 to 539), length of packets in bytes (1 to 539) and data content in hex (0x00 to 0xFF).

4. Select *[Start-CR]* to begin ping. The AP dynamically displays ping packets transmitted and received:

```
                 Pinging Station...



      Station Address      ØØ:AØ:F8:1Ø:4A:13
      Pings Transmitted    1
      Pings Received       1







                 Press any key to stop
```

```
To abort the process, press any key.
```

2.16 Mobile IP Using MD5 Authentication

Users can achieve true authentication by using the *MD5 algorithm* with a shared key configured into the AP and its MU. MD5 is *a message-digest algorithm* that takes an arbitrarily long message and computes a fixed-length digest version, consisting of 16 bytes (128 bits), of the original message. Users can think of the message-digest as a *fingerprint* of the original message. Since the message-digest is computed using a mathematical formula or algorithm, the probability of an entity reproducing the message-digest is equivalent to two people having the same fingerprints. The message-digest is the authentication checksum of a message from a mobile MU to an AP during the Home Agent registration process. The MD5 algorithms purpose, therefore, prevents an MU from impersonating an authenticated MU.

2.17 Saving the Configuration

The AP keeps only saved configuration changes after a reset. To make configuration changes permanent, save changes as needed.

To save all changes:

- Press F1 in the configuration screens that display the `Save` option.

OR

1. Select *Special Functions* from the *Main Menu* to display:

```
Symbol Access Point
                             Special Functions Menu

   Clear All Statistics      Use TFTP to update Access Point's:
   Clear MU Table              Firmware   HTML file   BOTH
   Clear ACL
   Clear Address Filters     Use XMODEM to update Access Point's:
                               Firmware   HTML file   BOTH
   Load ACL from MU List
                             Use TFTP to update ALL Access Points':
   Modem Dialout               Firmware   HTML file
   Modem Hangup
                             Alter Filename(s)/HELP URL/TFTP Server/DHCP
   Reset AP                    .Firmware Filename uap_fw.bin
                               .HTML Filename     uap_html.bin
   Run MKK Tests               .HELP URL http://www.symbol.com
                               .TFTP Server       157.235.99.236
   Restore Factory Config.     .DHCP              Disabled
   Save Configuration          Save All APs
   Save Config. to All APs



                                  Exit-[ESC]
```

2. Select *Save Configuration* and press `ENTER`.
3. The `Save All APs` function saves only the five preceding items. The function does not save other configuration parameters when selected.

The NVRAM stores saved configuration information. To clear the NVRAM-stored configuration, see 2.17 Restoring Configuration on page 67.

2.18 Resetting the AP

Resetting an AP clears statistics and restores the last saved configuration information. If users make unsaved changes, the AP clears those changes and restores the factory defaults on reset.

- Select Special Functions from the Main Menu.
- Select *Reset AP*.

The AP flashes its LEDs as if powering up and returns to a STATUS-flashing state.

2.19 Restoring Configuration

If the AP fails to communicate due to improper settings, it might be necessary to restore the factory configuration defaults. Restoring configuration settings clears all configuration and statistics for the AP.

To restore factory configuration:

1. Select Special Functions from the Main Menu.
2. Select Restore Factory Configuration. The AP erases all configuration information and replaces it with the factory configuration.

Chapter 3 Monitoring Statistics

The AP keeps statistics of its transactions during operation. These statistics indicate traffic, transmission success and the existence of other radio network devices. Clear statistics as needed.

3.1 System Summary

The *Show System Summary* screen displays information about the APs configuration.

To view information about the AP configuration:

1. Select *Show System Summary* from the *Main Menu* to display:

```
Symbol Access Point
                             System Summary

 Unit Name          Symbol Access Point
 MAC Address (BSS)  ØØ:AØ:F8:73:51:F2     Access Control    Disabled
 IP Address         157.235.95.225        WLAP Mode         Enabled
 Net_ID (ESS)       CA2
                                          Model Number      AP-3Ø2Ø
 Hopping Set          1                   Serial Number     ALPH3Ø69
 Hopping Sequence    23                   Hardware Revision Rev 4
 Country            United States
 Antenna Selection  Primary Only          AP Firmware Ver.  Ø4.Ø1-13
 Rate Control          2 only             HTML  File  Ver.   1.Ø2
 WEP Algorithm       Shared Key Only

 Current MUs           Ø
 Total Assoc           Ø

 System Up Time       27:54:21



                             Exit-[ESC]
```

Information includes:

Unit Name Identifies the AP name.

Mac Address (BSS) Identifies the unique 48-bit, hard-coded Media Access Control address.

IP Address Identifies the network-assigned Internet Protocol address.

Net_ID (ESS) Identifies the unique 32-character, alphanumeric, case-sensitive network identifier.

Hopping Set An industry standard requires three hop sets identified by the numerals 1 - 3. To establish these hop sets, divide the number of hop sequences for each country by three.

Hopping Sequence	*3 sets of*	*1 through 26*	Standard
	3 sets of	*1 through 11*	Israel and France
	3 sets of	*1 through 9*	Spain
	3 sets of	*1 through 4*	Japan and Korea
	3 sets of	*1 through 6*	Belgium (outdoor)
	3 sets of	*1 through 9*	Mexico

Country Identifies AP country code that in turn determines the AP hopping sequence and channel range.

Antenna Selection Indicates whether the AP is configured for single or dual antenna mode.

Rate control defines the data transmission rate:

1 reqd, 2 optl - allows the AP to automatically select the best transmit rate allowed by the conditions. All management and broadcast traffic transmits at 1 Mbps. This mode allows a mixture of 1 Mbps and 2 Mbps radios in the same network.

2 only - forces the AP to transmit at 2 Mbps and does not allow 1 Mbps stations to associate with it.

1 only - forces the AP to always transmit at the lower rate regardless of whether a station is capable of the higher rate.

1 & 2 reqd - allows the AP to automatically select the best transmit rate allowed by the conditions and allows the AP to ACK received 2Mb packets at 2 Mbps. Also allows *Broadcast traffic* matching the *Broadcast Mask* sending at 2 Mbps.

Encryption Mode Indicates whether the AP has been manufactured with Encryption capabilities enabled.

WEP Algorithm Specifies an Encryption algorithm of the AP.

Open System Only: Encryption is not enabled.

Shared Key Only: Encryption is enabled using a shared key between the AP and its associated MUs. Non-Encryption enabled MUs or MUs with a different key/key order cannot communicate with this option selected.

Open & Shared: MUs with or without encryption enabled can communicate with the AP.

Access the System Summary Screen to find the APs encryption capability. Encryption is enabled at the factory.

Note: When using the Shared Key option, the MU and AP are required to use the same key with the same value.

Current MUs Specifies the current number of MUs associated with this AP.

Total Assoc Specifies the total MU associations handled by this AP.

System Up Time Specifies how long the system has been operational. System Up Time resets to zero after reaching a maximum 120 hours.

Access Control Specifies if the access control feature is enabled or disabled. If enabled, the ACL specifies the MAC addresses of the MUs that can associate with this AP.

WLAP Mode Specifies if enabling the wireless AP operation status.

If enabled, the AP sets up automatically for wireless operation. This feature is disabled by default.

Model Number Identifies the model number.

Serial Number States the APs unique identifier.

Hardware Revision Specifies the hardware version.

AP Firmware Ver Specifies the firmware version.

2. Press `ESC` to return to the previous menu.

3.2 Interface Statistics

The *Interface Statistics* screen provides:

- packet forwarding statistics for each interface (Ethernet, PPP, RF)
- performance information for each interface in packets per second (PPS) and bytes per second (BPS).

The AP interface indicates packets sent to the AP protocol stack (e.g. configuration requests, SNMP, Telnet).

- Select *Interface Statistics* from the *Main Menu* to display:

```
Symbol Access Point            Interface Statistics

------------------- Interface Counts ----------------------

              Packets     Packets       Bytes       Bytes
               Sent        Rcvd         Sent        Rcvd

Ethernet          14Ø66          Ø      126Ø844           Ø
PPP                   Ø          Ø            Ø           Ø
RF                    Ø          Ø            Ø           Ø
AP                13975          Ø      125775Ø           Ø

------------------ Interface Rates -----------------------

                 PPS         PPS         BPS         BPS
                 Sent        Rcvd        Sent        Rcvd

Ethernet              Ø           Ø           Ø           Ø
PPP                   Ø           Ø           Ø           Ø
RF                    Ø           Ø           Ø           Ø
AP                    Ø           Ø           Ø           Ø

        Refresh-[F1]       Timed-[F2]         Exit-[ESC]
```

– To update the values manually at the status display select `Refresh`.

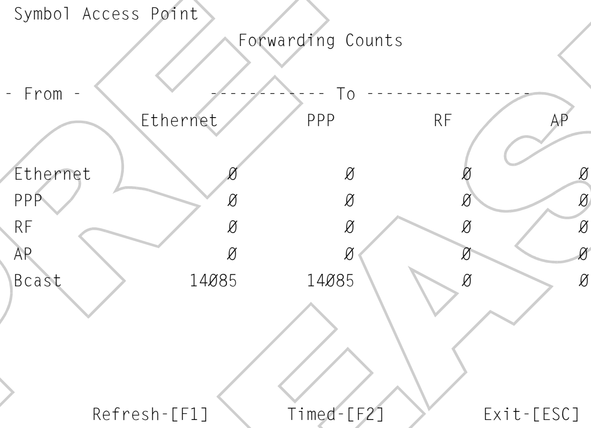
– To have the AP automatically update the display every two seconds select `Timed`.

– To return to the previous menu press ESC.

3.3 Forwarding Counts

Forwarding Counts provides information on packets transmitted from one interface to another (Ethernet, PPP, radio, AP). Forwarding Counts also displays the broadcast packets (Bcast) transmitted from the AP.

- Select *Forwarding Counts* from the *Main Menu* to display:



```
 Symbol Access Point
                        Forwarding Counts

- From -            ------------ To ----------------
              Ethernet         PPP          RF           AP

 Ethernet            Ø            Ø            Ø            Ø
 PPP                 Ø            Ø            Ø            Ø
 RF                  Ø            Ø            Ø            Ø
 AP                  Ø            Ø            Ø            Ø
 Bcast           14Ø85        14Ø85            Ø            Ø




         Refresh-[F1]        Timed-[F2]         Exit-[ESC]
```

– To update the values manually at the status display select `Refresh`.

– To have the AP automatically update the display every two seconds select `Timed`.

– To return to the previous menu press ESC.

3.4 Mobile Units

Mobile Units statistics provide information on MUs associated with the AP. The statistics include information on data sent and received, activity and association. An MU shows only in the *Home/Foreign Agent Table* screens when an MU has roamed to another AP on a different subnet. Once an MU has roamed, the MU *IP Address* displays on the *Home Agent Table* screen of the MU "home" AP with the IP Address of the *Foreign Agent* to tell the "home" AP where to forward packets. The MU IP Address is also shown in the *Foreign Agent Table* and *Regular* screens of the new "foreign" AP to tell the new AP where to expect packets from for newly associated MUs. The AP Regular screen shows only the MUs associated locally on the same subnet.

- Select *Show Mobile Units* from the *Main Menu* to display:

```
Symbol Access Point
                             MAIN MENU
   Show System Summary                  AP Installation
   Show Interface Statistics            Special Functions
   Show Forwarding Counts               Set System Configuration
   Show Mobile Units                    Set RF Configuration
   Show Known APs                       Set Serial Port Configuration
   Show Ethernet Statistics             Set Access Control List
   Show RF Statistics                   Set Address Filtering
   Show Misc. Statistics                Set Type Filtering
   Show Event History                   Set SNMP Configuration
   Enter Admin Mode                     Set Event Logging Configuration
   Regular   Home Agent   Foreign Agent
```

Use the TAB or arrow keys to highlight the desired screen. Press ENTER to display the selected screen.

- Select *Regular* from the *Mobile Units* prompt to display:

```
Symbol Access Point          Mobile Units



00:A0:F8:29:C9:E2: C:R2:E
00:A0:F8:10:4B:AB: P:R2:V
00:A0:F8:10:4A:13: P:R1:
00:A0:F8:10:3C:85: C:R2:






    Information-[CR]    Ping-[F1]    Timed-[F2]    Next-[F3]    Exit-[ESC]
```

The display shows the currently associated MUs listed by MAC address. The list appears as follows:

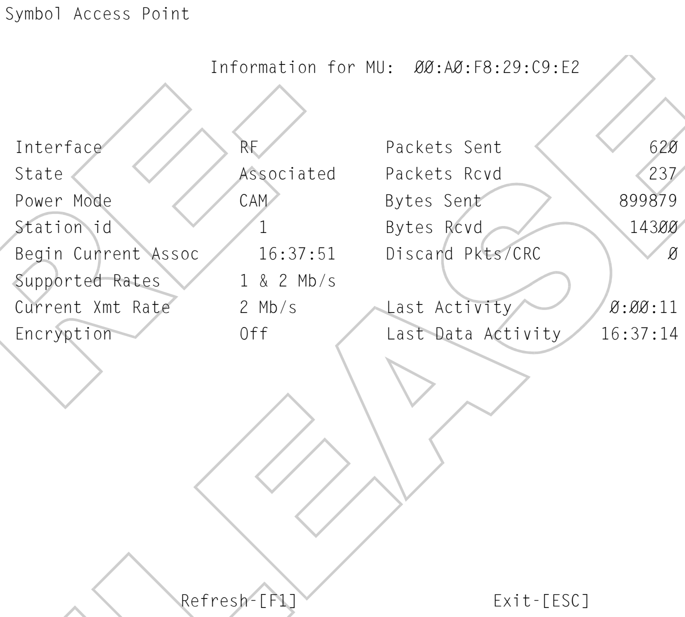
```
addr [p:i#:e]
```

Where:

addr	MU MAC address in xx:xx:xx:xx:xx:xx format
p	MUs power mode: P for PSP, C for CAM. An unassociated MU does not display any character.
i	MU location on AP interfaces. R for radio, P for PPP. MUs with an A were associated with the AP in the past, but no longer associate with it at time of verifying status.
#	AP current Radio transmit rate for the messages sent to this MU: 1 for 1 Mbps, 2 for 2 Mbps.
e	Encryption is enabled for this MU.
V	Indicates a Symbol Voice enabled device.

- To bring up the *WNMP Packet Ping Function* screen, press TAB to highlight the MU and select `Ping`. This allows the AP to ping an MU. See 2.18 Performing Pings on page 68.
  - to have the AP automatically update the display every two seconds select `Timed`
  - to display the next screen select `Next`
  - to return to the previous menu press ESC

- To bring up more detailed information on an MU, press TAB to highlight the MU and select `Information` to display:



```
Symbol Access Point


                         Information for MU:  00:A0:F8:29:C9:E2



 Interface              RF              Packets Sent               620
 State                  Associated      Packets Rcvd               237
 Power Mode             CAM             Bytes Sent              899879
 Station id               1             Bytes Rcvd               14300
 Begin Current Assoc      16:37:51      Discard Pkts/CRC             0
 Supported Rates        1 & 2 Mb/s
 Current Xmt Rate       2 Mb/s          Last Activity          0:00:11
 Encryption             Off             Last Data Activity    16:37:14









                  Refresh-[F1]                     Exit-[ESC]
```

Information displayed includes:

Interface the AP interface shows the MU connection (RF, Ethernet, PPP or AP)

State the connection state between the AP and the MU:

- *Host* indicates the unit is on the AP or PPP interface
- *Associated* indicates current association on the radio interface
- *Away* indicates the unit is no longer associated with the AP.

Power Mode the MU power mode (CAM, PSP or N/A)

Station ID the IEEE 802.11 specification requires that each AP assign a station ID to all associated MUs, regardless of the MU power mode (PSP or CAM)

Begin Current Assoc the time the current association begins in hours, minutes and seconds

Supported Rates data transmission rates the station supports

Current Xmt Rate the current rate the AP transmits data to the station

Encryption MU encryption type supported: *Open* or *Shared*.

Packets Sent the packets sent by the AP to the MU

Packets Rcvd the packets received by the AP from the MU

Bytes Sent the bytes sent by the AP to the MU

Bytes Rcvd the bytes received by the AP from the MU

Discard Pkts/CRC the packets discarded because of data error

Last Activity the time in hours, minutes and seconds since the last communication with the AP

Last Data Activity the time in hours, minutes and seconds since the last data transfer

- To update the values manually, select the `Refresh` command at the status display.
- To return to the previous menu, press ESC.

3.5 Mobile IP

The following tables display the mapping of MUs to mobility agents. See Mobile IP (Roaming Across Routers) on page 23.

- Select *Home Agent* from the *Mobile Units* prompt to display:

```
Symbol Access Point
                            Home Agent Table
   Mobile Unit       Foreign Agent       Mobile Unit       Foreign Agent
 157.235.95.184     157.235.96.141
 157.235.95.111     157.235.97.157
 157.235.95.125     157.235.96.141
 157.235.95.34      157.235.93.245









    Refresh-[F1]        Timed-[F2]        Next-[F3]        Exit-[ESC]
     Select Foreign Agent from the Mobile Units prompt to display:
Symbol Access Point
                            Foreign Agent Table
   Mobile Unit        Home Agent         Mobile Unit        Home Agent
 157.235.95.184     157.235.95.18Ø
 157.235.95.125     157.235.95.18Ø
 157.235.97.114     157.235.97.27







    Refresh-[F1]        Timed-[F2]        Next-[F3]        Exit-[ESC]
```

3.6 Known APs

The AP displays a list of the known APs derived from AP-to-AP communication. The list includes the MAC and IP addresses and configuration information for each AP. The first AP on the list provides the information. The AP recognizes other APs listed in subsequent lines. A broadcast message to APs every 12 seconds determines this list.

Note

The `Save All APs` function from the *Special Functions Menu* updates configures all APs firmware, HTML code shown in the *Known APs* menu.

- Select *Known APs* from the *Main Menu* to display:

```
Symbol Access Point               Known Access Points


                             Net_ID:        101
 MAC Address        IP Address        HST  HSQ  MUS  KBIOS  FW_Ver     Away


 00:A0:F8:78:43:5D  157.235.96.52      1    8    0    0     04.01-13
 00:A0:F8:FF:FF:FF  157.235.99.34      1   16    0    0
 00:A0:F8:10:A7:04  157.235.99.65      1   14    2    5
 00:A0:F8:10:31:66  157.235.99.47      2    6    0    0                  *









                                   X = non-802.11 AP
  Ping-[F1]      Delete-[F2]      Next-[F3]      Previous-[F4]     Exit-[ESC]
```

The AP displays for each known AP:

MAC Address the unique 48-bit, hard-coded Media Access Control address, known as the devices station identifier

IP Address the network-assigned Internet Protocol address

An x after the IP address indicates the AP on this line is not using the 802.11 protocol. Upgrade its firmware.

HST hop set

HSQ AP hopping sequence or pattern

MUS The MUs associated with the AP.

KBIOS The data traffic handled by the AP in kilobytes in and out per second

FW_Ver the firmware version used by the specified AP

Away Determines if the AP is a functional part of the network or *away*. Away indicates the last known transmission took place 12 or more seconds.

3.7 Ethernet Statistics

The AP keeps Ethernet performance statistics including packet transmission and data retries until reset. The display also includes information used only by the Symbol Support Center.

- Select *Ethernet Statistics* from the *Main Menu* to display:

```
Symbol Access Point     Ethernet Statistics

 Packets Seen                 Ø     Packets Sent             138
 Packets Forwarded            Ø     Any Collisions             Ø
   Discarded/NoMatch          Ø     1 + Collisions             Ø
   Discarded/Forced           Ø     Maximum Collisions         Ø
   Discarded/Buffer           Ø     Late Collisions            Ø
   Discarded/CRC              Ø     Defers                     Ø

 Broadcast/Multicast          Ø
 Individual Address           Ø



         Refresh-[F1]       Timed-[F2]          Exit-[ESC]
```

Packet display for Ethernet statistical units:

Packets Seen packets received on Ethernet interface

Packets Forwarded packets forwarded from Ethernet interface to other interfaces

Discarded/NoMatch packets discarded because of unknown destinations (destinations not in the known list of database entries)

Discarded/Forced packets discarded because of the applied address filters

Discarded/Buffer packets discarded because insufficient buffers in AP

Discarded/CRC packets discarded because of data errors

Broadcast/Multicast total broadcast or multicast packets received

Individual Address packets received with designated individual addresses

Packets Sent total packets sent out

Any Collision packets affected by at least one collision

1 + Collisions	packets affected by more than one collision
Maximum Collisions	packets affected by the maximum number of collision
Late Collisions	collisions occurring after the first 64 bytes
Defers	the times the AP had to defer transmit requests on the Ethernet because of a busy medium

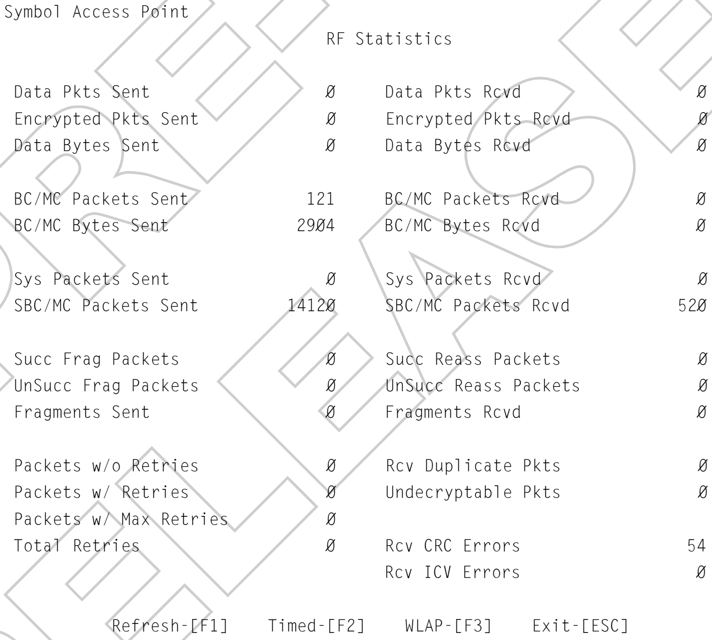
- To update the values manually at the status display select `Refresh`.
- To have the AP automatically update the display every two seconds select `Timed`.
- To return to the previous menu press ESC.

3.8 Radio Statistics

The AP keeps radio performance statistics including packet and communication information.

To view RF statistics:

- Select *Show RF Statistics* from the *Main Menu* to display:



```
Symbol Access Point
                                 RF Statistics

 Data Pkts Sent                  0     Data Pkts Rcvd                  0
 Encrypted Pkts Sent             0     Encrypted Pkts Rcvd             0
 Data Bytes Sent                 0     Data Bytes Rcvd                 0

 BC/MC Packets Sent            121     BC/MC Packets Rcvd              0
 BC/MC Bytes Sent             2904     BC/MC Bytes Rcvd                0

 Sys Packets Sent                0     Sys Packets Rcvd                0
 SBC/MC Packets Sent         14120     SBC/MC Packets Rcvd           520

 Succ Frag Packets               0     Succ Reass Packets              0
 UnSucc Frag Packets             0     UnSucc Reass Packets            0
 Fragments Sent                  0     Fragments Rcvd                  0

 Packets w/o Retries             0     Rcv Duplicate Pkts              0
 Packets w/ Retries              0     Undecryptable Pkts              0
 Packets w/ Max Retries          0
 Total Retries                   0     Rcv CRC Errors                 54
                                       Rcv ICV Errors                  0

           Refresh-[F1]    Timed-[F2]    WLAP-[F3]    Exit-[ESC]
```

Radio performance statistics include:

Data Packets Sent	total data packets transmitted
Encrypted Pkts Sent	total encrypted packets transmitted
Data Bytes Sent	total data packets transmitted in bytes
BC/MC Packets Sent	broadcast/multicast user data packets successfully transmitted
BC/MC Bytes Sent	broadcast/multicast user data bytes successfully transmitted
Sys Packets Sent	system packets successfully transmitted
SBC/MC Packets Sent	broadcast/multicast system packets successfully transmitted
Succ Frag Packets	fragmented packets successfully transmitted
Unsucc Frag Packets	fragmented packets unsuccessfully transmitted
Fragments Sent	packet fragments transmitted
Packets w/o Retries	transmitted packets not affected by retries
Packets w/ Retries	transmitted packets affected by retries
Packets w/ Max Retries	transmitted packets affected by the maximum limit of retries
Total Retries	Retries occurring on the interface. A retry occurs if the device fails to receive an *acknowledgment (ACK)* from a destination.
Data Packets Rcvd	total data packets received
Encrypted Pkts Rcvd	total encrypted packets received
Data Bytes Rcvd	total data packets received in bytes
BC/MC Packets Rcvd	broadcast/multicast user data packets successfully received
BC/MC Bytes Rcvd	broadcast/multicast user data bytes successfully received
Sys Packets Rcvd	system packets successfully received
SBC/MC Packets Rcvd	broadcast/multicast system packets successfully received

Succ Reass Packets	packets successfully reassembled
Unsucc Reass Packets	packets unsuccessfully reassembled
Fragments Rcvd	packet fragments received
Rcv Duplicate Pkts	Duplicate packets received by the AP. This indicates the AP sent an ACK, but the MU did not receive it and transmitted the packet again.
Undecryptable Pkts	total data packets that could not be decrypted
Rcv CRC Errors	Packets received that contained *CRC (Cyclic Redundancy Check)* errors. An MU transmitted a corrupt data packet and failed to pass the CRC verification. Ensure that any acknowledgment of the data packet contains the correct CRC word. An incorrect CRC causes the AP to discard the data packet.
Rcv ICV Errors	Packets received containing *ICV (Identity Check Value)* errors. An MU transmitted a corrupt data packet and failed to pass the ICV verification. The calculated ICV value does not match with the ICV value in the received packet.

– To update the values manually at the status display select `Refresh`.

– To have the AP automatically update the display every two seconds select `Timed`.

– To return to the previous menu press ESC.

- To display the *WLAP RF Statistics* screen select `WLAP-[F3]`.

```
Symbol Access Point            WLAP RF Statistics

 Current # WLAP  Itf   0                Root Interface       0
 Current # INTLR Itf   0                Root Priority     8000 hex
 Current State    Functional            Root MAC Addr     00:A0:F8:73:51:F2
 Priority         8000 hex              Root Path Cost       0



         ------------  Wireless AP Interface Table  --------------

 Itf      WLAP Itf      Itf   Path         Designated             Designated
 ID       MAC Addr     State  Cost    Root ID      Cost       WLAP ID      Itf ID

8001 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   8001
8002 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   8002
8003 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   8003
8004 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   8004


     Refresh-[F1]   Timed-[F2]   INTLR-[F3]   Previous-[F4]   Exit-[ESC]
```

Where:

Current # WLAP Itf refers to the current Wireless AP interfaces in use in a 1-4 range

Current # INTLR Itf refers to the current International Roaming Access Bridge interfaces in use in a 1-10 range

Current State on initialization, the AP can be in any of the following states of wireless operation:

- starting the initializing process:
  - Initializing
  - Sending Probe
  - *Send Assoc Req* (association request)
  - *Send Cfg BPDU (configuration Bridge Protocol Data Unit)*
  - Wait for Probe
  - *Send Probe Rsp* (probe response)
  - *Send Assoc Rsp* (association response)
  - *Send Cfg Rsp* (configuration response)
  - *Received Root Rsp* (Root response)
- operating in wireless mode:
  - Root WLAP lost
  - Disabled
  - Functional

The 1.2.2 Quick Wireless AP Setup on page 7 provides an explanation of a Root AP.

Priority states the WLAP priority value assigned to the AP under *2.5 Configuring Radio Parameters* on page 40

Root Interface states the interface leading to the Root AP

Root Priority states the priority value of the Root AP

Root MAC Address states the MAC address of the Root AP

Root Path Cost indicates the hops between the current WLAP and the Root AP

Itf ID identifies the wireless interface the AP uses to communicate with another device

WLAP Itf MAC Addr states the MAC address of the associated WLAP

Itf State identifies the state of the interface from:

- *DIS* - the interface is disabled
- *LIS* - the AP listens for information
- *LRN* - the AP learns the information
- *FWD* - the AP forwards data
- *BLK* - the AP blocks transmission.

Path Cost An abstract unit added to the *Root Path Cost* field in the *Config BPDU* received on this interface. The unit represents a hop on the path to the Root AP.

Designated Root ID An ID designated by the Root AP. APs in WLAP mode negotiate the position of Root AP at power up. The AP with the lowest Root ID, path and WLAP ID becomes the Root AP. The Root ID and the WLAP ID are 16-digit numbers. The first 4 digits represent the Priority value and the remaining 12 digits represent the MAC address of the AP.

Designated Cost a path cost designated by the Root AP

Designated WLAP ID a WLAP ID assigned by the Root AP

Designated Itf ID an Itf ID assigned by the Root AP

– To update the values manually at the status display select `Refresh`.

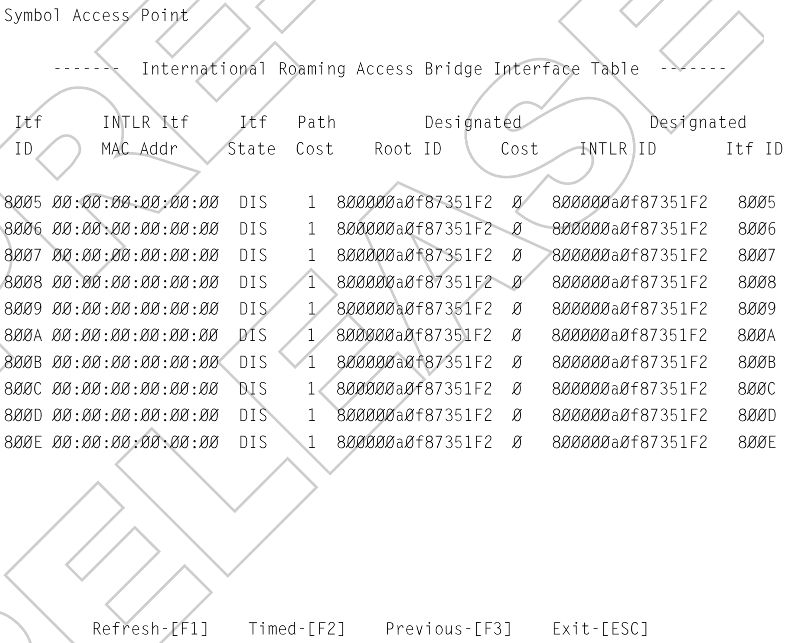
– To have the AP automatically update the display every two seconds select `Timed`.

– To return to the previous menu press ESC or `Previous-[F4]`.

- To display the *International Roaming Access Bridge Interface Table* select `INTLR-[F3]`.

Note

This screen is for future applications in development. For more information, contact a Symbol Representative.



```
Symbol Access Point

     -------  International Roaming Access Bridge Interface Table  -------

  Itf      INTLR Itf      Itf   Path         Designated              Designated
  ID       MAC Addr      State  Cost    Root ID       Cost    INTLR ID        Itf ID

8005 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   8005
8006 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   8006
8007 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   8007
8008 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   8008
8009 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   8009
800A 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   800A
800B 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   800B
800C 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   800C
800D 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   800D
800E 00:00:00:00:00:00  DIS    1  800000a0f87351F2  0   800000a0f87351F2   800E




        Refresh-[F1]    Timed-[F2]    Previous-[F3]    Exit-[ESC]
```

Itf ID identifies the wireless interface the AP uses to communicate with another device

INTLR Itf MAC Addr states the MAC address of the associated International Roaming Access Bridge

Itf State identifies the state of the interface from:

- *DIS* - the interface is disabled
- *LIS* - the AP listens for information
- *LRN* - the AP learns the information
- *FWD* - the AP forwards data
- *BLK* - the AP blocks transmission.

Path Cost An abstract unit added to the *Root Path Cost* field in the *Config BPDU* received on this interface. The unit represents a hop on the path to the Root AP.

Designated Root ID An ID designated by the Root AP. APs in International mode negotiate the position of Root AP at power up. The AP with the lowest Root ID, path and WLAP ID becomes the Root AP. The Root ID and the WLAP ID are 16-digit numbers. The first 4 digits represent the Priority value and the remaining 12 digits represent the MAC address of the AP.

Designated Cost a path cost designated by the Root AP

Designated INTLR ID An International Roaming Access Bridge ID assigned by the Root AP

Designated Itf ID an Itf ID assigned by the Root AP

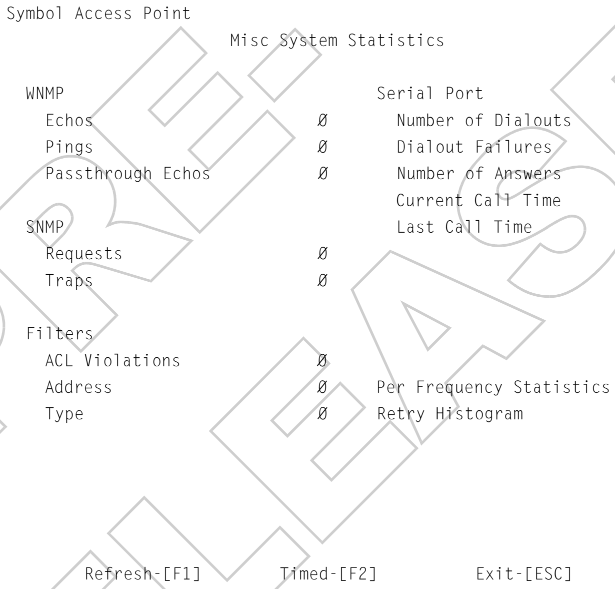
The AP can have up to ten Access Bridges associated in addition to four associated WLAPs.

- To update the values manually at the status display select `Refresh`.
- To have the AP automatically update the display every two seconds select `Timed`.
- To return to the previous menu press ESC or `Previous-[F4]`.

3.9 Miscellaneous Statistics

The AP keeps statistics on WNMP and SNMP packets, filtering violations and serial port use. The *Miscellaneous Statistics* screen shows grouped statistics.

- Select *Show Misc Statistics* from the *Main Menu* to display:



```
Symbol Access Point
                       Misc System Statistics

  WNMP                                Serial Port
    Echos                       Ø       Number of Dialouts         Ø
    Pings                       Ø       Dialout Failures           Ø
    Passthrough Echos           Ø       Number of Answers          Ø
                                        Current Call Time          Ø
  SNMP                                  Last Call Time             Ø
    Requests                    Ø
    Traps                       Ø

  Filters
    ACL Violations              Ø
    Address                     Ø     Per Frequency Statistics
    Type                        Ø     Retry Histogram




        Refresh-[F1]        Timed-[F2]          Exit-[ESC]
```

WNMP statistics are:

Echoes	echo requests received by the AP
Pings	ping requests received by the AP
Passthrough Echoes	echoes for MUs associated with the AP

SNMP statistics are:

Requests	configuration requests received from the SNMP manager
Traps	AP messages sent to the SNMP manager

Filter statistics are:

ACL Violations	attempts by MU, not in ACL list to associate with this AP
Address	packets discarded by address filter
Type	packets discarded by type filter

Modem statistics for the serial port are:

Number of Dialouts	dialout attempts by the AP
Dialout Failures	dialout failures by the AP
Number of Answers	answer attempts by the AP
Current Call Time	current connection session length in seconds
Last Call Time	last connection session length in seconds

- To update the values manually at the status display select `Refresh`.
- To have the AP automatically update the display every two seconds select `Timed`.
- To return to the previous menu press ESC.

3.9.1 Analyzing Frequency Use

The AP keeps statistics for individual frequencies (channels). These identify channels that have difficulty transmitting or receiving due to retries.

To view statistics for individual frequencies:

1. Select *Show Misc Statistics* from the *Main Menu*.
2. Select Per *Frequency Statistics* to display:

```
Chnnl     Sent     Rcvd    Retry      Chnnl     Sent     Rcvd    Retry
=====     ====     ====    =====      =====     ====     ====    =====
  2:      591      925       1          3:      591      270       0
  4:      586      153       0          5:      577      128       5
  6:      590      114       0          7:      594      360       1
  8:      587      247       2          9:      581      127       0
 10:      589      232       0         11:      591      145       0
 12:      600      176       1         13:      605      253       1
 14:      593      246       0         15:      599      169       0
 16:      583      219       0         17:      593      218       2
 18:      579      185       0         19:      586      305       0
 20:      587      142       0         21:      592      140       0
 22:      587      231       0         23:      593      167       0
 24:      594      126       0         25:      585      206       0
 26:      594      243       0         27:      599      161       1
 28:      592      242       1         29:      588      245       0
 30:      596      121       0         31:      582      265       0
 32:      588      134       3         33:      578      134       0
 34:      582      170       0         35:      586      146       0
 36:      594      176       0         37:      582      143       0
 38:      590      206       0         39:      584      130       1
 40:      582      200       2         41:      598      212       0
 42:      597      130       1         43:      591      224       1
                              Press any key to continue
```

The display shows counters for the packets sent, received and retries for each channel.

3. Press any key to continue.

Note

The AP displays a maximum of 79 channels.

3.9.2 Analyzing Retries

The AP keeps statistics of packets with multiple retries. Use these statistics to identify severe occurrences of retries. Retries occur when the transmitting station fails to receive an acknowledgment for a transmitted packet. This lack of acknowledgment can result from:

- two or more stations transmitting simultaneously and causing collisions
- the receiving station moving out of range
- the receiving station being powered off.

Any one of these results causes both devices to backoff and retry later at random times. Too many retries can indicate a system problem.

To view retry severity:

1. Select *Show Misc Statistics* from the *Main Menu*.
2. Select *Retry Histogram* to display:

```
Retries     Packets
=======     =======
      0       65795
      1         320
      2         112
      3          86
      4          21
      5          12
      6           8
      7           3
      8           0
      9           0
     10           1
     11           0
     12           0
     13           0
     14           0
     15           0
```

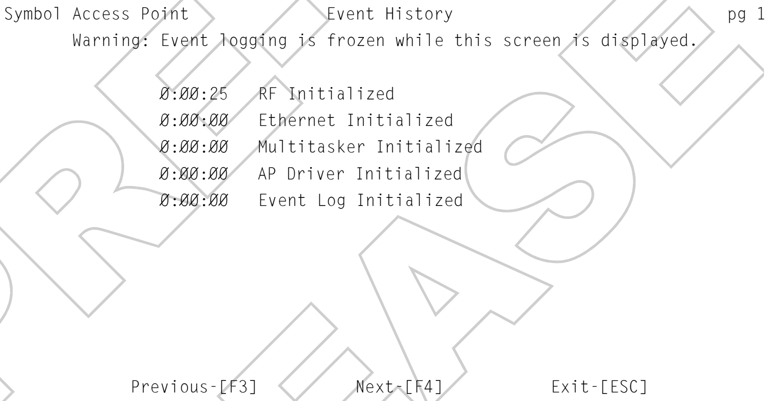
The display indicates the packets that experience retries (up to 15 retries).

3. Press any key to return to the *Main Menu*.

3.10 Event History

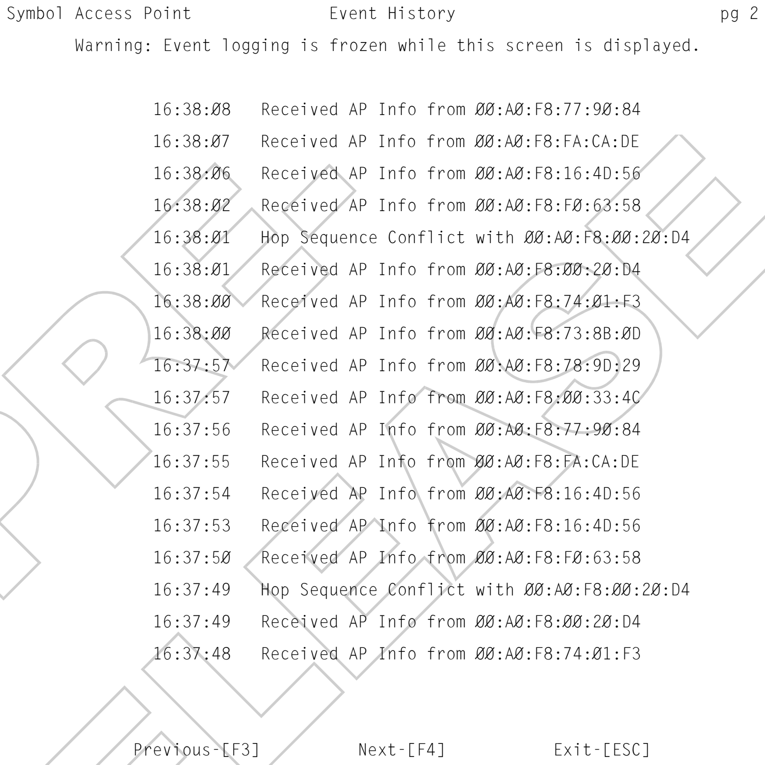
The AP also tracks the occurrence of specific events. The types of events logged are configurable. The log is a 128-entry circular buffer. After the 128th entry, the earliest event entry deletes.

- Select *Show Event History* from the *Main Menu* to display:



```
Symbol Access Point            Event History                         pg 1
       Warning: Event logging is frozen while this screen is displayed.

                0:00:25   RF Initialized
                0:00:00   Ethernet Initialized
                0:00:00   Multitasker Initialized
                0:00:00   AP Driver Initialized
                0:00:00   Event Log Initialized







             Previous-[F3]        Next-[F4]          Exit-[ESC]
```

The *Event History* displays the most recent event at the top of the list. Each event lists a time stamp recorded in hh:mm:ss from the time the AP powered up or reset. The type of event logged follows the time stamp. If the event involves an MU or AP, the unit MAC address displays.



```
Symbol Access Point              Event History                         pg 2
       Warning: Event logging is frozen while this screen is displayed.

               16:38:08   Received AP Info from 00:A0:F8:77:90:84
               16:38:07   Received AP Info from 00:A0:F8:FA:CA:DE
               16:38:06   Received AP Info from 00:A0:F8:16:4D:56
               16:38:02   Received AP Info from 00:A0:F8:F0:63:58
               16:38:01   Hop Sequence Conflict with 00:A0:F8:00:20:D4
               16:38:01   Received AP Info from 00:A0:F8:00:20:D4
               16:38:00   Received AP Info from 00:A0:F8:74:01:F3
               16:38:00   Received AP Info from 00:A0:F8:73:8B:0D
               16:37:57   Received AP Info from 00:A0:F8:78:9D:29
               16:37:57   Received AP Info from 00:A0:F8:00:33:4C
               16:37:56   Received AP Info from 00:A0:F8:77:90:84
               16:37:55   Received AP Info from 00:A0:F8:FA:CA:DE
               16:37:54   Received AP Info from 00:A0:F8:16:4D:56
               16:37:53   Received AP Info from 00:A0:F8:16:4D:56
               16:37:50   Received AP Info from 00:A0:F8:F0:63:58
               16:37:49   Hop Sequence Conflict with 00:A0:F8:00:20:D4
               16:37:49   Received AP Info from 00:A0:F8:00:20:D4
               16:37:48   Received AP Info from 00:A0:F8:74:01:F3


             Previous-[F3]          Next-[F4]          Exit-[ESC]
```

3.11 Clearing Statistics

To clear statistics:

1. Select *Special Functions* from the *Main Menu*.
2. Select *Clear All Statistics*. The AP zeroes all statistics.

Note

Resetting the AP also clears statistics.

Chapter 4 Hardware Installation

AP installation includes connecting the AP to the wired network, attaching antennas, AP placement and power up. Installation procedures vary for different environments.

4.1 Precautions

Before installing the AP verify the following:

- The location for the unit is dry and dust free. Do not install in wet or dusty areas without additional protection. Contact a Symbol representative for more information.
- Verify the environment has a temperature range between -20° C to 55° C.
- If attaching to a wired Ethernet, keep AP on the same subnet.

4.2 Package Contents

Check package contents for:

- AP
- power adapter
- antenna

Note

If an item is missing or not functioning properly contact Symbol Support Center.

Verify the AP model indicated on the bottom of the unit and packaging.

4.3 Requirements

The minimum installation requirements for a single-cell, peer-to-peer network are:

- a power outlet
- an antenna

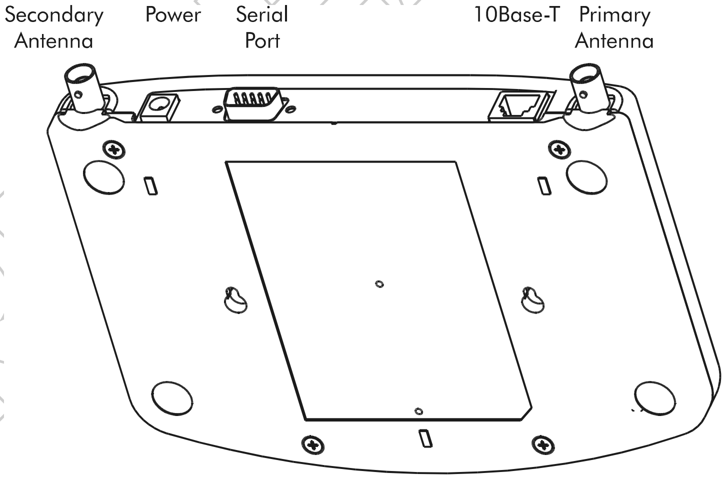
The AP supports a 10Base-T *unshielded twisted pair (UTP)* standard. Users can order a null-modem cable, part number 61383-00-0, for direct serial connections by contacting a Symbol sales representative.

Note

Test and use the radio network with an MU.

4.3.1 Network Connection

Locate connectors for Ethernet, antennas and power on the back of the AP.



Ethernet configurations vary according to the environment. Determine the Ethernet wiring to connect the AP, 10Base-T UTP or single cell.

Note

The site survey determines the APs to install and their location.

4.3.2 10Base-T UTP

Use a 10Base-T connection for multiple APs or an AP attached to a wired UTP Ethernet hub. Normal 10Base-T limitations apply.

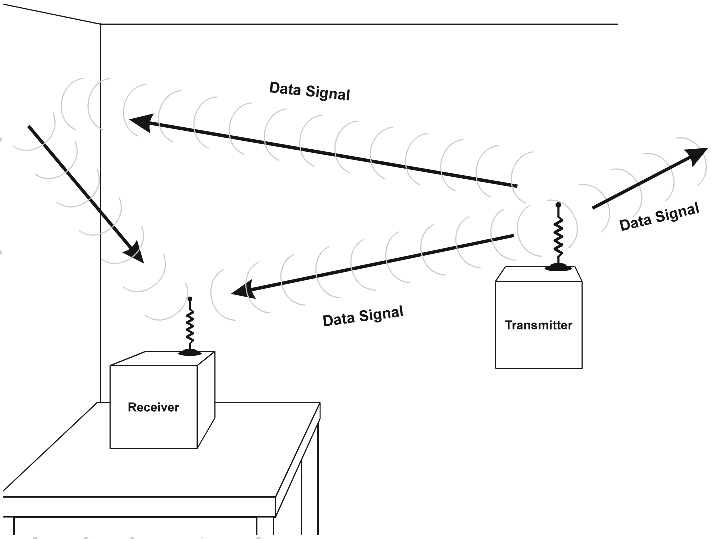
1. Plug the data cable RJ-45 connector into the AP RJ-45 connector.
2. Plug the other end of the data cable into the LAN access port (possibly a hub or wall connection).
3. Add additional APs as needed.

4.3.3 Single Cell

The single-cell connection option allows a single AP to bridge MUs without a wired network. MUs appear as peers as in any Ethernet environment.

4.4 Attaching the Antenna(s)

Antenna coverage resembles lighting in that an area lit from far away might not be bright enough. An area lit sharply minimizes coverage and creates *dark areas* where no light exists. Even antenna placement in an area (like an even placement of light bulbs) provides even, efficient coverage.



Place the antenna using the following guidelines:

- Install the antenna as high as practical
- Orient the antenna vertically for best reception
- Point the antenna downward if attaching the antenna to the ceiling.

The AP requires one antenna and can use two. Two antennas provide diversity that can improve performance and signal reception.

1. Attach antennas to ANTENNA connectors on the back of the AP. For a single antenna, use the PRIMARY ANTENNA connector.
2. Refer to antenna documentation for mounting.

The standard antenna works for most office environments. Obtain additional or higher performance antennas from Symbol. Contact a Symbol sales representative to order the following models:

standard rubber antenna	ML 2499-APA1-00
single high performance antenna	ML 2499-HPA1-00
twin high performance diversity antennas	ML 2499-DVA1-00
mountable F-plane antenna	ML 2499-PSA1-00

Symbol continues to add antenna options for Spectrum24 devices. Contact a Symbol sales representative for available antenna options.

If installing two antennas, enable the Antenna Selection in the *User Interface*. See 2.3 Access Point Installation on page 37.

4.4.1 Antenna Extension Cables

Symbol offers extension cables for AP antennas. Some range loss occurs when increasing the distance between the antenna and the AP.

Model	Length	Loss	Range Loss
25-19371-01	6 ft	2.0 db	5%
25-19371-02	12 ft	4.0 db	10%

To order extension cables contact a Symbol representative.

4.5 Power Options

- Standard power supply Part Number: 50-24000-006 115/230VAC, 50/60Hz.
  - US line cord Part Number: 23844-00-00
- Remote power distribution system, Part Number: AP-PS-11
  - Refer to application note AP-PS-01 located on the Symbol Technologies web page.

4.6 Mounting the AP

The AP rests on a flat surface or attaches to a wall, or any hard, flat, stable surface. Position the AP at any angle. Use the standard-mounting kit provided.

Users can obtain a *universal wall-mounting bracket* (ML-2499-APB1-00) and *an AP-3020 adapter bracket* (12-20436-01) from Symbol for attaching the AP and antennas to the wall or ceiling. Contact a Symbol sales representative to order.

Choose one of the options based on environment

Resting flat	Rests on the four rubber pads on the underside of the AP. Place on a surface clear of debris and away from traffic.
Attaching on the wall	Rests on screws. Orient the AP in a downward position on the wall so the LEDs face the floor.

4.7 Connecting the Power Adapter

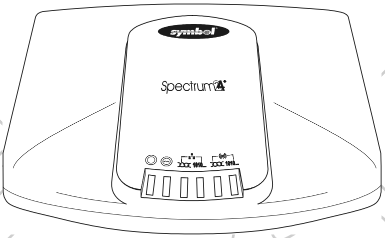
The power adapter connects to the rear of the AP and to a power outlet.

1. Verify the power adapter is correct according to the country.
2. Plug the power adapter cable into the socket at the back of the AP.
3. Plug the adapter into an outlet. The AP is functional when the Status indicator on the front of the AP reaches a consistent flashing and *the Wireless LAN Activity* indicator begins flickering. This indicates that the AP is ready for MUs to associate with it.

The AP works without user intervention after setup. See the AP LED indicators to verify that the unit operates properly.

4.8 LED Indicators

The top panel LED indicators provide a status display indicating transmission, error condition, and other activity. The indicators are:



○	*Status*	One flash per second indicates normal operation. A steady on or off, or irregular flashing indicates a fault condition.
⊖	*Serial*	Flashing indicates serial port activity.
	Wired LAN Attached	On indicates a valid Ethernet connection for a 10BaseT connection.
1010...	*Wired LAN In Use*	Flashing indicates data transfers on wired connection.
((·))	*Wireless LAN Attached*	On indicates an MU is associated with the AP.
((·)) 1010...	*Wireless LAN In Use*	Flickering indicates beacons and data transfers with MUs.

4.8.1 WLAP mode LED display.

When in the WLAP mode this chart signifies the APs LED indicator status. For the IEEE 802.11 protocol and APs using firmware version 4.00-20 or above only.

1. After power up, system initialization begins:

LED	**State**
Status	Blinks
Serial	Blinks if activity occurs.
Wired LAN Attached	on if Ethernet cable attached
Wired LAN Activity	Blinks if activity occurs
Wireless LAN Attached	Off
Wireless LAN Activity	Off

2. When a WLAP begins a full scan:

LED	**State**
Status	On
Serial	Off
Wired LAN Attached	Off
Wired LAN Activity	Off
Wireless LAN Attached	Blinks slowly
Wireless LAN Activity	Blinks slowly

3. When one or more WLAPs are found, but still in full scan state:

LED	**State**
Status	On
Serial	Off
Wired LAN Attached	Off
Wired LAN Activity	Off
Wireless LAN Attached	Blinks slowly
Wireless LAN Activity	Off

4. When the WLAP is in functional state, but one or more WLAP connections are not in Forward state:

LED	State
Status	blinks regularly
Serial	blinks if activity occurs
Wired LAN Attached	on if Ethernet cable attached
Wired LAN Activity	blinks if activity occurs
Wireless LAN Attached	blinks slowly
Wireless LAN Activity	blinks if activity occurs

5. When all WLAP connections are in Forward state:

LED	State
Status	blinks regularly
Serial	blinks if activity occurs
Wired LAN Attached	on if Ethernet cable attached
Wired LAN Activity	blinks if activity occurs
Wireless LAN Attached	on
Wireless LAN Activity	blinks if activity occurs

Special cases:

- If the WLAP manual BSS_ID is NOT set and no other WLAP is found the WLAP goes to the functional state.
- If the WLAP manual BSS_ID is set and the specified WLAP not found, the WLAP remains in FULL Scan state permanently. The LEDs have the following indicator status permanently:

LED	State
Status	on
Serial	off
Wired LAN Attached	off
Wired LAN Activity	off
Wireless LAN Attached	blinks slowly
Wireless LAN Activity	blinks slowly

- If the WLAP manual BSS_ID is set with the broadcast bit ON (i.e.: the first Byte is 01) and the specified WLAP not found, the WLAP tries to associate with another WLAP. If it still cannot find another WLAP, it goes to Functional State.
- If the RF interface is disabled the LED indicator status displays:

LED	State
Status	on
Serial	off
Wired LAN Attached	blinks slowly
Wired LAN Activity	blinks slowly
Wireless LAN Attached	off
Wireless LAN Activity	off

4.9 Troubleshooting

Check the following symptoms and their possible causes before contacting the Symbol Support Center.

4.9.1 Ensure wired network is operating.

Verify AP operation:

1. AP does not power up:
   - faulty AP power supply
   - failed AC supply
   - *Electrical Management System (EMS)* operating outlet.
2. After the AP resets and hardware is initialized, it performs an SRAM test. If the test passes, all six LEDs turn on. If the test fails, the LEDs all turn off and the AP resets. The LEDs turn off sequentially, in the order shown, as each of the following tests pass.

LED	State	Test Passed
Wireless LAN Activity	Off	Serial port initialized, flush FIFO buffer, serial port to AP connection checked.

Wireless LAN Attached	Off	Exit the AP manufacturing environment.
Wired LAN Activity	Off	LAN adapter present.
Wired LAN Attached	Off	Valid manufacturing configuration exists.
Serial	Off	Valid runtime code exists.
Status	Blinks continuously	Bootup and runtime codes downloaded to AP flash memory successful. Runtime code controls the AP.

Identify wired network problems:

3. No operation:
   - Verify AP configuration via Telnet, PPP or UI. Review procedures for Ethernet and serial connection of the AP. Review AP firmware revisions and update procedures.
   - Verify network configuration by ensuring that there are no duplicate IP addresses. Power down the device in question and ping the assigned address of the device. Ensure no other device responds to that address.
4. AP powered on but has no connection to the wired network:
   - Check connections for proper wiring.
5. Verify network wiring and topology for proper configuration:
   - Check that the cables used have proper pinouts and connectors.
   - Verify router configuration and filtration setting.
   - Check that network band use does not exceed 37% of bandwidth.
   - Verify MU operations.
   - Confirm AP operation.
   - Confirm AP and MU Net_ID (ESSID).
   - Check that the radio driver loaded properly.
   - Check that the MU PROTOCOL.INI or NET.CFG file is compatible with the network operating system.

6. Slow or erratic performance:
   - Check MU and RF communications range.
   - Check antenna, connectors and cabling.
   - Verify the AP is using the primary antenna connection for single antenna use.
   - Verify that antenna diversity setting for AP is appropriate. If using one antenna, the setting is `Primary Only`, if using two antennas, the setting is `Primary and Secondary`.
   - Verify network traffic does not exceed 37% of bandwidth.
   - Check to see that the wired network does not exceed 10 broadcast messages per second.
   - Verify wired network topology and configuration.

4.10 Setting Up MUs

Refer to MU documentation for installing drivers, client software and testing. Use the default values for the Net_ID (ESSID) and other configuration parameters until network connection verification.

MUs attach to the network and interact with the AP transparently.

Appendix A
Specifications

A.1 Physical Characteristics

Dimensions	1.25″ H x 5.5″ L x 7.75″ W (3.18 cm H x 14.97 cm L x 19.69 cm W)
Weight (w/power supply)	1 lbs. (0.454 kg)
Operating Temperature	-4° F to 131° F (-20° C to 55° C)
Storage Temperature	-40° F to 149° F (-40° C to 65° C)
Humidity	10% to 95% noncondensing
Shock	40 G, 11 ms, half-sine
ESD	meets CE-Mark
Drop	withstands up to a 30 in. (76 cm) drop to concrete with possible surface marring

A.2 Radio Characteristics

Frequency Range	country dependant; within 2400 MHz to 2500 MHz	
Frequency Hopping	Hops	79 Standard 35 in France 27 in Spain 23 in Japan 20 in Belgium (outdoor) 29 in Mexico
	Hop Rate	configurable
	Hop Sequences	78 (per IEEE 802.11 standard)
Radio Data Rate	1 and 2 Mbps per channel	
Radio Power Output	100mW and 500mW versions	
1Mbps Range	open environment - over 1000 ft. (303 m) typical office or retail environment - between 180 and within 250 ft. (54.5 to 75.7 m)	
2 Mbps Range	open environment - 500 ft. (152 m) typical office or retail environment - between 125 and within 175 ft. (38 to 53 m)	
TX Max. Radiated EIRP	US: FCC part 15.247 Europe: ETS 300 320 Japan: RCR STD-33	
Modulation	Binary GFSK	
TX Out-of-Band Emissions	US: FCC part 15.247, 15.205, 15.209 Europe: ETS 300 320 Japan: RCR STD-33	

A.3 Network Characteristics

Driver Support	ODI v1.6, NDIS v2.01
Ethernet Frame	DIX, Ethernet_II and IEEE 802.3
Filtering Packet Rate	14,400 frames per second filtering and forwarding
Ethernet Connection	10Base-T (RJ-45)
Serial	PC/AT serial port - DB9 Female, RS-232 using a DTE termination, 19200 bps
SNMP	Version 1, MIB-II and Symbol MIB

Appendix B
Supported Modems

The AP supports modems that use the generic Hayes Smartmodem command set.

The AP uses Hayes commands and is capable of working with various modems of 19200 baud or faster.

Symbol does not support modems the company has not qualified.

The following modems qualify to work with the AP:

- Practical Peripherals PM288MT II V.34
- Supra Fax Modem 288
- USRobotics Sportster Modem 28.8

Appendix C
Customer Support

Symbol Technologies provides its customers with prompt and accurate customer support. Use the Symbol Support Center as the primary contact for any technical problem, question or support issue involving Symbol products.

If the Symbol Customer Support specialists cannot solve a problem, access to all technical disciplines within Symbol becomes available for further assistance and support. Symbol Customer Support responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements.

When contacting Symbol Customer Support, please provide the following information:

- serial number of unit
- model number or product name
- software type and version number.

North American Contacts

Inside North America, contact Symbol by:

- Symbol Technologies, Inc.
  One Symbol Plaza
  Holtsville, New York 11742-1300
  Telephone: 1-516-738-2400/1-800-SCAN 234
  Fax: 1-516-738-5990
- Symbol Support Center:
  - telephone: 1-800-653-5350
  - fax: (516) 563-5410
  - Email: support@symbol.com

International Contacts

Outside North America, contact Symbol by:

- Symbol Technologies Technical Support
  12 Oaklands Park
  Berkshire, RG41 2FD, United Kingdom
  Tel: 011-44-118-945-7000 or 1-516-738-2400
  ext. 6213

Additional Information

Obtain additional information by contacting Symbol at:

- 1-800-722-6234, inside North America
- +1-516-738-5200, in/outside North America
- http://www.symbol.com/

Appendix D

Regulatory Compliance

To comply with U.S. and international regulatory requirements, the following information has been included. The document applies to the complete line of Symbol products. Some of the labels shown, and statements applicable to other devices might not apply to all products.

Radio Frequency Interference Requirements

This device has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the Federal Communications Commissions Rules and Regulation. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Radio Frequency Interference Requirements - Canada

This Class A digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

CE Marking & European Union Compliance

Products intended for sale within the European Union are marked with the CEMark which indicates compliance to applicable Directives and European Normes (EN), as follows. Amendments to these Directives or ENs are included: Normes (EN), as follows.

Applicable Directives:

- Electromagnetic Compatibility Directive 89/336/EEC
- Low Voltage Directive 73/23/EEC

Applicable Standards:

- EN 55 022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information technology Equipment
- EN 50 082-1 - Electromagnetic Compatibility - Generic Immunity Standard, Part 1: Residential, commercial, Light Industry
- IEC 801.2 - Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment Part 2: Electrostatic Discharge Requirements
- IEC 801.3 - Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment Part 3: Radiated Electromagnetic Field Requirements
- IEC 801.4 - Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment Part 4: Electrical Fast Transients Requirements
- EN 60 950 + Amd 1 + Amd 2 - Safety of Information Technology Equipment Including Electrical Business Equipment
- EN 60 825-1 (EN 60 825) - Safety of Devices Containing Lasers

RF Devices

Symbol's RF products are designed to be compliant with the rules and regulations in the locations into which they are sold and will be labeled as required. The majority of Symbol's RF devices are type approved and do not require the user to obtain license or authorization before using the equipment. Any changes or modifications to Symbol Technologies equipment not expressly approved by Symbol Technologies could void the user's authority to operate the equipment.

Telephone Devices (Modems)

United States

If this product contains an internal modem it is compliant with Part 68 of the Federal Communications Commission Rules and Regulations and there will be a label on the product showing the FCC ID Number and the REN, Ringer Equivalence Number.   The REN is used to determine the quantity of devices which maybe connected to the telephone line. Excessive RENs on the telephone line may result in the device not ringing in response to an incoming call. In most but not all areas, the sum of the RENs should not exceed 5.0. To be certain of the number of devices that may be connected to the line, as determined by the total number of RENs, contact the telephone company to determine the maximum REN for the calling area.

If the modem causes harm to the telephone network, the telephone company will notify you in advance; however, if advance notice is not practical, you will be notified as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the modem. If this happens the telephone company will provide advance notice so you may make any necessary modifications to maintain uninterrupted service.

Canada

If this product contains an internal modem it is compliant with CS-03 of Industry Canada and there will be a Canadian certification number (CANADA: _____) on a label on the outside of the product. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single-line, individual service maybe extended by means of a certified convector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

User should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

User should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to the telephone loop which is used by the device, to prevent overloading. The termination of a loop may consist of any combination of devices, subject only to the requirement that the total of the Load Numbers of all devices not exceed 100.

The Load Number is located on a label on the product.

Contact your local Symbol Technologies, Inc., representative for service and support;

Symbol Technologies, Inc.,
Canadian Sales and Service
2540 Matheson Boulevard East
Mississauga, Ontario
Canada L4W 4Z2
Phone - 905 629 7226

Laser Devices

Symbol products using lasers comply with US 21CFR1040.10, Subchapter J and IEC825/EN 60 825 (or IEC825-1/EN 60 825-1, depending on the date of manufacture). The laser classification is marked one of the labels on the product.

Class 1 Laser devices are not considered to be hazardous when used for their intended purpose. The following statement is required to comply with US and international regulations:

Caution

Use of controls, adjustments or performance of procedures other than those specified herein may result in hazardous visible or invisible laser light exposure.

Class 2 laser scanners use a low power, visible light diode. As with any very bright light source, such as the sun, the user should avoid staring directly into the light beam. Momentary exposure to a Class 2 laser is not known to be harmful.

Laser information labels are found in the product Quick Reference Guide.