

# Spectrum24 AP-4121HR Access Point

## Product Reference Guide

70E-20688-03  
Revision A  
June 2000

---

# Copyright

Copyright © 2000 by Symbol Technologies, Inc. All rights reserved.

No part of this publication may be modified or adapted in any way, for any purposes without permission in writing from Symbol. The material in this manual is subject to change without notice.

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.

IBM is a registered trademark of International Business Machine Corporation.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Novell and LAN Workplace are registered trademarks of Novell Inc.

Toshiba is a trademark of Toshiba Corporation.

# Patents

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

## U.S. Patent No.

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; 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; 5,216,232;  
5,229,591; 5,230,088; 5,235,167; 5,243,655; 5,247,162; 5,250,791; 5,250,792; 5,260,553; 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; 5,557,093; 5,578,810; 5,581,070; 5,589,679;  
5,589,680; 5,608,202; 5,612,531; 5,619,028; 5,627,359; 5,637,852; 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; 5,742,043; 5,745,794; 5,754,587; 5,762,516; 5,763,863; 5,767,500;  
5,789,728; 5,789,731; 5,808,287; 5,811,785; 5,811,787; 5,815,811; 5,821,519; 5,821,520; 5,823,812; 5,828,050; 5,850,078;  
5,861,615; 5,874,720; 5,875,415; 5,900,617; 5,902,989; 5,907,146; 5,912,450; 5,914,478; 5,917,173; 5,920,059; 5,923,025;  
5,929,420; 5,945,658; 5,945,659; 5,946,194; 5,959,285; 6,002,918; D305,885; D341,584; D344,501; D359,483; D362,453;  
D363,700; D363,918; D370,478; D383,124; D391,250; D405,077; D406,581; D414,171; D414,172; D419,548

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  
Holtville, N.Y. 11742-1300  
Telephone:(800)SCAN234, (516)738-2400, TLX:6711519  
[www.symbol.com](http://www.symbol.com)

# About This Document

---

## Reference Documents

This reference guide refers to the following documents:

Part Number	Document Title
70E-20706-02	Wireless LAN Adapter Models LA-4121 PC Card & LA-4123 PCI Adapter Product Reference Guide
70E-20709-02	Spectrum24 Plus Pack Users Guide
70E-20708-02	Spectrum24 Site Survey System Administrators Guide

## 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 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.
<i>Italics</i>	indicates the first use of a term, book title, variable or menu title.
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.
<a href="#">URL</a>	indicates Uniform Resource Locator.

---

This document uses the following for certain conditions or information:



---

Indicates tips or special requirements.

---



---

Indicates conditions that can cause equipment damage or data loss.

---



---

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

---

# Contents

---

<b>Chapter 1 Introduction</b> .....	1
1.1 Access Point (AP) .....	1
1.2 Radio Basics .....	3
1.2.1 S24 Network Topology .....	3
1.2.2 Cellular Coverage .....	8
1.2.3 Site Topography .....	10
1.3 Access Point Functional Theory .....	12
1.3.1 MAC Layer Bridging .....	12
1.3.2 Auto Fallback to Wireless Mode .....	14
1.3.3 DHCP Support .....	14
1.3.4 Media Types .....	15
1.3.5 Bridging Support .....	16
1.3.6 Direct-Sequence Spread Spectrum .....	20
1.3.7 MU Association Process .....	21
1.3.8 Mobile IP .....	23
1.3.9 Supporting CAM and PSP Stations .....	26
1.3.10 Data Encryption .....	27
1.3.11 HTTP, HTML Web Server Support .....	28
1.3.12 Management Options .....	29
<b>Chapter 2 Configuring the AP</b> .....	33
2.1 Gaining Access to the UI .....	33
2.1.1 Using Telnet .....	33
2.1.2 Using a Direct Serial Connection .....	35
2.1.3 Using a Dial-Up Connection .....	36
2.1.4 Using a Web Browser .....	37
2.2 Navigating the UI .....	43
2.2.1 Entering Admin Mode .....	45
2.2.2 Changing the Access to the UI .....	46

---

2.2.3 Configuring for Dial-Up to the UI.....	48
2.2.4 Navigating the UI Using a Web Browser .....	49
2.3 Access Point Installation.....	50
2.4 Configuring System Parameters.....	52
2.4.1 System Password Administration.....	56
2.5 Configuring Radio Parameters .....	58
2.5.1 Wireless Operation Parameters.....	64
2.5.2 Encryption Key Maintenance .....	69
2.5.3 Enable Strong Encryption.....	74
2.6 Configuring PPP.....	76
2.6.1 PPP Direct .....	76
2.6.2 Establishing Connection .....	77
2.6.3 PPP with Modems.....	77
2.6.4 Originating AP .....	77
2.6.5 Answering AP .....	78
2.6.6 Initiating Modem Connection.....	79
2.7 Configuring the SNMP Agent .....	80
2.8 Configuring the ACL .....	84
2.8.1 Range of MUs .....	84
2.8.2 Adding Allowed MUs .....	86
2.8.3 Removing Allowed MUs.....	86
2.8.4 Enable/Disable the ACL .....	87
2.8.5 Removing All Allowed MUs .....	87
2.8.6 Load ACL from MU List .....	87
2.9 Configuring Address Filtering.....	88
2.9.1 Adding Disallowed MUs .....	89
2.9.2 Removing Disallowed MUs .....	89
2.10 Configuring Type Filtering .....	89
2.10.1 Adding Filter Types .....	89
2.10.2 Removing Filter Types.....	89
2.10.3 Controlling Type Filters.....	90

---

2.11 Clearing MUs from the AP .....	90
2.12 Setting Logging Options .....	91
2.13 Manually Updating AP Firmware .....	93
2.13.1 Update using TFTP .....	93
2.13.2 Updating using Xmodem .....	96
2.14 Auto Upgrade all APs Through Messaging .....	98
2.15 Performing Pings .....	101
2.16 Mobile IP Using MD5 Authentication.....	104
2.17 Saving the Configuration .....	104
2.18 Resetting the AP .....	106
2.19 Restoring the Factory Configuration .....	106
<b>Chapter 3 Monitoring Statistics.....</b>	<b>107</b>
3.1 System Summary .....	107
3.2 Interface Statistics.....	110
3.3 Forwarding Counts .....	111
3.4 Mobile Units.....	112
3.5 Mobile IP.....	116
3.6 Known APs .....	117
3.7 Ethernet Statistics .....	118
3.8 Radio Statistics.....	120
3.9 Miscellaneous Statistics.....	126
3.9.1 Analyzing Channel Use .....	128
3.9.2 Analyzing Retries .....	129
3.10 Event History .....	130
3.11 Clearing Statistics.....	131
<b>Chapter 4 Hardware Installation.....</b>	<b>133</b>
4.1 Precautions .....	133
4.2 Package Contents .....	133
4.3 Requirements .....	134
4.3.1 Network Connection .....	134
4.3.2 10Base-T UTP .....	134

---

4.3.3 Single Cell .....	135
4.4 Placing the AP .....	135
4.5 Power Options.....	135
4.6 Mounting the AP .....	136
4.7 Connecting the Power Adapter .....	136
4.8 LED Indicators .....	137
4.8.1 WLAP mode LED display.....	138
4.9 Troubleshooting.....	140
4.9.1 Ensure wired network is operating .....	140
4.10 Setting Up MUs.....	141
<b>Appendix A Specifications .....</b>	<b>A-1</b>
A.1 Physical Characteristics .....	A-1
A.2 Radio Characteristics.....	A-2
A.3 Network Characteristics.....	A-3
<b>Appendix B Supported Modems.....</b>	<b>B-1</b>
<b>Appendix C Customer Support .....</b>	<b>C-1</b>
<b>Appendix D Regulatory Compliance .....</b>	<b>D-1</b>
<b>Index.....</b>	<b>Index-1</b>



## Chapter 1 Introduction

---

Spectrum24 is a 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 any environment.

The Symbol AP-4121 access point (AP) is a Spectrum24 direct-sequence (DS) product. Spectrum24 DS products use direct-sequence technology to provide a high-capacity, high-data-rate wireless network.

Spectrum24 DS infrastructure products include:

- bridging architecture to provide communication between radio and wired multiple network segments
- a design based on the IEEE 802.11 standard
- an 11 Mbps data rate for fast operation
- seamless roaming for mobile users with devices such as laptops, wireless PCs, scanning terminals and other computers with PCMCIA slots.

### 1.1 Access Point (AP)

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

The AP provides an 11 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
- built-in dual antenna assembly with optional diversity
- wireless MAC interface
- field upgradable Firmware
- 10baseT Ethernet port interface with full-speed filtering
- power supply IEC connector and a country-specific AC power cable
- PC/AT Serial Port Interface
- support for up to 127 MUs
- data encryption
- increased MIB support
- SNMP support
- Mobile IP support
- DHCP support
- HTTP Web server support
- short RF preamble
- wireless AP.

When properly configured, an MU communicating with an AP appears on the network as a peer to other network devices. The AP receives data from its wired interfaces and forwards the data to the power interface.

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

## 1.2 Radio Basics

Spectrum24 devices use both *electromagnetic waves* 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 transmit in the 2.4 to 2.5-GHz frequency range, a license-free range throughout most 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. A 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
- the data transfer rate
- the wireless AP (WLAP) interface.



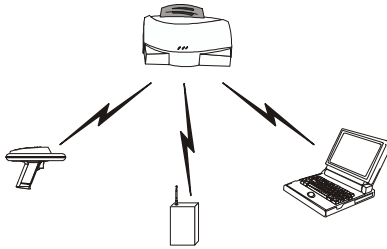
---

A WLAP communicates only with its root AP through the wireless interface as discussed in *The Root AP and Association Process* on page 9.

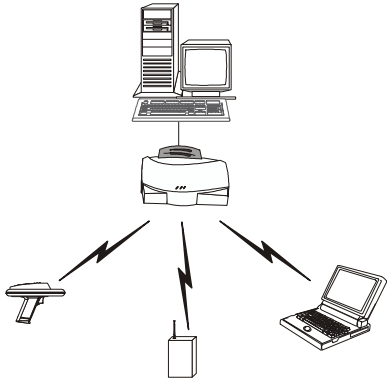
---

Select from the following topologies:

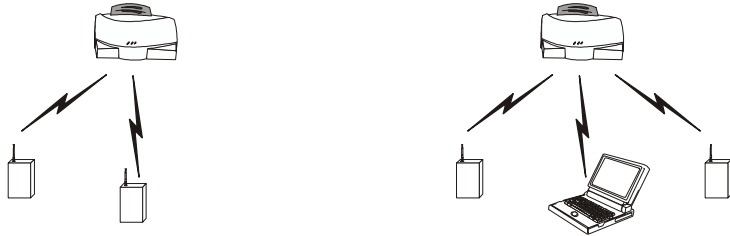
- A single AP used without the wired network provides a single-cell wireless network for peer-to-peer MUs.



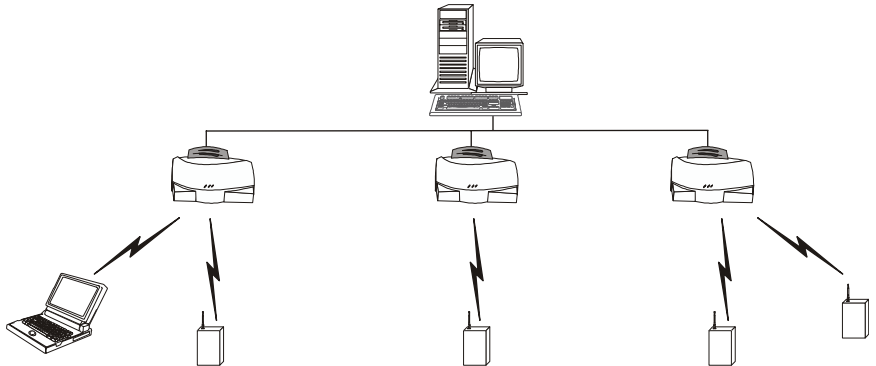
- A single AP can bridge the Ethernet and radio networks.



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

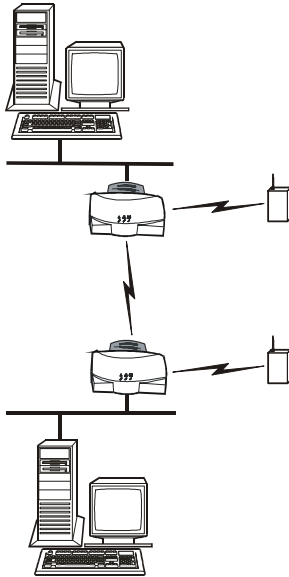


- Multiple APs wired together provide a network with better coverage area and performance when using the same Net\_IDs.

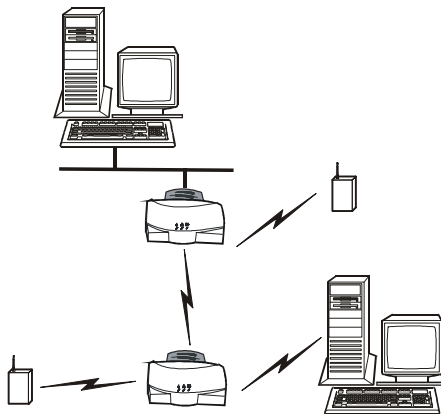


In WLAP mode, a wireless AP-to-AP connection functions:

- as a bridge to connect two Ethernet networks



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



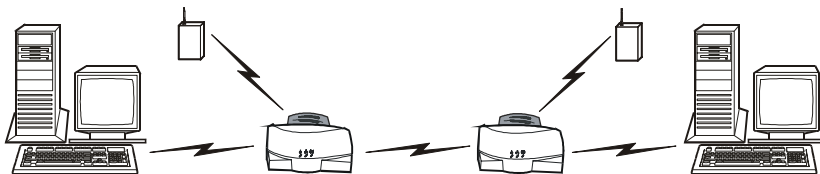


---

When using a wireless AP-to-AP connection, use the optimal antenna configuration for the site. For example, use an omnidirectional 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. To increase WLAP performance, disable *WNMP Functions* and *AP-AP State Xchg* parameters under the *Set System Configuration* screen.

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 58.



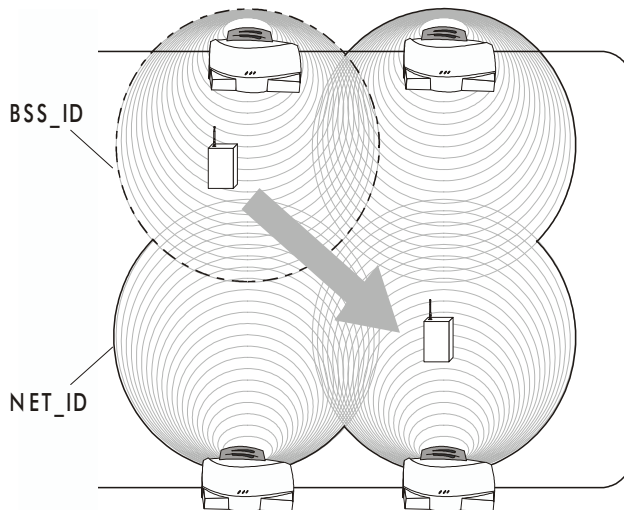
---

The WLAP initialization process length depends on the time specified in the *WLAP Forward Delay* field. See [2.5 Configuring Radio Parameters](#) on page 58.

---

## 1.2.2 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 IEEE 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 a 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*.



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

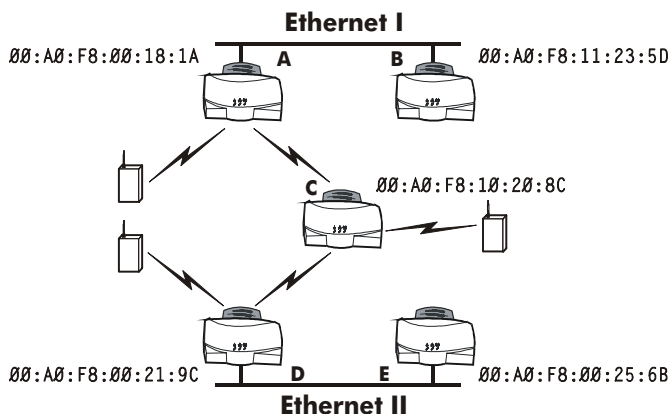
By default, APs with *WLAP Mode* enabled and within range of each other automatically associate and configure wireless operation parameters at power up. This association process determines the wireless connection viability and establishes the *Root AP* and subsequently designated WLAPs.



Note

APs communicating wirelessly together require the same: Net\_ID (ESS), Encryption mode, Data Rate and Short RF Preamble settings.

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. A concatenation of the *WLAP Priority* value and the MAC address becomes the *WLAP ID*. Ensure the WLAPs associated with the Root AP use the Root AP channel, *DTIM (Delivery Traffic Indication Message)* and *TIM (Traffic Indication Map)* 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 channel, 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 channel, DTIM and TIM interval.

To manually designate AP B as the Root AP, assign it a lower WLAP Priority value. See *2.5 Configuring Radio Parameters* on page 58. Assigning a WLAP Priority value of 7000 Hex to the AP B MAC address 00:A0:F8:11:23:5D causes AP B to become the Root AP by having the lowest WLAP ID 700000A0F811235D.

## IEEE 802.1d Spanning Tree Support

This protocol creates a *loop-free* topography with exactly ONE path between every device and LAN. This is the shortest path from the Root AP to each WLAP and LAN. If the connection between a WLAP and LAN fails, a new route is calculated and added to the tree. All packet forwarding follows the spanning tree path determined. APs in a network have to choose one AP as the Root AP.

### 1.2.3 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 APs in open areas or add APs as needed to improve coverage.

## Site Surveys

A site survey analyzes the installation environment and provides users with recommendations for equipment and its placement. The optimum placement of 11 Mbps access points differs for 1 or 2 Mbps access points, because the locations and number of access points required are different.



Symbol recommends conducting a new site survey and developing a new coverage area floor plan when switching from 1 or 2 Mbps frequency-hopping access points to 11 Mbps direct-sequence access points.

---

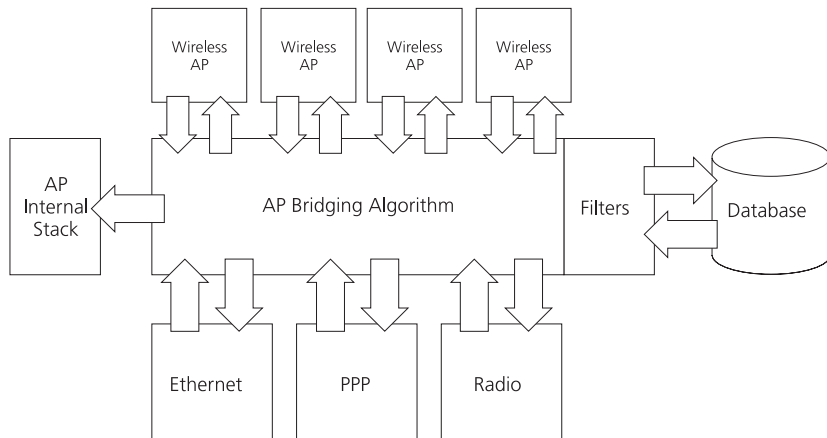
## 1.3 Access Point Functional Theory

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 associate with the AP. The AP uses the database to forward packets from one interface to another. The bridge forwards packets addressed to unknown systems to the Default Interface (either Ethernet or PPP).





---

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.



---

Transmitted ARP request packets echo back to other MUs.

---

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 provide network security or improve performance by eliminating broadcast/multicast packets from the radio network.

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

The AP uses 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. 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 Auto Fallback function operates only with an AP in WLAP Mode and connected to the Ethernet network. The AP resets itself and during initialization attempts to associate with any other WLAP in the network.

See 2.4 *Configuring System Parameters* on page 52 and 2.5.1 *Wireless Operation Parameters* on page 64.



---

To make this feature available: set the WLAP Mode to `Link Required`.

---

### 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 interoperate, the one that responds first becomes the server that allocates 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. 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 is not able to renew the IP address lease the AP sends out an SNMP trap.

---



---

Mobile IP is not available when DHCP is used. Disable DHCP support when configuring an AP and mobile device for Mobile IP.

---

### 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 11 Mbps. The Ethernet interface is optional for single-cell or PPP-connected networks.

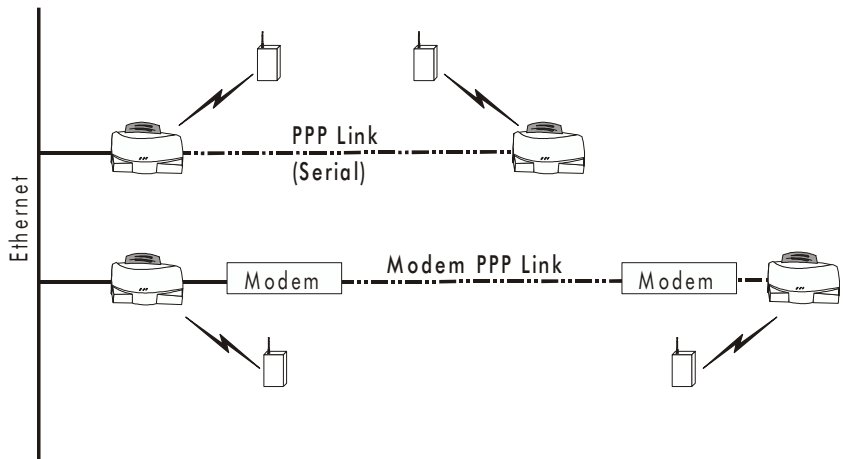
The *radio interface* conforms to IEEE 802.11 specifications. The interface operates at 11 Mbps using direct-sequence radio technology. The AP supports multiple-cell operations with fast roaming between cells. With the direct-sequence system, each cell operates independently. Each cell provides an 11 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

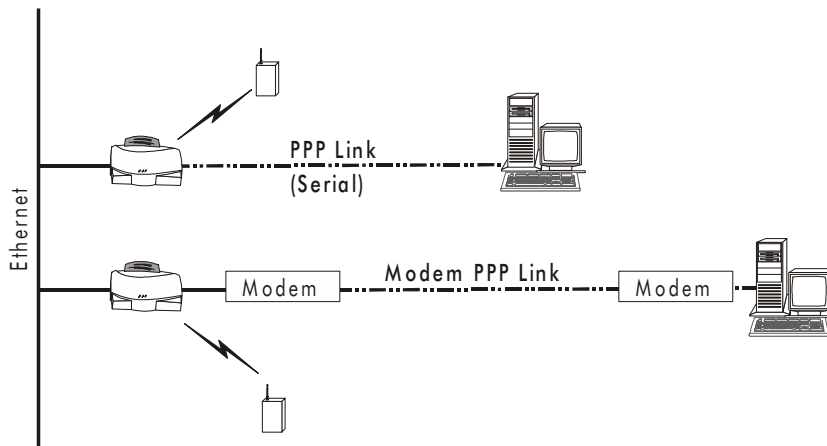
The AP PPP (*Point to Point Protocol*) interface, accessible from the serial port at the rear of the AP, provides two types of bridging operations:

- 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 through 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. Using Telnet, a remote computer 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.

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.

---



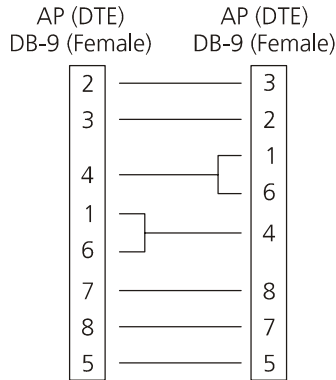
The PPP implementation in the AP uses the NCP as described in *RFC 1220: PPP Extensions for Bridging* to encapsulate packets at the Ethernet level. The PPP provides IP bridging control as defined by *RFC 1172 and MAC-level bridging*. It provides support for PPP negotiations conforming to *RFC 1661*.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

---

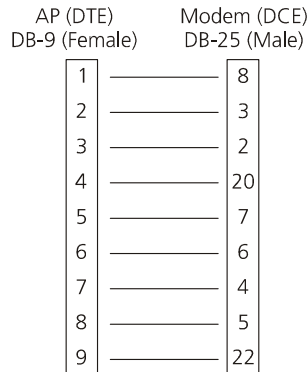
Refer to *RFC 1171: The Point to Point Protocol* and *RFC 1220: PPP Extensions for Bridging* for information.

## 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 a telephone line for as long as the link remains active.



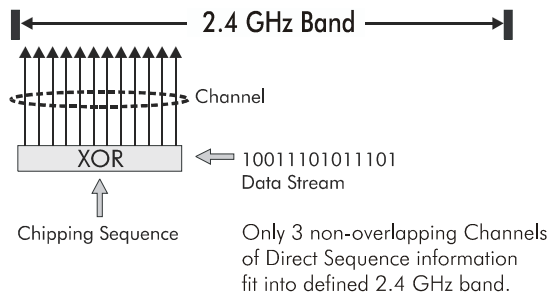
When using a modem connection, one AP represents the originating AP and the other represents the answering AP. When using a PPP link, do not use the serial port to access the UI. Access to the UI requires establishing a Telnet session with the AP.

### 1.3.6 Direct-Sequence Spread Spectrum

*Spread spectrum (broadband)* uses a narrowband signal to spread the transmission over a segment of the radio frequency band or spectrum. Direct-sequence is a spread spectrum technique where the transmitted signal is spread over a particular frequency range. The Spectrum24 AP-4121 HR Access Point uses direct-sequence spread spectrum (DSSS) for radio communication.

Direct-sequence systems communicate by continuously transmitting a redundant pattern of bits called a *chipping sequence*. Each bit of transmitted data is mapped into *chips* by the access point and rearranged into a pseudorandom *spreading code* to form the chipping sequence. The chipping sequence is combined with a transmitted data stream to produce the AP output signal.

#### Direct Sequence



Note

In the United States, the three non-overlapping direct-sequence channels are channels 1, 6 and 11.

Mobile Units receiving a direct-sequence transmission use the spreading code to map the chips within the chipping sequence back into bits to recreate the original data transmitted by the access point. Intercepting and decoding a direct-sequence transmission requires a predefined algorithm to associate the spreading code used by the transmitting access point to the receiving MU. This algorithm is established when the access point and MU are configured. The bit redundancy within the chipping sequence enables the receiving MU to recreate the original data pattern, even if bits in the chipping sequence are corrupted by interference.

The ratio of chips per bit is called the *spreading ratio*. A high spreading ratio increases the resistance of the signal to interference. A low spreading ratio increases the bandwidth available to the user. The access point uses two chips per bit among three channels within the 2.4 GHz band in a pattern avoiding any 1 or 2 Mbps systems operating in the same area. The access point is capable of an 11 Mbps data transmission rate, but the coverage area is less than a 1 or 2 Mbps access point since coverage area decreases as bandwidth increases.

### 1.3.7 MU Association Process

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

- the signal strength between the AP and MU
- MUs currently associated with the AP
- the MUs encryption and authentication capabilities and the type enabled
- the MU supported data rate (1 Mbps, 2 Mbps, 5.5 Mbps or 11 Mbps).

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 statistics and determine the direct-sequence channel used by the AP.

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 (ESS) 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 response within the time limit, it repeats the probe 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 (ESS) 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 a coverage area by switching APs. 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.

An MU selects the best available AP and adjusts itself to the AP direct-sequence channel to begin association. Once associated, the AP begins forwarding any frames it receives addressed to the MU. Each frame contains fields for the current direct-sequence channel. The MU uses these fields to resynchronize to the AP.

### 1.3.8 Mobile IP

The Internet Protocol identifies the MU point of attachment to a network through its IP address. The AP routes packets 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, causing forthcoming packets to become undeliverable.
- The MU changes its IP address when it moves to a new network, causing it to lose 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.

Mobile IP is like giving an individual a local post office forwarding address when leaving home for an extended period. When mail arrives for the individual home address, it is forwarded by the local post office to the current care-of-address. Using this method, only the local post office requires notification of the individual current address. While this example 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 MU home network. The home agent intercepts packets sent to the MU 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 MU location on a foreign link. The foreign agent 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 MU 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.



---

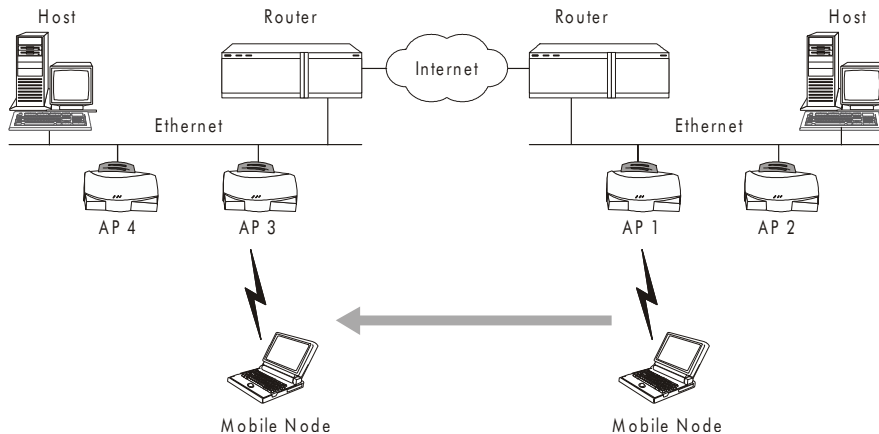
To configure this feature, see [2.4 Configuring System Parameters](#) on page 52.

---



The scanning and association process continues for active MUs. This allows the MUs to find new APs and discard out-of-range or deactivated APs. By 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 MU 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 to 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 Indication Message*) and the TIM (*Traffic Indication Map*).

PSP (*Power Save Polling*) stations power off their radios for long periods. When a Spectrum24 MU in PSP mode associates with an AP, it notifies the AP of its activity status. The Spectrum24 AP-4121 HR access point responds by buffering packets received for the MU. The Spectrum24 adapters use a PSP performance index from 1 to 5, where 1 provides the quickest response time and 5 provides the most efficient power consumption.

The performance index determines how long the adapter stays in CAM after transmit or receive activity. Regardless of the performance index used, adapters switch to CAM for data reception/transmission. The awake interval in PSP performance index 1 is long enough to allow for round-trip packet response times. The packet response time in PSP performance index 5 is only 25 msec, the adapter goes back to sleep and requires another wake up period to receive data.

When the MU wakes up and sees its bit set in the TIM, it issues a short frame to the AP for the packets stored. The AP sends them to the MU and the MU issues another short frame when the data has been received and is ready to go back to PSP. A DTIM field, also called a countdown field, informs MUs of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated MUs, it sends the next DTIM with a *DTIM Interval* value. 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

Spectrum24 devices operating on a wired or wireless network face possible information theft. This occurs when an unauthorized user eavesdrops on someone else to obtain information illegally. 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 entails scrambling and coding information, typically with mathematical formulas called *algorithms*, before the information is transmitted over a 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 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. The device takes plain text, encrypts or scrambles the text typically by mathematically combining the key with the plain text as instructed by the algorithm, then transmits the data over the network. At the receiving end another device takes the encrypted text and decrypts, or unscrambles, the text revealing the original message. An unauthorized 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 key.

Symbol uses the *Wired Equivalent Privacy (WEP)* algorithm, specified in IEEE 802.11 section 8, for encryption and decryption. WEP uses the same key for both encrypting and decrypting plain text. Typically an external key management service distributes the 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

Hypertext Transfer Protocol (HTTP) is the native language of the Web. The HTTP 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.

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 known as Uniform Resource Locators (URLs). A URL is essentially the name of the web page. The URL consists of three parts:

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

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 the network activity of associated MUs and data transfers on the AP interfaces.

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

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

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 networks operating characteristics and changing router and gateway parameters. The SNMP protocol consists of three elements:

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

Nodes can perform as 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 details of each specific event, including what, when and 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 through an SNMP manager application such as, HP Open View or Cabletron Spectrum MIB browser. The SNMP agent supports SNMP versions 1 and a subset of version 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* disk packaged with MUs contains the MIB.

## Increased MIB Support

The *MIB (Management Information Base)* has ten categories defining what the management station needs to understand and which objects the station manages.

## Using the UI

The *UI (User Interface)* is a 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:

- |                                 |  |
|---------------------------------|--|
| <i>Telnet Client</i>            | Access to the AP built-in Telnet server from any interface including remote Ethernet connections.<br>See 2.1.1 <i>Using Telnet</i> on page 33.   |
| <i>Direct Serial Connection</i> | The AP acts as a DTE device to connect directly to another DTE device with a null-modem serial cable. The direct serial access method requires a communication program with ANSI emulation.<br>See 2.1.2 <i>Using a Direct Serial Connection</i> on page 35.   |
| <i>Dial Up Access</i>           | 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.<br>See 2.1.3 <i>Using a Dial-Up Connection</i> on page 36. |
| <i>SNMP Using a MIB Browser</i> | Access to the AP SNMP function using a MIB Browser. Typically a Network Manager uses this feature, however, Symbol does not recommend accessing the AP using this interface method.<br>Refer to the MIB Browser documentation for usage.   |
| <i>Web Browser</i>              | Access to the AP built-in Web server from any AP interface including Ethernet connections.<br>See 2.1.4 <i>Using a Web Browser</i> on page 37.   |





## 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 update to all APs with the same Net\_ID (ESS) when choosing the `Save ALL APs-[F2]` option. Users can perform this option only among the same hardware platforms and same firmware versions.

---

### 2.1 **Gaining Access to the UI**

The method for establishing access to the UI depends on the connection used. Select the setup that best fits the network environment.

#### 2.1.1 **Using Telnet**

Using a Telnet session to gain access to the UI requires that a remote station 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 type the password:

```
Symbol
```



Note

The password is case-sensitive.

---

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

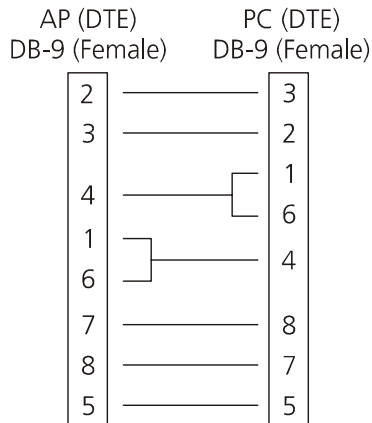
Symbol Access Point	MAIN MENU
Show System Summary	AP Installation
Show Interface Statistics	Special Functions
Show Forwarding Counts	Set System Configuration
Show Mobile Units	Set RF Configuration
Show Known APs	Set Serial Port Configuration
Show Ethernet Statistics	Set Access Control List
Show RF Statistics	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.
- Press CTRL+D to manually terminate the session.

Set the *System Passwords* 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 2.2.3 *Configuring for Dial-Up to the UI* on page 48.

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, such as HyperTerminal for windows.
3. Select the correct COM port along with the following parameters.

<i>emulation</i>	ANSI
<i>baud rate</i>	19200 bps
<i>data bits</i>	8
<i>stop bits</i>	1
<i>parity</i>	none
<i>flow control</i>	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 terminate 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 2.2.3 *Configuring for Dial-Up to the UI* on page 48.

---

## 2.1.4 Using a Web Browser

A Web Browser is a program used to view Web documents or pages. The browser retrieves the requested page, interprets its text and displays the page properly formatted on a computer screen.

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.



The Web Browser (Internet Explorer 4.0 or greater or Netscape) requires JavaScript to gain access to the UI.

---

### Setup Network Web Server Help File Access

A network Web server is required to access the Help file from the *Spectrum24 Access Point Configuration Management System* web pages. This procedure applies to the Microsoft Internet Information Server. The network Web server can be different, if so, some of the procedures differ.



This procedure is for Network or System Administration personnel only.

---

To create the Help file on a network Web server:

1. Create a directory on the network Web server for the AP Web Site Help Files to reside.

Often this is a subdirectory to C:\inetpub\wwwRoot.

2. Copy the \*.gif and \*.htm files to this directory/folder.

The files are maintained in the x:\firmware\AP\AP Web Site\Help File directory.

Where x is the letter assigned to the computer CDROM drive.



---

This installation example is for Windows NT 4.0.

---

3. From the windows Task Bar select **Start**.
4. From the drop down menu select **Programs**.
5. From this menu select **Microsoft Internet Server(common)**.
6. From this menu select **Internet Service Manager** to launch the Internet Information Server Service Manager.  
Click on the Web service.



---

Ensure the server WWW service is running.

---

7. Select **Properties**.
8. Select **Service Properties** to display the WWW service properties for the server.
9. The **WWW Service Properties** window opens.
10. Select the **Directories** Tab.
11. Select the **Add** button to open the Directories window.
12. Type the *Directory/Folder* path of the directory created in step one.
13. Select the **Virtual Directory** button.
14. Type a folder *alias* such as *WebHelp* and select **OK**.
15. Select the **Enable Default Document** checkbox.
16. Type *S24apHelp.htm* as the default document and select **Apply**.
17. Select **OK** to exit the window.
18. Test the accessibility to the Help file using a Web browser with a URL similar to: <http://xxx.xxx.xxx.xxx/WebHelp>  
Where xxx.xxx.xxx.xxx is IP address of the server.

## Accessing Web Browser UI

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.

Ensure the `Web Server` option is enabled for the AP:

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. Select `Save-[F1]` to save the configuration.

Reset the AP for changes to take effect.

1. Select the *Special Functions* screen.
2. Select `Reset AP`.
3. Select `Yes` at the confirmation prompt.

To enable Help file access, change the Help URL parameter:

1. Select the *Special Functions* screen.
2. Use the TAB or UP/DOWN ARROW key to select the `Alter Filename(s)/HELP URL/TFTP Server/DHCP`.
3. Press ENTER.
4. Use the TAB or DOWN ARROW key to select the `.HELP URL` field.
5. Type the IP address/URL (Universal Request Locator) of the Web server and the directory/folder of the Web server for the Help file location.  
<http://xxx.xxx.xxx.xxx/WebHelp>  
Where `xxx.xxx.xxx.xxx` is the IP address of the server.
6. Press ENTER.
7. Use the TAB or DOWN ARROW key to select `OK-[CR]` and press ENTER.
8. Select the `Save Configuration` option to save the new setting.

9. Select **Yes** at the confirmation prompt.
10. The *Main Menu* screen displays.

Reset the AP for changes to take effect.

1. Select the *Special Functions* screen.
2. Select **Reset AP**.
3. Select **Yes** at the confirmation prompt.

To access the AP UI using 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.



The workstation, in this case, is the workstation or laptop computer running the Web browser.

---

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.

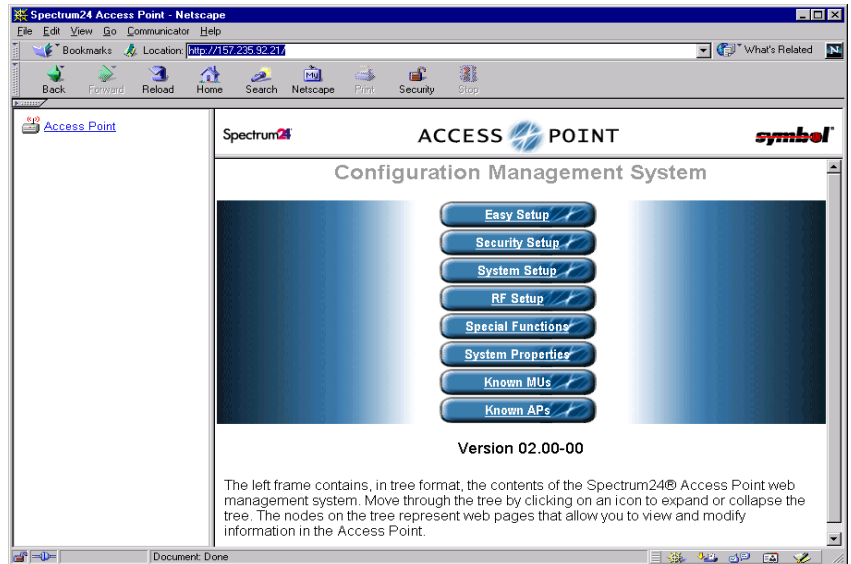
3. Start a Web browser such as Internet Explorer 4.0 or greater, or Netscape 3.0 or greater.

Type the IP Address for the associated AP to access the AP using a Web browser:

<http://xxx.xxx.xxx.xxx>



4. The Spectrum24 Access Point Configuration Management System main page displays:



Note

The Web pages look different than the Telnet, Direct Serial or Dial-Up Connections, but the contents are the same. 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.

- To view configuration, function or option changes on the Web page(s) turn off the caching function for the browser being used.
  - For Netscape, from the menu bar select Edit, Properties and Advanced, Cache.
  - Select Document in cache is compared to document on network: Every time.
  - For Internet Explorer, from the menu bar select View, Internet Options, Temporary Internet files and Settings.

- Select **Check for newer versions of stored pages: Every visit to the page.**

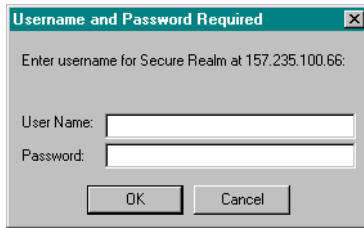


---

If this property/option is not turned off, the browser returns the previous view of the page without the changes. To ensure the latest version of a web page is viewed, set this option in the browser.

---

- To access help from any *Spectrum24 Access Point Configuration Management System* web page, select the **Help** button located in the top right-hand corner of each page.
- For access to the *Easy Setup* and *Configuration* pages this popup dialogue box appears:



1. Type the AP name.  
Symbol Access Point
2. Type the password:  
Symbol



---

The AP name and password are case-sensitive.

---

- Exit the browser to manually terminate the session.

## 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 arrow 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 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 Passwords*, 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 the [F1] key brings up the Ping function to Ping that AP.
- Press ESC to exit from submenus.

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 <i>NVM</i> ( <i>nonvolatile memory</i> ). A reset command returns to previously saved settings.
Save	Saves all settings (including ones not on that screen) to <i>NVM</i> . This is the same as <i>Save Configuration</i> in the <i>Special Functions</i> screen.
Save ALL APs	To save the <i>AP installation</i> configuration information to all APs with the same <i>Net_ID</i> (ESS). This option saves the configuration changes for the current AP on the <i>Known APs</i> table to update their configuration and reset after the configuration has been modified. Users can perform this option only among the same hardware platforms and same firmware versions.
Cancel	Does not register settings changed in a screen.

## 2.2.1 Entering Admin Mode

The UI defaults to *User* when in *Serial mode* allowing read-only access to the APs functions (e.g., view statistics). Entering *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. Type 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.



---

Set the *System passwords* 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 Passwords*.

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 Passwords*:

1. Select *Set System Configuration* from the Main Menu.
2. Press TAB to select *System Password Admin-[F4]*.

### 3. The *Change System Passwords* screen displays:

```

Symbol Access Point
                                Change System Passwords

User Password      *****

Admin Password     *****

Save-[F1]         Cancel-[ESC]

Password for user access(Monitor only)

```

### 4. Change the passwords using the following parameters:

<i>User Password</i>	Allows the user to only monitor or view the screens. Select any alphanumeric, case-sensitive entry up to 13 characters, the characters selected are displayed as asterisks. The default password is Symbol.
<i>Admin Password</i>	Allows the user to view and change the parameters on each screen. Select any alphanumeric, case-sensitive entry up to 13 characters, the characters selected are displayed as asterisks. The default password is Symbol.

5. Select *OK* or *Save* to register settings by writing changes to NVM. Selecting *Save* displays a confirmation prompt.
6. Select *Cancel* - [ESC] to disregard any changes made to this screen and return to the previous menu.

### 2.2.3 Configuring for Dial-Up to the UI

A dial-up connection 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).



---

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 time-out.



## Configuring the Dial-Up System

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

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

<i>emulation</i>	ANSI
<i>baud rate</i>	19200 bps
<i>data bits</i>	8
<i>stop bits</i>	1
<i>parity</i>	none
<i>flow control</i>	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*.

## Hangup

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 Using a Web Browser

Refer to the online help file for information on Web Browser navigation and basic functionality. For file download instructions and the associated file(s) refer to the Web page: ([http://www.symbol.com/services/downloads/download\\_spec24.html](http://www.symbol.com/services/downloads/download_spec24.html)) and select Spectrum24® - 1 and 2 Mbps FH Firmware, Software, Drivers, Tools and....

## 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         157.235.101.152              157.235.101.2
                                     0.0.0.0
.Gateway IP Address 157.235.101.1              0.0.0.0
                                     0.0.0.0
.Subnet Mask       255.255.255.0              0.0.0.0
                                     0.0.0.0
.Net_ID (ESS)      101                        0.0.0.0

.Antenna Selection Diversity On

.DHCP              Enabled

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.

---

<i>Subnet Mask</i>	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 subnetworks and simplify routing and data transmission. The subnet mask defines the size of the subnet.
<i>Net_ID (ESS)</i>	The unique 32-character, alphanumeric, case-sensitive network identifier of the AP.
<i>Antenna Selection</i>	Enables selection of antenna diversity.
<i>Additional Gateways</i>	The IP address of the additional gateways used. Access up to seven gateways.
<i>DHCP</i>	Enables the DHCP client to automatically send a DHCP request every XX hours/days to renew the IP address lease as long as the AP is running.

3. Verify the AP parameters reflect the network environment. Change them as needed.
4. In the *Antenna Selection* field, use the SPACE BAR or LEFT/RIGHT-ARROW keys to toggle between *Primary Only* and *Diversity On*.
5. Select *OK* or *Save* to register settings by writing changes to NVM. Selecting *Save* displays a confirmation prompt.
6. Select *Save ALL APs-[F2]* to save the *AP installation* configuration information to all APs with the same *Net\_ID (ESS)*. 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. Users can perform this option only among the same hardware platforms and same firmware versions.
7. Select *Cancel-[ESC]* to disregard any changes made to this screen and return to the previous menu.

## 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

Channel                          3          .Access Control    Disabled
                                .Type Filtering    Disabled

.Ethernet Timeout                Ø

.Telnet Logins                   Enabled    WNMP Functions     Enabled
                                .AP-AP State Xchg  Enabled

.Encryption Admin                Any       Ethernet Interface  On
                                PPP Interface      Off
                                RF Interface       On

.Agent Ad Interval               Ø
.S24 Mobile IP                  Disabled
.Mobile-Home MD5 key           *****   Default Interface  Ethernet

.Web Server                      Enabled   .MU-MU Disallowed  Off

System Password Admin-[F4]

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

Save, then reset AP to take effect.
    
```

2. Configure the direct-sequence channel settings.

<i>Frequency</i>	<i>Allowed Channel Range</i>	<i>Country</i>
2412-2470	1-11	United States
2430-2447	5-8	Israel
2457-2463	10-11	Spain
2458-2472	10-13	France
2483-2485	14	Japan

3. Configure the AP system settings as required:

*Ethernet Timeout* Disables 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. 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 and the WLAP has connected to the Root AP, 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.

When the Ethernet connection is broken the AP clears the MU table and disables the RF interface until the Ethernet connection comes up.

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

<i>Encryption Admin</i>	<p>Indicates which interface can change the encryption keys and the encryption key index. Without admin privileges users cannot change this parameter, or view the encryption keys.</p> <p><i>Any</i> allows users with admin privileges to change encryption keys through any interface.</p> <p><i>Serial</i> allows users with admin privileges to change this parameter and encryption keys only through the Serial port.</p>
<i>Agent Ad Interval</i>	<p>Specifies the interval in seconds between the mobility agent advertisement transmission.</p>
<i>S24 Mobile IP</i>	<p>If enabled, this feature allows MUs to roam across routers.</p>
<i>Mobile-Home MD5 key</i>	<p>Secret key used for Mobile-Home registration and authentication.</p>
<i>MU-MU Disallowed</i>	<p>If enabled, mobile units associated with the same AP are not allowed to communicate with each other.</p>
<i>Web Server</i>	<p>Enables the use of a Web based browser to access the UI instead of HyperTerminal or Telnet applications.</p> <p>An AP Reset is required for this feature to take effect.</p>
<i>System Password Admin</i>	<p>Allows the user to change the passwords for the AP.</p> <p>This screen can be accessed only when the AP is in <i>Telnet</i> mode.</p> <p><i>Serial</i> mode provides read-only privileges and does not allow the user to view this screen.</p>
<i>Access Control</i>	<p>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.</p>
<i>Type Filtering</i>	<p>Specifies filter type for packets received either Forward/Discard or Disabled.</p> <p>The default value is Disabled.</p>

- 
- |                         |   |
|-------------------------|---|
| <i>WNMP Functions</i>   | Specifies if the AP can perform WNMP functions. The default value is Enabled. |
| <i>AP-AP State Xchg</i> | Specifies AP-to-AP communication exchanged.                                   |
4. To enable or disable interfaces on the AP, modify the following parameters:

<i>Ethernet Interface</i>	Enables or disables wired Ethernet. The default value is On.
<i>PPP Interface</i>	Enables or disables serial PPP. The default value is Off.
<i>RF Interface</i>	Enables or disables radio. The default value is On.
<i>Default Interface</i>	Specifies the default interface (Ethernet, PPP or WLAP) that the AP forwards a frame to if the AP cannot find the address in its forwarding database. The default interface is Ethernet.
  5. Verify the values set reflect the network environment. Change them as needed.
  6. Select *OK* or *Save* to register settings by writing changes to NVM. Selecting *Save* displays a confirmation prompt.
  7. Select *Save ALL APs - [F2]* to save the *System Configuration* information to all APs with the same *Net\_ID* (ESS). 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. Users can perform this option only among the same hardware platforms and same firmware versions.
  8. Select *Cancel - [ESC]* to disregard any changes made to this screen and return to the previous menu.

## 2.4.1 System Password Administration

This screen allows the network administrator to configure the passwords for the AP. The user password allows the user to Telnet into the AP or use the serial port and have read-only privileges. Accessing the UI in an Admin mode session through the serial port the session does not time-out.



---

On entering the Admin mode with both the Telnet and Serial Port interfaces active enables Admin mode on both interfaces. This can cause a security breach if a user, without admin privileges, Telnets into the AP while the admin security level is enabled entitling the user to admin level access.

---

1. To access and change the System Passwords, select `System Password Admin-[F4]` from the System Configuration Menu. The *Change System Passwords* screen displays:

```
Symbol Access Point
                                     Change System Passwords

User Password      *****
Admin Password    *****

Save-[F1]         Cancel-[ESC]

Password for user access(Monitor only)
```



2. Change the passwords using the following parameters:

*User Password* Allows the user to only monitor or view the screens. Select any alphanumeric, case-sensitive entry up to 13 characters, the characters selected are displayed as asterisks. The default password is Symbol.

*Admin Password* Allows the user to view and change the parameters on each screen. Select any alphanumeric, case-sensitive entry up to 13 characters, the characters selected are displayed as asterisks. Changing this password changes the Read/Write Community password, set in the SNMP Configuration screen. The default password is Symbol.

3. Select *Save* to register settings by writing changes to NVM. Selecting *Save* displays a confirmation prompt.
4. Select *Cancel* - [ESC] to disregard any changes made to this screen and return to the previous menu.

## 2.5 Configuring Radio Parameters

The AP automatically configures most radio parameters. Only advanced users, Symbol trained users or Symbol representatives should adjust the 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
.Beacon Interval              100 K-us       WLAP Forward Delay       5
.Accept Broadcast ESSID       Disabled
.MU Inactivity Timeout        60 min.
.Rate Control
  11 Mb/s                      Optional
  5.5 Mb/s                     Optional
  2 Mb/s                       Optional
  1 Mb/s                       Required
.RTS Threshold                 2347 bytes
.CCA Mode                     Carrier Sense
.CCA Energy Threshold          60

OK-[CR]      Save-[F1]      Save All APs-[F2]      Cancel-[ESC]
The frequency of DTIM packets as a multiple of TIM packets. Range(1..255)
    
```



RTS Threshold, CCA Mode and CCA Energy Threshold are not user configurable parameters.

2. Configure the settings as required:

<i>DTIM Interval</i>	Configure DTIM packet frequency as a multiple of beacon packets. The DTIM Interval indicates how many beacons equal one cycle. Do not modify.
<i>BC/MC Q Max</i>	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.
<i>Reassembly timeout</i>	Sets the time in 0.5 ms units before a time-out occurs during a packet reassembly. Packet reassembly occurs when a large RF packet is fragmented into smaller wireless network packets. The default is 9000.
<i>Max Retries (d)</i>	The maximum allowed retries before aborting a single data packet transmission. The default is 15. Users should not modify.
<i>Max Retries (v)</i>	The maximum allowed retries before aborting a single voice packet transmission. The default is 5. Do not modify.
<i>Multicast Mask (d)</i>	Supports broadcast download protocols for any MU, typically Point-of-Sale terminals, requiring the expedited download of a new operating image over the network instead of using a local nonvolatile drive.  All multicast downstream data packets that match the top 32 bits of the multicast mask are forwarded immediately instead of being queued for transmission at the next DTIM interval.
<i>Multicast Mask (v)</i>	Supports broadcast, or <i>party-line</i> , voice communications. All multicast downstream data packets that match the top 32 bits of the multicast mask are forwarded immediately instead of being queued for transmission at the next DTIM interval.

<i>Beacon Interval</i>	The time between beacons in Kilo-microseconds. The default is 100. Avoid changing this parameter because it can adversely affect PSP-mode terminal performance.
<i>Accept Broadcast ESSID</i>	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 ESS 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.
<i>MU inactivity Timeout</i>	Allows industry-standard device 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.

---

<i>Rate Control</i>	<p>Defines the data transmission rate, the defaults are:</p> <ul style="list-style-type: none"> <li>• 11 Mbps - Optional</li> <li>• 5.5 Mbps - Optional</li> <li>• 2 Mbps - Optional</li> <li>• 1 Mbps - Required.</li> </ul> <p>The defaults allow the AP to automatically select the the best transmit rate allowed by the conditions. These settings allow a mixture of 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps radios in the same network.</p> <p>Any combination of the data rates can be selected as <i>Optional</i>, <i>Required</i> or <i>Not Used</i>, but it is essential to set the lowest selected rate to <i>Required</i>.</p> <p>All IEEE 802.11 broadcast and management frames are sent out on the lowest required data rate.</p>
<i>RTS Threshold</i>	<p>Request to send threshold (256 – 2347). Allows the AP to use RTS (Request To Send) on frames longer than the specified length.</p> <p>The default is 2347 Bytes.</p>
<i>CCA Mode</i>	<p>Clear Channel Assessment (CCA) mode is the method used to detect transmissions from sources other than the access point.</p> <p>The default is <code>Carrier Sense</code>.</p>
<i>CCA Energy Threshold</i>	<p>The energy threshold or level above which the airwaves are considered busy. The default is <code>60</code>.</p>
<i>WEP (Privacy)</i>	<p>Defines the WEP algorithm. Admin privileges are required to make changes to this parameter.</p> <p>The default is <code>Disabled</code>.</p>

<i>WEP Algorithm</i>	Defines the number of bits and type of WEP algorithm used. Admin privileges are required to make changes to this parameter. The default is 40 bit shared key.
<i>Encryption Key ID</i>	Allows the user to change the <code>Active Key</code> number. Admin privileges are required to make changes to this parameter. The default key ID is 1. Reset the AP for the new key value to become the active key.
<i>Encryption Key Maintenance</i>	Allows the user to create or change the values for each encryption key. Admin privileges are required to make changes to this parameter.
<i>Enable Strong Encryption</i>	Allows access to and use of the 128 bit encryption keys. Some countries will not have access to the 128 bit encryption screens due to encryption export restrictions. To access the 128 bit encryption key screen contact the Symbol Customer Support Center for a unique access code to enable this feature.

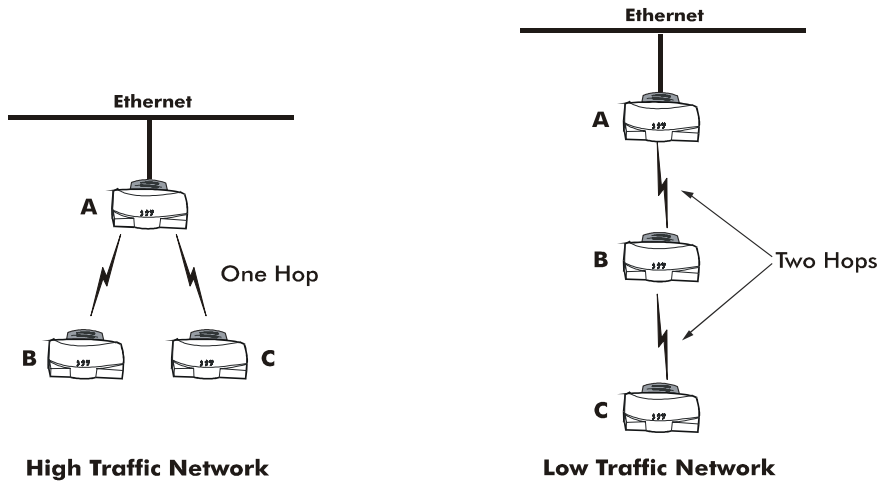
*Short RF Preamble* Determines whether the AP uses a short or long preamble. The preamble is approximately 8 bytes of the packet header generated by the AP and attached to the packet prior to transmission. The preamble length is transmission data rate dependant. The short preamble is 50% shorter than the long preamble.

This feature is only available to version 2.0 radio hardware. Equipment without the version 2.0 radios can not enable the short preamble function and can not see, receive or acknowledge messages from short preamble enabled version 2.0 hardware. Disable this feature in a mixed hardware network and use the long preamble. MUs and APs are required to have the same Short RF Preamble settings for interoperability. The default is *Enabled*.

3. Verify the values set reflect the network environment. Change them as needed.
4. Select *OK* or *Save* to register settings by writing changes to NVM. Selecting *Save* displays a confirmation prompt.
5. Select *Save ALL APs - [F2]* to save the *RF Configuration* information to all APs with the same *Net\_ID (ESS)*.  
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. Users can perform this option only among the same hardware platforms and same firmware versions.
6. Select *Cancel - [ESC]* to disregard any changes made to this screen and return to the previous menu.

## 2.5.1 Wireless Operation Parameters

The AP supports up to four WLAP interfaces. Symbol recommends using one WLAP as an interface on high traffic networks, for low traffic networks no more than two WLAPs, because excessive channel contention causes the WLAP to miss beacons from the Root AP shown in the example.



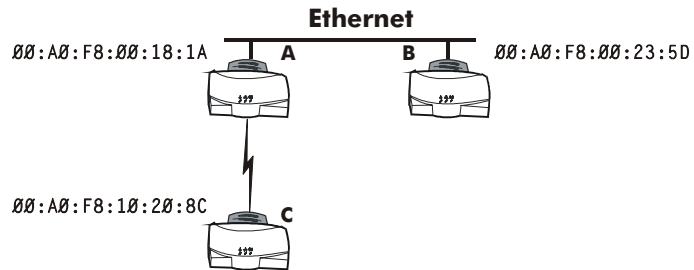
See 4.8 LED Indicators on page 137 for indication of AP status. If more than two WLAPs operate in a repeater configuration, Symbol recommends the WLAPs with the lowest WLAP IDs be placed on the wired network.

To avoid forming a loop, per the IEEE 802.1d Spanning Tree Protocol, the Wireless WLAP associates with only one wired WLAP.

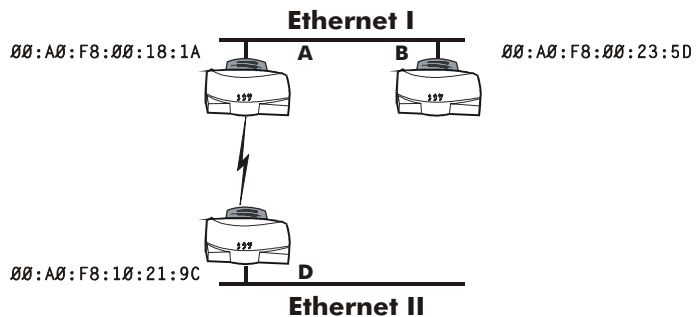
1. Set the default interface for AP A to Ethernet.
2. Set the default interface for AP B to Ethernet.



3. Set the default interface for AP C to WLAP.  
This allows the MUs to roam and transmit data between AP B and C.



If an AP functions as a bridge between wired LANs, Symbol recommends one LAN contain all the lower WLAP IDs.



To configure the AP for wireless operation:

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

<i>WLAP Mode</i>	<p>Specifies the APs wireless-AP operation status.</p> <p><i>Enabled</i>, the AP sets up automatically for wireless operation. The AP can operate in any of these configurations: Wireless, Repeater or Ethernet Bridge.</p> <p><i>Disabled</i>, no wireless operation possible. Default setting.</p> <p><i>Link Required</i>. At power up:</p> <ul style="list-style-type: none"><li>• If the WLAP is the Root AP, an Ethernet connection is required.</li><li>• If the WLAP is a designated WLAP, association to the Root AP is required.</li></ul> <p>During normal operation:</p> <ul style="list-style-type: none"><li>• If the Ethernet connection is lost, the Root AP resets.</li><li>• If the WLAP association is lost, the designated WLAP resets.</li></ul>
<i>WLAP Priority</i>	<p>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 AP. The default is 8000 hex from the 0 - 0xFFFF range.</p>

---

<i>WLAP Manual BSS_ID</i>	<p>Specifies the BSS_ID of a particular WLAP and forces the current AP to associate only with that WLAP.</p> <p>If setting the <i>WLAP Manual BSS_ID</i> to the current BSS_ID, the current AP jumps into <i>Functional State</i> immediately and waits for an Association Request from the other WLAP. See 3.8 <i>Radio Statistics</i> on page 120. This feature speeds up the association process and minimizes confusion when more than two WLAPs try to associate with each other.</p>
<i>WLAP Hello Time</i>	<p>Sets the time lapse, in seconds, between <i>Config BPDUs</i> 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 <i>WLAP Max Age</i> time, it removes the designated WLAP from its interface table.</p> <p>The <i>WLAP Hello Time</i> of the Root AP overwrites the <i>WLAP Hello Time</i> of designated WLAPs. The <i>WLAP Hello Time</i> 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 AP has lost the Root status.</p>
<i>WLAP Max Age</i>	<p>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 <i>WLAP Hello Time</i>. The default is 100 seconds.</p> <p>The <i>WLAP Max Age</i> of the Root AP overwrites the <i>WLAP Max Age</i> of designated WLAPs.</p>

*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 120, affect the *WLAP Forward Delay* time. This delay ensures that all WLAP nodes are heard. The default is 5 seconds per wireless operation state.

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

## 2.5.2 Encryption Key Maintenance

The Encryption Key Maintenance screens allow the user to configure the encryption keys used for the site network. The WEP Algorithm used determines which encryption Key screen displays. To enable the Open System option, select *Disabled* for WEP (privacy) on the RF Configuration screen.

This table shows the AP association capability with the selected WEP Algorithm.

<i>AP Selected WEP Algorithm</i>	<i>MU Selected WEP Algorithm</i>	<i>Association Status</i>
Open (disable)	Open	Associated
Open (disable)	40	No Association
Open (disable)	128	No Association
40	Open	No Association
40	40	Associated
40	128	Associated, but cannot transmit data
128	Open	No Association
128	40	Associated, but cannot transmit data
128	128	Associated

Each 40 bit encryption key is a subset of the respective 128 bit encryption key. The first 40 bits of each encryption key is the same for the respective 40 bit and 128 bit encryption keys. When a 40 bit encryption key is changed the first 40 bits of the respective 128 bit key is also changed. Consequently, when a 128 bit encryption key is changed the first 40 bits of the 40 bit encryption key is changed. Moreover, configuring the encryption Keys using the SNMP Trap Manager overrides the Key value(s) for the AP(s) accessed by the SNMP Trap Manager.

Symbol provides a total of four Encryption Keys. Each key enables encryption between the AP and an associated MU with the same encryption Key and Key value.

Two screens are available, one for 40 bit encryption and one for 128 bit encryption.

Considerable care is required when assigning keys. Keys have to be in the same order with the same value per key for the AP and MU to authenticate data transmission using encryption.

Example: An AP uses Key 1 with a value of 1011121314. The associated MU requires the same Key 1 to have the value 1011121314.

---



Some countries do not have access to the 128 bit encryption screens due to imposed encryption export restrictions. To access the 128 bit encryption screen contact the Symbol Customer Support Center at 1-800-653-5350 for the unique access code to enable this feature.

---

To access the *Encryption Key Maintenance* screen determined by the WEP algorithm chosen, select *Encryption Key Maintenance* from the *RF Configuration Menu*.

## 40 Bit Encryption

If 40 bit encryption is the selected WEP Algorithm, this screen is displayed.

Symbol Access Point

Encryption Key Maintenance

.Key 1 \* 1Ø111 21314

.Key 2 2Ø212 22324

.Key 3 3Ø313 23334

.Key 4 4Ø414 24344

\* = Active Key

OK-[CR]

Save-[F1]

Save All APs-[F2]

Cancel-[ESC]

Each key has 40 bits available to the user for configuration and are displayed in two 20 bit segments. The remaining 24 IV (*initialization vector*) bits are factory set and not user configurable.

1. Select the desired key and enter the new value to change the Key value.
2. Verify and change the values set as needed to reflect the network environment.
3. Select **OK** or **Save** to register settings by writing changes to NVM. Selecting **Save** displays a confirmation prompt.

4. Select `Save ALL APs-[F2]` to save the *Encryption Key Maintenance* information to all APs with the same `Net_ID` (ESS).  
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. Users can perform this option only among the same hardware platforms and same firmware versions.
5. Select `ESC` to disregard any changes made to this screen and return to the previous menu.

## 128 Bit Encryption

If 128 bit encryption is the selected WEP Algorithm, this screen is displayed.

Symbol Access Point

### Encryption Key Maintenance

```
.Key 1 * 10111 21314 1516 1718 191A 1B1C
.Key 2    20212 22324 2526 2728 292A 2B2C
.Key 3    30313 23334 3536 3738 393A 3B3C
.Key 4    40414 24344 4546 4748 494A 4B4C
```

\* = Active Key

`OK-[CR]`

`Save-[F1]`

`Save All APs-[F2]`

`Cancel-[ESC]`



Each key has 124 bits available to the user for configuration and are displayed in two 20 bit segments and four 16 bit segments. The remaining 24 IV (*initialization vector*) bits are factory set and not user configurable.

1. Select the desired key and enter the new value to change the Key value.
2. Verify and change the values set as needed to reflect the network environment.
3. Select **OK** or **Save** to register settings by writing changes to NVM. Selecting **Save** displays a confirmation prompt.
4. Select **Save ALL APs-[F2]** to save the *Encryption Key Maintenance* information to all APs with the same Net\_ID (ESS).  
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. Users can perform this option only among the same hardware platforms and same firmware versions.
5. Select **ESC** to disregard any changes made to this screen and return to the previous menu.

### 2.5.3 Enable Strong Encryption

Some countries do not have access to the 128 bit encryption screens due to encryption export restrictions. For countries outside the United States an access code is required to enable the Strong Encryption, i.e. 128 bit encryption. Obtain an access code by contacting Symbol Customer Service at 1-800-653-5350.

1. To enable Strong Encryption (128 bit encryption) select *Enable Strong Encryption* on the RF Configuration screen. This screen is displayed.

Symbol Access Point

Enable Strong Encryption

US regulations restrict the export of products containing strong forms of encryption technology. Please see user's manual for information on obtaining an access code to unlock strong encryption.

.Access Code    \_\_\_\_ - \_\_\_\_ - \_\_\_\_

OK-[CR]

Save All APs-[F2]

Cancel-[ESC]

2. Enter the acquired access code in the space provided.
3. Select **OK** or **Save** to register settings by writing changes to NVM. Selecting **Save** displays a confirmation prompt.

4. Select `Save ALL APs-[F2]` to save the *Enable Strong Encryption* access code to all APs with the same `Net_ID` (ESS).  
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. Users can perform this option only among the same hardware platforms and same firmware versions.
5. Select ESC to disregard any changes made to this screen and return to the previous menu.

## 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	PPP	Answer Wait Time	60
Connect Mode	Answer	Inactivity Timeout	5
Modem Connected	No	PPP Timeout	3
Dialout Mode	Auto	PPP Terminates	10
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 into 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 type the dial-out 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:

<i>Answer Wait Time</i>	Time in seconds waiting for a remote connection before dropping attempt. The default is 60 from a 5 to 255-second range.
<i>Modem Speaker</i>	Sends a command to the modem to turn on or off the modem speaker. The default is 0n.
<i>PPP Timeout</i>	Controls the time-out 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 time-out. The default is 3 from a 0 to 255-second range.
<i>PPP Terminates</i>	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.

For automatic dial-out:

1. Select the *Serial Port Configurations* screen from the *Main Menu*.
2. Set the *Dialout Mode* to *Auto*.
3. Select *Save-[F1]* to save the changes in NVM.
4. Select the *Special Functions* screen from the *Main Menu*.
5. Select *Reset AP*.

The AP LEDs flash as if powering up and the AP returns to a *STATUS*-flashing state.

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. An AP can be accessed through the SNMP Trap Manager to configure settings and parameters, Symbol does not recommend this process.



Configuring the encryption Keys using the SNMP Trap Manager overrides the Key values for the Ap or APs accessed by the SNMP Trap Manager.

---

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.



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

---

The AP supports SNMP Version 1, a limited feature set of SNMP Version 2, the IEEE 802.11 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  .Trap Host1 IP Address 0.0.0.0
                                .Trap Host2 IP Address 0.0.0.0

.Read-Only Community  *
.Read-Write Community *
.All Traps            Disabled

Generic Traps:
.Cold Boot           Disabled
.Authentication failure Disabled

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

<i>SNMP Agent Mode</i>	<p>Defines the SNMP agent mode:</p> <p><i>Disabled</i> disables SNMP functions.</p> <p><i>Read-only</i> allows get and trap operations.</p> <p><i>Read/Write</i> (default) allows get, set and trap operations.</p>
<i>Read-Only Community</i>	User-defined password string up to 31 characters identifying users with read-only privileges.
<i>Read/Write Community</i>	<p>User-defined password up to 13 characters for users with read/write privileges.</p> <p>Ensure the password used matches the Admin Password used to gain access to the System Password Administration screen.</p>
<i>All Traps</i>	<p>Enables or disables all trap operations.</p> <p>The default value is Disabled.</p>
<i>Cold Boot</i>	<p>Send a trap to the manager when the AP cold boots.</p> <p>The default value is Disabled.</p>
<i>Authentication failure</i>	<p>Indicates that community strings other than those specified for the Read-Only and Read/Write Community were submitted.</p> <p>The default value is Disabled.</p>
<i>Radio Restart</i>	<p>Send a trap to the manager for radio restart.</p> <p>The default is value Disabled.</p>
<i>Access Cntrl Violation</i>	Send a trap to the manager when an ACL violation occurs. The default value is Disabled.
<i>Trap Host1 IP Address</i>	<p>The Trap Host1 manager IP address.</p> <p>The default is 0.0.0.0.</p>
<i>Trap Host2 IP Address</i>	<p>The Trap Host2 manager IP address.</p> <p>The default is 0.0.0.0.</p>

- 
- |                               |   |
|-------------------------------|---|
| <i>DHCP Change</i>            | If enabled, this trap generates the following enterprise-specific traps: <ul style="list-style-type: none"><li>• <b>Gateway Address change</b><br/>Indicates the gateway address for the router has changed.</li><li>• <b>IP Address Change</b><br/>Indicates the IP address for the AP has changed.</li><li>• <b>IP Address Lease is up</b><br/>Informs the user the IP address leased from the DHCP server is about to expire.</li></ul>  |
| <i>WLAP Connection Change</i> | If enabled, this trap generates the following enterprise-specific traps: <ul style="list-style-type: none"><li>• <b>Root WLAP Up</b><br/>Indicates that the Root AP connection is setup and ready to forward data.</li><li>• <b>Root WLAP Lost</b><br/>If the current WLAP fails to receive a Beacon packet from its Root AP within one second, it considers the Root AP lost. The WLAP eventually resets itself to reestablish the network topology.</li><li>• <b>Designated WLAP Up</b><br/>Indicates that the Designated WLAP connection is setup and ready to forward data.</li><li>• <b>Designated WLAP Lost</b><br/>If the current WLAP fails to receive a <i>Config BPDU</i> packet from its Designated WLAP for <i>MAX AGE</i> time, it considers the Designated WLAP lost.</li></ul> |

3. Verify the values reflect the network environment. Change them as needed.
4. Select **OK** or **Save** to register settings by writing changes to NVM. Selecting **Save** displays a confirmation prompt.

5. Select `Save ALL APs-[F2]` to save the *SNMP Configuration* information to all APs with the same `Net_ID` (ESS).  
This option saves the configuration changes for the current AP, and sends two WNMPP messages to all other APs on the *Known APs* table to update their configuration and reset after the configuration has been modified. Users can perform this option only among the same hardware platforms and same firmware versions.
6. Select `Cancel-[ESC]` to disregard any changes made to this screen and return to the previous menu.

## 2.8 Configuring the ACL

The ACL supports adding MU entries by individual MAC address or by a range of MAC addresses. The maximum number of entries is 512 if no entries have been made for Disallowed Address Filtering. Only 512 entries are available to both ACL and Disallowed Address Filtering.

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:  
`00:0A:F8:F0:01:01`
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:  
`00:0A:F8:F0:02: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
      00:A0:F8:F0:01:01  00:A0:F8:F0:02:FF
      00:A0:F8:29:10:02  00:A0:F8:29:11:00

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

```

6. Verify values reflect the network environment. Change them as needed.
7. Select `Delete-[F1]` to delete a range of Mobile Units.
8. Select `Add-[F2]` to add a range of Mobile Units.
9. Select `Save ALL APs-[F3]` to save the *Ranges of Allowed Mobile Units* information to all APs with the same `Net_ID` (ESS).  
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. Users can perform this option only among the same hardware platforms and firmware versions.
10. Select `Exit-[ESC]` to return to the previous menu.

When users enable the *Access Control* option, all MUs within the specified range 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.



Users can enter MAC addresses without colons.

---

5. Select *Save ALL APs-[F3]* to save the *Adding Allowed MU* information to all APs with the same *Net\_ID* (ESS).  
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. Users can perform this option only among the same hardware platforms and firmware version.

## 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 type 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 the MUs not allowed to associate with it. The *Disallowed Addresses* option provides security by preventing unauthorized access by known devices. Use it for preferred association of MUs to APs. The maximum number of entries is 512 if no entries have been made for the ACL. 512 is the number of entries available to both ACL and Disallowed Address Filtering entries.

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

```

Symbol Access Point
                                Disallowed Addresses

00:A0:F8:F0:00:0A                00:A0:F8:FF:FF:C7
00:A0:F8:F0:00:01                00:A0:F8:FF:FF:89
00:A0:F8:FE:10:01
00:A0:F8:F0:03:0A
00:A0:F8:F0:03:A1
00:A0:F8:B0:A0:09
00:A0:F8:F1:A2:08
00:A0:F8:F0:08:08
00:A0:F8:F2:06:01
00:A0:F8:F2:0B:02
00:A0:F8:F2:0C:04
00:A0:F8:F0:04:01
00:A0:F8:F4:03:02
00:A0:F8:F0:07:0C
00:A0:F8:F0:0C:07
00:A0:F8:F1:21:30
00:A0:F8:F0:20:A1
00:A0:F8:F0:A0:03
00:A0:F8:F0:09:0B

Delete-[F1]  Add-[F2]  Next-[F3]  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.



Users can enter MAC addresses without colons.

---

## 2.9.2 Removing Disallowed MUs

The *Disallowed Addresses* screen provides a facility to 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. Select *Save ALL APs-[F2]* to save the *Type Filtering Setup* information to all APs with the same *Net\_ID* (ESS). Users can perform this option only among the same hardware platforms and firmware versions.



Users can only enable one type filtering option at a time.

---

## 2.11 Clearing MUs from the AP

Clear the MU association table for diagnostic purposes. Clear MUs from the AP 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 the MUs associated with it. MUs cleared from the 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*:

<i>Any Event Logging</i>	Logs all events listed in the screen.
<i>Security Violations</i>	ACL filter or administrative password access violations.
<i>MU State Changes</i>	Allows logging all MU state changes.
<i>WNMP Events</i>	WNMP events such as MUs using WNMP.
<i>Serial Port Events</i>	Serial port activity.
<i>AP-AP Msgs</i>	AP to AP communication.
<i>Telnet Logins</i>	Telnet sessions for monitoring and administration.
<i>System Events</i>	Internal use only.
<i>Ethernet Events</i>	Events such as packet transmissions and errors.

3. Verify the values reflect the network environment. Change them as needed.
4. Select `OK` or `Save` to register settings by writing changes to NVM. Selecting `Save` displays a confirmation prompt.
5. Select `Save ALL APs-[F2]` to save the *Event Logging Configuration* information to all APs with the same `Net_ID` (ESS). 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. Users can perform this option only among the same hardware platforms and firmware versions.
6. Select `Cancel-[ESC]` to disregard any changes made to this screen and return to the previous menu.

## 2.13 Manually Updating AP Firmware

To update Access Points with firmware and HTML file versions older than 1.50, the user must update the AP firmware and HTML files to version 1.50 first, then update the firmware and HTML files to version 2.00. Conversely, if the user wanted to downgrade the firmware and HTML files from version 2.00 to version 1.00 the user would need to downgrade the firmware and HTML files to version 1.50 first, then downgrade the firmware and HTML files to version 1.00. When updating or downgrading the HTML files the user is required to use the *Both* option under the function heading *Use XMODEM to Update Access Point's*. Both the firmware and HTML files are required to be loaded on the TFTP server or users hard disk.

Options for manually updating the firmware:

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

The files required for firmware updates are DSAP\_FW.BIN and DSAP\_HTM.BIN.

### 2.13.1 Update 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 DSAP\_FW.BIN and DSAP\_HTM.BIN on the terminal or PC hard disk.
2. Telnet to the AP using its IP address.

3. At the prompt type the password:

Symbol



The password is case-sensitive. Set the *System Passwords* 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 file-name in the *Download Filename* field:



Change this only if the user or system/network administrator requires a new file-name. The defaults are DSAP\_FW.BIN and DSAP\_HTM.BIN.

---

dsap\_fw.bin or dsap\_htm.bin



Ensure the file name is DSAP\_FW.BIN and DSAP\_HTM.BIN unless the user changed the file-name.

---



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.



Caution

---

If using telnet to connect to the AP through an Ethernet interface, do not use the *Use XMODEM to Update Access Point's Firmware* option. This option causes the AP to reset and look for the firmware file over the serial interface.

---

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 type the password:

Symbol

---



Note

---

The password is case-sensitive.

---

The AP displays the *Main Menu*.

15. Verify the accuracy of the version number 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. 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 DSAP\_FW.BIN and DSAP\_HTM.BIN to the PC hard disk that runs a terminal emulation program.
2. Attach a null modem serial cable from the AP to the PC serial port.
3. On the PC, start the communication program.
4. Name the 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:

<i>emulation</i>	ANSI
<i>baud rate</i>	19200 bps
<i>data bits</i>	8
<i>stop bits</i>	1
<i>parity</i>	none
<i>flow control</i>	none

6. Select **OK**.
7. Press **ENTER** to display the *Main Menu*.



8. Select *Enter Admin Mode* and type 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 DSAP\_FW.BIN and DSAP\_HTM.BIN files separately. Ensure both files 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 DSAP\_FW.BIN and DSAP\_HTM.BIN are the firmware files.



Caution

---

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

---

13. From the emulation program menu bar, select *Transfer*.
14. Select the *Send File* command.
15. Select the *Browse* button and locate the file(s), DSAP\_FW.BIN and DSAP\_HTM.BIN.
16. Select the *XModem* protocol from the drop down list.
17. Click *Send*.

18. The terminal or PC displays the transfer process through a progress bar.

19. If downloading both the firmware and HTML files, the screen flashes:

```
Downloading HTML file using XMODEM.  
Send HTML file with XMODEM now ...
```

If downloading both files, repeat the steps beginning at step 13 to download the next file and avoid a transfer time-out error. If not, continue to step 20.

20. The download is complete when the UI displays:

```
Download Successful  
Updating AP  
Update Successful
```

If the firmware update fails, the UI displays an error code indicating the cause.

The AP automatically resets after all file transfers are completed.

- Exit the communication program to terminate the session.
- Repeat this process for other APs in the network.

## 2.14 Auto Upgrade all APs Through Messaging

The Update ALL Access Points option upgrades or downgrades the firmware of all associated APs with the same Net\_ID (ESS) on the same subnet and includes all recognized hardware platforms regardless of firmware version. The initiating AP sends the correct file name for each Symbol platform. The initiating AP does not send update commands to non-Symbol platforms.

Users can find the specific APs that have firmware upgraded or 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 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 DSAP\_FW.BIN and DSAP\_HTM.BIN on the terminal or PC hard disk.
2. Telnet to the AP using its IP address.
3. At the prompt type the password:

```
Symbol
```



The password is case-sensitive. Set the *System Passwords* 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. Type the firmware file-name in the *Download Filename* field:

```
dsap_fw.bin or dsap_htm.bin
```

Change this only if the user or system/network administrator requires a new file-name. The defaults are DSAP\_FW.BIN and DSAP\_HTM.BIN.



Ensure the file name is DSAP\_FW.BIN and DSAP\_HTM.BIN unless the user changed the file-name.

---



---

Verify the accuracy of the path for the file name. (See step one)

---

7. Type 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.  
"Are you sure (Y/N)?" is displayed. Type "y".  
The Telnet session ends when the user answers "y" at the prompt.



---

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

---

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

12. Telnet to the AP using its IP address.
13. At the prompt type the password:  
Symbol



---

The password is case-sensitive.

---

The AP displays the *Main Menu*.

14. Verify the accuracy of the version number on the *System Summary* screen.
15. Press CTRL+D to end the Telnet session.

## 2.15 Performing Pings

An access point sends a ping packet to an MU and waits for a response. Use pings to evaluate signal strength between two stations. The other station can exist on any AP interface.



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

No pings returned or fewer pings returned 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:R11:E
00:A0:F8:10:4B:AB: P:R11:
00:a0:F8:10:4A:13: P:R11:
00:A0:F8:10:3C:85: C:R11:

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

Select **TAB** to highlight the MAC address of the station, and press the **[F1]** key to display the *Echo Test* screen:

```
                                     Echo Test

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

[Start-CR]        [Cancel-ESC]

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

3. Enter the number of echo requests (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. The AP dynamically displays packets transmitted and received:

```
Echo Test in Progress...
```

```
Station Address      00:A0:F8:10:4A:13
Requests Transmitted 1
Responses Received   1
```

```
Press any key to stop
```

## 2.16 Mobile IP Using MD5 Authentication

Users can achieve 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 algorithm 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 displaying the `Save` option.

OR complete the following procedure:



## 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

Modem Dialout           Use TFTP to update ALL Access Points':
Modem Hangup            Firmware HTML file

Reset AP                Alter Filename(s)/HELP URL/TFTP Server/DHCP
                          .Firmware Filename dsap_fw.bin
                          .HTML Filename dsap_htm.bin
Run MKK Tests           .HELP URL http://157.233.68.100/Spectrum24WebHelp
                          .TFTP Server 157.235.99.236

Restore Factory Config.
Save Configuration      Save All APs
Save Config. to All APs

Exit-[ESC]

```

## 2. Select *Save Configuration* and press ENTER.

The `Save All APs` function saves only the five preceding items. The function does not save other configuration parameters when selected. Users can perform this option only among the same hardware platforms and firmware versions.

The NVRAM stores saved configuration information. To clear the NVRAM-stored configuration, see [2.19 Restoring the Factory Configuration](#) on page 106.

## 2.18 Resetting the AP

Resetting an AP clears statistics and restores the last saved configuration. If users make unsaved changes, the AP clears those changes and restores the last saved configuration 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 the Factory Configuration

If the AP fails to communicate due to improper settings, restore the factory configuration defaults. Restoring configuration settings clears all configuration and statistics for the AP depending on the DHCP setting.

*DHCP Disabled* all AP configuration and statistics are reset, except the AP *Installation* screen

*DHCP Enabled* all AP configuration and statistics are reset

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.



---

When the factory configuration is restored, the ACL list is not erased.

---

## 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)  00:A0:F8:00:C2:24   Access Control   Disabled
IP Address         157.235.92.156       WLAP Mode       Enabled
Net_ID (ESS)      CA2

Channel            3
Model Number      AP-4121-100-US
Serial Number     L498912
Hardware Revision 3.01

Country           United States
Antenna Selection Diversity On
WEP (Privacy)     Disabled
WEP Algorithm     40 bit shared key
AP Firmware Ver.  02.00-08
RF Firmware Ver.  V2.00-14
HTML File Ver.   02.00-01

Current MUs       0
Start Flashing All LEDs
Total Assoc      4
Reset AP

System Up Time    0:40:47
```

Exit-[ESC]

## 2. Configure the AP system settings as required:

<i>Unit Name</i>	Identifies the AP name.
<i>MAC Address (BSS)</i>	Identifies the unique 48-bit, hard-coded Media Access Control address.
<i>IP Address</i>	Identifies the network-assigned Internet Protocol address.
<i>Net_ID (ESS)</i>	Identifies the unique 32-character, alphanumeric, case-sensitive network identifier.
<i>Channel</i>	Identifies the direct-sequence channel used by the access point. The channel used is within the range required for the operating country.
<i>Country</i>	Identifies AP country code that in turn determines the AP direct-sequence channel range.
<i>Antenna Selection</i>	Indicates if the AP is configured for single or dual antenna mode.
<i>WEP (Privacy)</i>	Defines the WEP algorithm. Admin privileges are required to make changes to this parameter. The default is <code>Disabled</code> .
<i>WEP Algorithm</i>	Defines the number of bits and type of WEP algorithm used. Admin privileges are required to make changes to this parameter. The default is <code>40 bit shared</code> .
<i>Current MUs</i>	Specifies the current number of associated MUs.
<i>Total Assoc</i>	Specifies the total MU associations handled by this AP.
<i>System Up Time</i>	Specifies how long the system has been operational. System Up Time resets to zero after a 119,304 hours.
<i>Access Control</i>	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.

<i>WLAP Mode</i>	Specifies if enabling the wireless AP operation status. If enabled, the AP sets up automatically for wireless operation. This feature is <code>Disabled</code> by default.
<i>Model Number</i>	Identifies the model number.
<i>Serial Number</i>	States the APs unique identifier.
<i>Hardware Revision</i>	Specifies the hardware version.
<i>AP Firmware Ver</i>	Specifies the firmware version.
<i>RF Firmware Ver</i>	Specifies the Radio firmware version.
<i>HTML File Ver</i>	Specifies the HTML file version.
<i>Start Flashing All LEDs</i>	Begins a test routine to check the LED functionality and allows the user to determine the AP location.
<i>Reset AP</i>	Clears the APs statistics and restores the last saved configuration.

3. 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        14066         0   1260844         0
PPP              0           0         0           0
RF              0           0         0           0
AP             13975         0   1257750         0

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

                PPS     PPS     BPS     BPS
                Sent   Rcvd    Sent    Rcvd

Ethernet        0         0         0         0
PPP             0         0         0         0
RF             0         0         0         0
AP             0         0         0         0

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

```

- Select `Refresh` at the status display to update values manually.
- Select `Timed` to automatically update this display every two seconds.
- Press `ESC` to return to the previous menu.

### 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          0           0           0           0
PPP               0           0           0           0
RF               0           0           0           0
AP               0           0           0           0
Bcast            14085       14085       0           0

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

```

- Select *Refresh* at the status display to update values manually.
- Select *Timed* to automatically update this display every two seconds.
- Press *ESC* to return to the previous menu.

## 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 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:R11:
00:A0:F8:10:4A:13  P:R11:

Information-[CR]   Echo-[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:V]
```

Where:

- |             |   |
|-------------|---|
| <i>addr</i> | MU MAC address in xx:xx:xx:xx:xx:xx format  |
| <i>p</i>    | MUs power mode: P for PSP, C for CAM. An unassociated MU does not display any character.  |
| <i>i</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. |
| <i>#</i>    | AP current Radio transmit rate for the messages sent to this MU:<br>11 for 11 Mbps.   |
| <i>e</i>    | Encryption is enabled for this device.  |
| <i>V</i>    | 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 2.15 *Performing Pings* on page 101.
  - Select *Timed* to automatically update this display every two seconds.
  - Select *Next* to display the next screen.
  - Press ESC to return to the previous menu.

- To bring up 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, 5.5 & 11 Mb/s		
Current Xmt Rate	5.5 Mb/s	Last Activity	0:00:11
Priority	Normal	Last Data Activity	16:37:14
Encryption	Off		

Refresh-[F1]

Exit-[ESC]

Displayed information includes:

- |                            |   |
|----------------------------|---|
| <i>Interface</i>           | The AP interface shows the MU connection as: RF, Ethernet, PPP or AP.   |
| <i>State</i>               | The connection state between the AP and the MU: <ul style="list-style-type: none"> <li><i>Host</i> indicates the unit is on the AP or PPP interface</li> <li><i>Associated</i> indicates the current association on the radio interface</li> <li><i>Away</i> indicates the unit is no longer associated with the AP.</li> </ul> |
| <i>Power Mode</i>          | The MU power mode: CAM, PSP or N/A.   |
| <i>Station ID</i>          | 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)  |
| <i>Begin Current Assoc</i> | The time the current association begins in hours, minutes and seconds.  |

---

<i>Supported Rates</i>	Data transmission rates the station supports.
<i>Current Xmt Rate</i>	The current rate the AP transmits data to the station.
<i>Priority</i>	Indicates whether the MU is a voice or data type device. <i>Voice</i> indicates packet delivery is time critical and a high priority. <i>Normal</i> indicates packet delivery is not time critical.
<i>Encryption</i>	MU encryption support: <i>On</i> or <i>Off</i> .
<i>Packets Sent</i>	The packets sent by the AP to the MU.
<i>Packets Rcvd</i>	The packets received by the AP from the MU.
<i>Bytes Sent</i>	The bytes sent by the AP to the MU.
<i>Bytes Rcvd</i>	The bytes received by the AP from the MU.
<i>Discard Pkts/CRC</i>	The packets discarded because of data error.
<i>Last Activity</i>	The time in hours, minutes and seconds since the last communication with the MU.
<i>Last Data Activity</i>	The time in hours, minutes and seconds since the last data transfer.

- Select `Refresh` at the status display to update values manually.
- Press `ESC` to return to the previous menu.

## 3.5 Mobile IP

The following tables display the mapping of MUs to mobility agents.  
See 1.3.8 *Mobile IP* on page 23.

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

Symbol Access Point		Foreign Agent Table	
Mobile Unit	Home Agent	Mobile Unit	Home Agent
157.235.95.184	157.235.95.180		
157.235.95.125	157.235.95.180		
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.



The *Save All APs* function from the *Special Functions Menu* updates and configures all APs firmware, HTML code shown in the *Known APs* menu. Users can perform this option only among the same hardware platforms and firmware versions.

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

Symbol Access Point		Known Access Points							
MAC Address	IP Address	Net_ID:				101			
		CH	HST	HSQ	MUS	KBIOS	FW_Ver	Away	
00:A0:F8:8A:2F:FF	111.111.12.62	3	-	-	0	0	02.00-08		
00:A0:F8:8A:30:CD	111.111.12.63	6	-	-	4	0	01.50-10		
00:A0:F8:8A:30:49	111.111.12.64	11	-	-	4	0	01.00-31		

Echo-[F1]      Delete-[F2]      Next-[F3]      Previous-[F4]      Exit-[ESC]

The AP displays for each known AP:

<i>MAC Address</i>	the unique 48-bit, hard-coded Media Access Control address, known as the devices station identifier
<i>IP Address</i>	the network-assigned Internet Protocol address
<i>DS Channel</i>	The direct-sequence channel used by the AP.
<i>MUS</i>	The MUs associated with the AP.
<i>KBIOS</i>	The data traffic handled by the AP in kilobytes in and out per second
<i>FW_Ver</i>	the firmware version used by the specified AP
<i>Away</i>	Determines if the AP functions as a 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.

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

Symbol	Access Point	Ethernet Statistics	
	Packets Seen	∅	Packets Sent 138
	Packets Forwarded	∅	Any Collisions ∅
	Discarded/NoMatch	∅	1 + Collisions ∅
	Discarded/Forced	∅	Maximum Collisions ∅
	Discarded/Buffer	∅	Late Collisions ∅
	Discarded/CRC	∅	Defers ∅
	Broadcast/Multicast	∅	
	Individual Address	∅	
	Refresh-[F1]	Timed-[F2]	Exit-[ESC]

---

Packet display for Ethernet statistical units:

<i>Packets Seen</i>	packets received on Ethernet interface
<i>Packets Forwarded</i>	packets forwarded from Ethernet interface to other interfaces
<i>Discarded/NoMatch</i>	packets discarded because of unknown destinations (destinations not in the known list of database entries)
<i>Discarded/Forced</i>	packets discarded because of the applied address filters
<i>Discarded/Buffer</i>	packets discarded because insufficient buffers in AP
<i>Discarded/CRC</i>	packets discarded because of data errors
<i>Broadcast/Multicast</i>	total broadcast or multicast packets received
<i>Individual Address</i>	packets received with designated individual addresses
<i>Packets Sent</i>	total packets sent out
<i>Any Collision</i>	packets affected by at least one collision
<i>1 + Collisions</i>	packets affected by more than one collision
<i>Maximum Collisions</i>	packets affected by the maximum number of collision
<i>Late Collisions</i>	collisions occurring after the first 64 bytes
<i>Defers</i>	the times the AP had to defer transmit requests on the Ethernet because of a busy medium

- Select `Refresh` at the status display to update values manually.
- Select `Timed` to automatically update this display every two seconds.
- Press `ESC` to return to the previous menu.

## 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	∅	Data Pkts Rcvd 494
Data Bytes Sent	∅	Data Bytes Rcvd 36524
BC/MC Packets Sent	28	BC/MC Packets Rcvd 23
BC/MC Bytes Sent	29∅4	BC/MC Bytes Rcvd ∅
Sys Packets Sent	5	Sys Packets Rcvd ∅
SBC/MC Packets Sent	1412∅	SBC/MC Packets Rcvd 52∅
Succ Frag Packets	∅	Succ Reass Packets ∅
UnSucc Frag Packets	∅	UnSucc Reass Packets ∅
Fragments Sent	∅	Fragments Rcvd ∅
Packets w/o Retries	∅	Rcv Duplicate Pkts ∅
Packets w/ Retries	∅	Undecryptable Pkts ∅
Packets w/ Max Retries	∅	
Total Retries	∅	Rcv CRC Errors 54
		Rcv ICV Errors ∅
	Refresh-[F1]	Timed-[F2]
		WLAP-[F3]
		Exit-[ESC]



---

Radio performance statistics include:

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

<i>Fragments Rcvd</i>	packet fragments received
<i>Rcv Duplicate Pkts</i>	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.
<i>Undecryptable Pkts</i>	total data packets that could not be decrypted
<i>Rcv CRC Errors</i>	Packets received that contained CRC ( <i>Cyclic Redundancy Check</i> ) 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.
<i>Rcv ICV Errors</i>	Packets received containing ICV ( <i>Identity Check Value</i> ) 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.

- Select `Refresh` at the status display to update the values manually.
- Select `Timed` to automatically update this display every two seconds.
- Press `ESC` to return to the previous menu.

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

```

Symbol Access Point          WLAP RF Statistics

Current # WLAP  Itf  1          Root Interface      1
Current State   Functional      Root Priority        1000 hex
Priority         8000 hex          Root MAC Addr       00:A0:F8:8A:30:77
                  Root Path Cost      1

```

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

Itf ID	WLAP Itf MAC Addr	Itf State	Path Cost	Designated Root ID	Designated Cost	Designated WLAP ID	Designated Itf ID
8001	00:A0:F8:8A:30:77	FWD	1	100000a0f88a3077	0	800000a0f88a3077	8001
8002	00:00:00:00:00:00	DIS	1	800000a0f88b7221	0	800000a0f88b7221	8002
8003	00:00:00:00:00:00	DIS	1	800000a0f88b7221	0	800000a0f88b7221	8003
8004	00:00:00:00:00:00	DIS	1	800000a0f88b7221	0	800000a0f88b7221	8004

Refresh-[F1]    Timed-[F2]                    Previous-[F4]    Exit-[ESC]

Where:

<i>Current # WLAP If</i>	Refers to the current Wireless AP interfaces in use in a 1 - 4 range.
<i>Current State</i>	<p>On initialization, the AP can be in any of the following states of wireless operation:</p> <ul style="list-style-type: none"> <li>• starting the initializing process: <ul style="list-style-type: none"> <li>– Initializing</li> <li>– Sending Probe</li> <li>– <i>Send Assoc Req</i> (association request)</li> <li>– <i>Send Cfg BPDU</i> (<i>configuration Bridge Protocol Data Unit</i>)</li> <li>– Wait for Probe</li> <li>– <i>Send Probe Rsp</i> (probe response)</li> <li>– <i>Send Assoc Rsp</i> (association response)</li> <li>– <i>Send Cfg Rsp</i> (configuration response)</li> <li>– <i>Received Root Rsp</i> (Root response)</li> </ul> </li> <li>• operating in wireless mode: <ul style="list-style-type: none"> <li>– Root WLAP lost</li> <li>– Disabled</li> <li>– Functional</li> </ul> </li> </ul> <p>The <i>1.2.2 Cellular Coverage</i> on page 8 provides an explanation of a Root AP.</p>
<i>Priority</i>	States the WLAP priority value assigned to the AP under <i>2.5 Configuring Radio Parameters</i> on page 58.
<i>Root Interface</i>	States the interface leading to the Root AP.
<i>Root Priority</i>	States the priority value of the Root AP.
<i>Root MAC Address</i>	States the MAC address of the Root AP.
<i>Root Path Cost</i>	Indicates the hops between the current WLAP and the Root AP.

<i>lth ID</i>	Identifies the wireless interface the AP uses to communicate with another device.
<i>WLAP lth MAC Addr</i>	States the MAC address of the associated WLAP.
<i>lth State</i>	Identifies the state of the interface from: <ul style="list-style-type: none"><li>• <i>DIS</i> - the interface is disabled</li><li>• <i>LIS</i> - the AP listens for information</li><li>• <i>LRN</i> - the AP learns the information</li><li>• <i>FWD</i> - the AP forwards data</li><li>• <i>BLK</i> - the AP blocks transmission.</li></ul>
<i>Path Cost</i>	An abstract unit added to the <i>Root Path Cost</i> field in the <i>Config BPDU</i> received on this interface. The unit represents a hop on the path to the Root AP.
<i>Designated Root ID</i>	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.
<i>Designated Cost</i>	A path cost designated by the Root AP.
<i>Designated WLAP ID</i>	A WLAP ID assigned by the Root AP.
<i>Designated lth ID</i>	An lth ID assigned by the Root AP. <ul style="list-style-type: none"><li>– Select <i>Refresh</i> at the status display to update the values manually.</li><li>– Select <i>Timed</i> to automatically update this display every two seconds.</li><li>– Press <i>ESC</i> to return to the previous menu.</li></ul>

### 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
Echoes                             Ø          Number of Dialouts    Ø
Pings                               Ø          Dialout Failures     Ø
Passthrough Echoes                 Ø          Number of Answers     Ø
                                          Current Call Time     Ø
SNMP                               Last Call Time       Ø
Requests                           Ø
Traps                              Ø
Filters
ACL Violations                     Ø
Address                             Ø
type                                Ø
                                          Mobile IP
                                          Agent Ad Sent        Ø
                                          Reg. Request Rcvd   Ø
                                          Reg. Reply Sent      Ø
Per Channel Statistics
Retry Histogram

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

```

WNMP statistics include:

*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 include:

<i>Requests</i>	configuration requests received from the SNMP manager
<i>Traps</i>	AP messages sent to the SNMP manager

Filter statistics include:

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

Modem statistics for the serial port include:

<i>Number of Dialouts</i>	dial-out attempts by the AP
<i>Dialout Failures</i>	dial-out failures by the AP
<i>Number of Answers</i>	answer attempts by the AP
<i>Current Call Time</i>	current connection session length in seconds
<i>Last Call Time</i>	last connection session length in seconds

Mobile IP statistics include:

<i>Agent Ad Sent</i>	number of agent advertisements sent from the AP
<i>Reg Request Received</i>	number of Mobile IP registration requests received
<i>Reg Reply Sent</i>	number of Mobile IP registration replies sent

- Select `Refresh` at the status display to update values manually.
- Select `Timed` to automatically update this display every two seconds.
- Press `ESC` to return to the previous menu.

### 3.9.1 Analyzing Channel Use

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

To view statistics for individual channels:

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

Chnl.	Sent	Rcvd	Retry
=====	=====	=====	=====
1:	Ø	Ø	Ø
2:	Ø	Ø	Ø
3:	88	89	3
4:	Ø	Ø	Ø
5:	Ø	Ø	Ø
6:	Ø	Ø	Ø
7:	Ø	Ø	Ø
8:	Ø	Ø	Ø
9:	Ø	Ø	Ø
10:	Ø	Ø	Ø
11:	Ø	Ø	Ø

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.



### 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 suspend transmitting and retry later. 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 tracks 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.

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.

```

0:07:44 MU Assoc 00:A0:F8:12:59:C3
0:06:42 Telnet Session Start From 111.111.12.169
0:06:00 Telnet Session End
0:01:51 MU Assoc 00:A0:F8:12:59:E8
0:01:38 MU Assoc 00:A0:F8:12:59:9B
0:01:38 MU Assoc 00:A0:F8:12:5A:05
0:00:42 Telnet Session Start From 111.111.12.169
0:00:10 WLAP Assoc 00:A0:F8:8A:30:77
0:00:10 MU Assoc 00:A0:F8:12:59:C3
0:00:02 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]

## 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.



Resetting the AP also clears statistics.

---



## Chapter 4 **Hardware Installation**

---

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

### 4.1 **Precautions**

Before installing the AP verify the following:

- 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



Contact the Symbol Support Center to report missing or improperly functioning items.

---

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:

- a power outlet
- an AP 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.



Test and use the radio network with an MU.

---

### 4.3.1 Network Connection

Locate connectors for Ethernet 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.



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

---

### 4.3.2 10Base-T UTP

Use a 10Base-T connection for 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).

### 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 Placing the AP

AP 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 AP placement (like even placement of a light bulb) provides even, efficient coverage.

Place an AP using the following guidelines:

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

The AP-4121 HR dual antenna assembly provides diversity that can improve performance and signal reception.

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

## 4.5 Power Options

- Standard 24 volt, 1 amp power supply 115/230VAC, 50/60Hz. Part Number: 50-24000-024
- US line cord Part Number: 23844-00-00



A Symbol BIAS-T system can also be used to combine low-voltage DC with Ethernet data in a single cable connecting to an access point. For information on the BIAS-T system, go to ([www.symbol.com](http://www.symbol.com)) and search for the BIAS-T low power distribution system.

---

## 4.6 Mounting the AP

The AP rests on a flat surface or attaches to a wall, or any hard, flat, stable surface. Use the standard-mounting kit provided with the Spectrum24 AP-4121 HR access point.

Choose one of the options based on environment

- |                              |   |
|------------------------------|---|
| <i>Resting flat</i>          | Rests on the four rubber pads on the underside of the AP. Place on a surface clear of debris and away from traffic. |
| <i>Attaching on the wall</i> | 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.

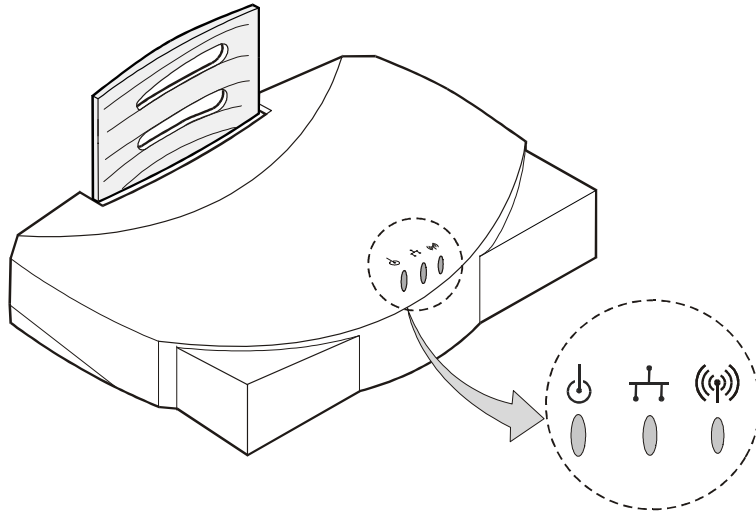
1. Verify the power adapter is correct according to the country.
2. Plug the power adapter cable into the socket at the back of the AP.
3. Plug the adapter into an outlet. The AP is functional when the Status indicator on the front of the AP reaches a consistent flashing and the *Wireless LAN Activity* 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, and other activity. The indicators are:



*Power*

Flashing indicates AP initialization.  
Steady Green during operation.



*Wired LAN Activity*

Flashing indicates data transfers on  
wired connection.



*Wireless LAN Activity*

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 2.00-02 or above only.

1. After power up, system initialization begins:

<b>LED</b>	<b>State</b>
<i>Status</i>	Blinks
<i>Wired LAN Activity</i>	Blinks if activity occurs
<i>Wireless LAN Activity</i>	Off

2. When a WLAP begins a full scan:

<b>LED</b>	<b>State</b>
<i>Status</i>	On
<i>Wired LAN Activity</i>	Off
<i>Wireless LAN Activity</i>	Blinks slowly

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

<b>LED</b>	<b>State</b>
<i>Status</i>	On
<i>Wired LAN Activity</i>	Off
<i>Wireless LAN Activity</i>	Blinks slowly

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

<b>LED</b>	<b>State</b>
<i>Status</i>	Blinks regularly
<i>Wired LAN Activity</i>	Blinks if activity occurs
<i>Wireless LAN Activity</i>	Blinks slowly

5. When all WLAP connections are in Forward state:

LED	State
<i>Status</i>	Blinks regularly
<i>Wired LAN Activity</i>	Blinks if activity occurs
<i>Wireless LAN Activity</i>	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
<i>Status</i>	On
<i>Wired LAN Activity</i>	Off
<i>Wireless LAN Activity</i>	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 Ethernet Timeout in the System Configuration menu is set to 3, the WLAP will keep track of the WLAP Alive BPDU. If the BPDU is missing for *WLAP Hello Time* seconds, the WLAP state changes to *WLAP Lost on Ethernet* and the LEDs have the following states:

LED	State
<i>Status</i>	On
<i>Wired LAN Activity</i>	Blinks slowly
<i>Wireless LAN Activity</i>	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, the LEDs turn on. If the test fails, the LEDs all turn off and the AP resets. The LEDs turn off sequentially as each test passes.

Identify wired network problems:

1. No operation:
  - Verify AP configuration through 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.
2. AP powered on but has no connection to the wired network:
  - Check connections for proper wiring.
3. 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 (ESS).
  - Check that the radio driver loaded properly.
  - Check that the MU PROTOCOL.INI or NET.CFG file is compatible with the network operating system.
4. Slow or erratic performance:
- Check MU and RF communications range.
  - Check antenna, connectors and cabling.
  - Verify that antenna diversity setting for AP is appropriate. If using one antenna, the setting is *Primary Only*, if using both 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 (ESS) and other configuration parameters until network connection verification.



# Appendix A

## Specifications

---

### A.1 Physical Characteristics

<i>Dimensions</i>	1.75" H x 6" L x 8.5" W (4.45" cm H x 15.24" cm L x 21.59" cm W)
<i>Weight</i> (w/power supply)	1 lbs. (0.454 kg)
<i>Operating Temperature</i>	-4° F to 131° F (-20° C to 55° C)
<i>Storage Temperature</i>	-40° F to 149° F (-40° C to 65° C)
<i>Humidity</i>	10% to 95% noncondensing
<i>Shock</i>	40 G, 11 ms, half-sine
<i>ESD</i>	meets CE-Mark
<i>Drop</i>	withstands up to a 30 in. (76 cm) drop to concrete with possible surface marring

---

## A.2 Radio Characteristics

*Frequency Range* country dependent; within 2400 MHz to 2500 MHz

<i>Frequency</i>	<i>Allowed Channel Range</i>	<i>Country</i>
2412-2470	1-11	United States
2430-2447	5-8	Israel
2457-2463	10-11	Spain
2458-2472	10-13	France
2483-2485	14	Japan

<i>Radio Data Rate</i>	<ul style="list-style-type: none"><li>• 11 Mbps -- Optional</li><li>• 5.5 Mbps -- Optional</li><li>• 2 Mbps -- Optional</li><li>• 1 Mbps -- Required</li></ul>
------------------------	--

*11 Mbps Range* open environment - over 100 ft. typical office or retail environment - 30 to 50 ft.

*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

<i>Driver Support</i>	NDIS v4.0 and v5.0
<i>Ethernet Frame</i>	DIX, Ethernet_II and IEEE 802.3
<i>Filtering Packet Rate</i>	14,400 frames per second filtering and forwarding
<i>Ethernet Connection</i>	10Base-T (RJ-45)
<i>Serial</i>	PC/AT serial port - DB9 Male, RS-232 using a DTE termination, 19200 bps
<i>SNMP</i>	Version 1, Version 2 subset, Symbol MIB, 802.11 MIB and MIB-II



## Appendix B

# Supported Modems

---

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-4121 HR access point:

- US Robotics Faxmodem v.90.56K
- US Robotics Faxmodem v.33.6K
- US Robotics Faxmodem v.34 and v.32 bis Sportster 28.8K
- Diamond Supra Express 56K



## 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

## Symbol Developer Program Web Site

<http://sdp.symbol.com>

## 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:

- Reorient 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 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 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.



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:



---

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.

# Index

---

## Numerics

- 10Base-T connection 134
- 10Base-T unshielded twisted pair 134
- 10Base-T UTP 134

## A

- access control 13
  - disallowed address 13
  - MU 13
  - unauthorized access 13
- Access Control List 13
- Access Point 1
  - 10Base-T connection 134
  - access control 108
  - Access Control List 1
  - adding allowed MUs 86
  - adding disallowed MUs 89
  - advanced radio theory 12
  - analyzing retries 129
  - antenna selection 108
  - ARP request packet 13
  - ARP response packet 13
  - Basic Service Set 8
  - bridging 16
  - BSS\_ID 8
  - CAM 26
  - cell 8
  - cellular coverage 8
  - Characteristics A-1
  - chipping sequence 20
  - clear statistics 131
  - clearing MUs 90
  - clearing statistics 131
  - configure 24
  - country code 108
  - data encryption 2
  - data rate 1
  - decryption 27
  - dial-up access 31
  - direct-sequence 21
  - disallowed address 13
  - encryption 27
  - Ethernet device 3
  - Ethernet statistics 118
  - Ethernet traffic 1
  - Ethernet wired LANs 1
  - event history 130
  - Extended Service Set 8
  - features 2
  - filtering 14
  - firmware version 109
  - foreign agent 112, 116
  - forwarding counts 111
  - hardware installation 133
  - hardware version 109
  - home agent 116
  - HTML 28
  - HTTP 28
  - IEEE 802.11 8
  - interface 110
  - interface statistics 110
  - Internet Protocol Control Protocol 17
  - Introduction 1
  - known APs 117
  - LED indicators 137

---

MAC address 12  
management options 29  
manually updating the firmware 93  
media types 15  
miscellaneous statistics 126  
Mobile IP 24  
model number 109  
monitoring statistics 107  
mounting 136  
Net\_ID 8  
network connection 134  
power adapter 136  
power options 135  
PPP interface 77  
PPP timeout 78  
PSP 26  
Radio Characteristics A-2  
radio performance statistics 120  
removing allowed MUs 86  
removing disallowed MUs 89  
RF statistics 120  
roaming across routers 24  
RSSI 23  
serial port 48  
shared key authentication 28  
single-cell connection 135  
site survey 11  
site topography 10  
SNMP management 29  
Supported Modems B-1  
system password 46  
system summary 107  
TCP/IP 37  
Telnet 33  
topologies 4  
troubleshooting 140  
type filtering option 14  
UI 31  
Web browser 37  
wired network 140  
WNMP statistics 126

ACL 84  
adding allowed MUs 86  
configuring 84  
disallowed address 13  
enable/disable 87  
filtering 14  
load ACL from MU list 87  
removing allowed MUs 86  
unauthorized access 13

address filtering 88  
configuration 90  
disallowed addresses 88  
MAC addresses 88  
remove MUs 89

advanced radio theory 12  
MAC layer bridging 12

analyzing retries 129

antenna 135  
antenna options 135  
AP placement 135  
site survey 134

AP  
Bridge Protocol Data Unit 9  
DTIM 9  
IEEE 802.1d Spanning Tree support 10  
radio parameters 7  
repeater 6  
TIM 9  
wireless operation parameters 64  
WLAP mode 6, 9, 109  
WLAP mode LED display 138

---

- WLAP priority value 10
- WNMP function 7
- AP installation 50
  - additional gateways 51
  - antenna selection 51
  - gateway IP address 50
  - IP address 50
  - Net\_ID 51
  - subnet mask 51
- association process 21
  - beacon 26
  - Bridge Protocol Data Unit 9
  - CCA 22
  - direct-sequence systems 20
  - DTIM 9, 26
  - IEEE 802.1d Spanning Tree support 10
  - MU 21
  - MU ACK 22
  - roaming 21
  - root AP 9
  - RSSI 23
  - scanning 22
  - TIM 9
  - WLAP mode 9
  - WLAP priority value 10
- auto fallback to wireless mode
  - enabling 14
  - introduction 14

## **B**

- Basic Service Set 8
- BC/MC Q configuration 59
- beacon 26
  - CAM stations 26
  - PSP stations 26
  - TIM 27

- bridge
  - WLAP mode 6
- bridging 16
  - data-link bridge 16
  - Ethernet topologies 17
  - IP 17
  - Link Control Protocol 18
  - Network Control Protocol 18
  - PPP 17
  - radio coverage 16
  - TCP/IP 17
  - telnet 17
- bridging architecture 1
- broadcast ESS ID 60
- BSS\_ID 8

## **C**

- carrier signal 3
- configuration 33
  - ACL 84
    - address filtering 88
  - BC/MC Q 59
  - beacon interval 60
  - broadcast ESSID 60
  - data transmission rate 61
  - dial-up connection 48
  - dial-up system 49
  - DTIM packet frequency 59
  - Encryption Key Maintenance 69
  - manually updating AP firmware 93
  - maximum retries 59
  - Mobile IP 116
  - MU 60
  - multicast mask 59
  - PPP 76
  - PPP Direct 76

- 
- radio parameters 7, 58
  - resetting 106
  - restoring 106
  - saving 104
  - serial port connection 48
  - Setting Logging Options 91
  - SNMP agent 80
  - Special Functions 105
  - Strong Encryption 74
  - system parameters 52
  - System Password Administration 56
  - TCP/IP 33
  - Telnet 33
  - UI 33
  - wireless operation parameters 64
  - WLAP forward delay 68
  - WLAP hello time 67
  - WLAP manual BSS ID 67
  - WLAP Max Age 67
  - WLAP mode 66
  - WLAP priority 66
  - configuring ACL 84
    - range of MUs 84
    - removing allowed MUs 86
  - configuring PPP 76
    - answering AP 78
    - establishing connection 77
    - initiating modem connection 79
    - originating AP 77
    - PPP Direct 76
    - PPP with modems 77
  - configuring SNMP agent
    - WLAP connection change 83
  - configuring the SNMP agent 80
    - access cntl violation 82
    - all traps 82
    - authentication failure 82
    - cold boot 82
    - DHCP change 83
    - radio restart 82
    - read/write community 82
    - read-only community 82
    - SNMP agent mode 82
    - trap host1 IP address 82
  - connecting power adapter 136
  - country code 53
  - coverage area 8
    - AP 8
    - Basic Service Set 8
    - BSS\_ID 8
    - cell 8
    - MU 8
    - WLAP mode 6
  - customer support C-1
    - additional information C-2
    - international contacts C-2
    - North American contacts C-1
- ## D
- data decryption 27
    - types of authentication 28
    - WEP algorithm 27
  - data encryption 27
    - AP 28
    - types of authentication 28
    - WEP algorithm 27
  - Delivery Traffic Indicator Map. See DTIM
  - DHCP Support
    - AP 14
    - Mobile IP 15
  - DHCP support 14
  - dial-up connection
    - configuration 48
-



- 
- digital data 3
  - disallowed address 13
    - access control 13
    - ACL 13
    - AP 13
  - disallowed MUs 89
  - DTIM
    - AP 9
    - association process 9
    - root AP 9
  - E**
  - electromagnetic waves 3
  - encryption 27
    - 128 Bit 72
    - 40 Bit 71
    - enable strong encryption 74
  - environment 3
  - ESSID 60
  - Ethernet interface 15
  - ethernet statistics 118
  - Ethernet wired LAN 1
  - F**
  - features 2
    - 10baseT Ethernet port interface 2
    - built-in diagnostics 2
    - built-in dual antenna assembly 2
    - DHCP support 2
    - HTTP Web server support 2
    - increased MIB support 2
    - Mobile IP support 2
    - PC/AT serial port interface 2
    - power supply IEC connector 2
    - short RF preamble 2
    - SNMP support 2
    - support for up to 127 MUs 2
    - upgradable firmware 2
    - wireless AP 2
    - wireless MAC interface 2
  - filtering
    - ACL 13
    - introduction 13
  - firmware 93
    - auto upgrade all APs via messaging 98
    - manually updating 93
    - update using TFTP 93
    - updating using Xmodem 96
  - firmware version 109
  - frequency 3
  - frequency modulation 3
  - frequency range 3
  - G**
  - gigahertz 1
  - H**
  - hardware installation 133
    - 10Base-T 134
    - antenna 135
    - antenna coverage 135
    - dual antenna assembly 135
    - mounting the AP 136
    - network connection 134
    - package contents 133
    - power adapter 136
    - power options 135
    - precautions 133
    - single-cell connection 135
    - site survey 134
  - Help 37
  - Help file
    - network Web server 37
-

- 
- I**
  - ICMP 101
  - IEEE 802.1d Spanning Tree support
    - association process 10
    - LAN 10
  - IEEE address 3
    - MAC 3
  - IP 17
    - bridging 17
    - forwarding address 24
    - roaming across routers 24
  - IP Address 112
    - AP 112
    - MU 112
  - K**
  - known APs 117
    - MAC and IP addresses 117
    - statistics 117
  - L**
  - LAN
    - IEEE 802.1d Spanning Tree support 10
  - LED indicators 137
    - description 137
    - flashing all LEDs 109
    - special cases 138, 139
    - WLAP mode LED display 138
  - M**
  - MAC Layer Bridging 12
    - address database 12
    - MAC address 12
  - management options 29
    - SNMP 29
    - Telnet 29
    - WLAN 29
  - miscellaneous statistics 126
  - Mobile IP 23
    - configuration 104
    - foreign agent 24, 116
    - mapping 116
    - roaming across routers 24
    - using MD5 authentication 104
  - Model Number 109
  - monitoring statistics 107
    - ethernet statistics 118
    - interface statistics 110
    - miscellaneous statistics 126
    - radio statistics 120
  - MU 8
    - access control 13
    - ACL 13
    - association process 25
    - authentication 28
    - CAM 26
    - carrier signal 3
    - cellular coverage 8
    - clearing MUs from the AP 90
    - current transmit rate 115
    - data decryption 27
    - data encryption 27
    - DTIM 27
    - filtering 13
    - home agent 25
    - known APs 117
    - Mobile IP 23, 116
    - performing pings 101
    - power mode 114
    - priority 115
    - scanning 25
    - security 27

---

- statistics 112
- supported rates 115
- MU association process 21
- multiple APs 5

## **N**

- network topology 3

## **P**

- PPP 16
  - implementation 18
  - interface 16
  - link 17
  - mode 17
- programmable SNMP trap 29
  - management stations 29
  - MIB 29
  - SNMP agent 29
- PSP stations 26
  - beacon 26
  - MU 26

## **R**

- radio basics 3
  - carrier signal 3
  - center frequency 3
  - digital data 3
  - electromagnetic waves 3
  - environment 3
  - ethernet device 3
  - IEEE address 3
  - MAC 3
  - radio links 3
  - receiving antenna 3
  - wireless network 4
- radio interface 15

- radio parameters 58
  - AP 7, 58
  - BC/MC Q maximum 59
  - beacon interval 60
  - broadcast ESS 60
  - CCA Mode 61
  - configuration 7
  - configure 58
  - data transmission rate 61
  - DTIM interval 59
  - Enable Strong Encryption 62
  - Encryption Key ID 62
  - Encryption Key Maintenance 62
  - max retries 59
  - multicast mask 59
  - RTS threshold 61
  - Short RF Preamble 63
  - WEP (Privacy) 61
  - WEP Algorithm 62
- radio performance statistics 121
  - packets reassembled 121
  - packets received 121
  - packets transmitted 121
  - retries 121
- radio statistics 120
  - AP 120
  - viewing 120
- rate control 61
- repeater
  - AP 6
    - coverage area 6
    - WLAP mode 6
- roaming across routers 24
  - AP 25
    - home agent 25
    - IP address 24

---

- Mobile IP 23
- MU 25
- TIM 26
- root AP
  - association process 9
  - Bridge Protocol Data Unit 9
  - DTIM 9
  - TIM 9
  - WLAP mode 9

## S

- security 27
  - decryption 27
  - encryption 27
  - WEP algorithm 27
- Site 11
- site survey 11
  - antenna coverage 135
  - AP 135
  - floor plan 11
  - hardware installation 133
- site topography 10
  - AP 10
  - MU 10
  - signal loss 10
- SNMP 29
  - agent 29
  - configuration 29
  - support 30
  - trap 29
- Spectrum24 1
  - introduction 1
  - management options 29
  - network topologies 3
  - radio basics 3
  - regulatory requirements 2

- wireless network 1
- spread spectrum
  - 2.4GHz 1
  - 2.5GHz 1
- statistics 107
  - ethernet 118
  - filter 127
  - forwarding counts 111
  - interface statistics 110
  - IP address 118
  - known APs 117
  - Mobile IP 116
  - modem 127
  - RF Statistics 120
  - SNMP 127
  - WNMP 126
- Strong Encryption 74
- system parameters 52
  - access control 54
  - Admin Password 57
  - configuration 53
  - Encryption Admin 54
  - Ethernet timeout 53
  - MD5 key 54
  - System Password Admin 54
  - Telnet logins 53
  - type filtering 54
  - User Password 57
  - Web Server 54
  - WNMP functions 55
- system password 42
- system summary 107
  - access control 108
  - antenna selection 108
  - country code 108
  - current MUs 108

---

- firmware version 109
- IP address 108
- MAC address 108
- model number 109
- Net\_ID 108
- serial number 109
- WLAP mode 109

## T

### TIM

- association process 9
- root AP 9

Traffic Indicator Message. See TIM

transmission medium 3

troubleshooting 140

- AP does not power up 140
- no connection 140
- slow or erratic performance 141
- SRAM test 140
- wired network operation 140
- wired network problems 140

## U

### UI 33

- access 33
- changing access 46
- configuration 33
- dial-up access 31
- dial-up connection 36
- direct serial access 31
- hanging up 49
- navigation 43
- password 33
- Telnet 31
- Usage 31
- Web browser 31

## W

Web browser 37

WEP algorithm 27

WEP privacy 61

wireless operation parameters

- configuration 64

- IEEE 802.1d Spanning Tree Protocol 64

- WLAP forward delay 68

- WLAP hello time 67

- WLAP interfaces 64

- WLAP manual BSS ID 67

- WLAP Max Age 67

- WLAP mode 66

- WLAP priority 66

WLAP

- priority value 10

WLAP forward delay  
configuration 68

WLAP hello time  
configuration 67

WLAP manual BSS ID  
configuration 67

WLAP Max Age  
configuration 67

WLAP mode

- AP 6

- association process 9

- bridge 6

- configuration 66

- repeater 6

- root AP 9

- system summary 109

WLAP mode LED display  
special cases 139

WLAP priority  
configuration 66

---

WNMP function  
AP 7

**X**  
Xmodem 96