Intel® PRO/Wireless 2011B LAN

Access Point Product Reference Guide

Product Model

Intel® PRO/Wireless 2011B LAN Access Point product model: WEAP2011BWW

Copyright

Intel Corporation, 5200 N.E. Elam Young Parkway, Hillsboro, OR 97124-6497

Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

Intel® PRO/Wireless 2011B LAN is a registered trademark of Intel Corporation.

†Other product and corporate names mentioned herein may be trademarks of other companies are are used only for explanation and to the owners' benefit, without intent to infringe.

Patents

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

U.S. Patent No.

4,360,798; 4,369,361; 4,387,297; 4,460,120; 4,496,831; 4,593,186; 4,603,262; 4,607,156; 4,652,750; 4,673,805; 4,736,095; 4,758,717; 4,816,660;
4,845,350; 4,896,026; 4,897,532; 4,923,281; 4,933,538; 4,992,717; 5,015,833; 5,017,765; 5,021,641; 5,029,183; 5,047,617; 5,103,461; 5,113,445;
5,130,520; 5,140,144; 5,142,550; 5,149,950; 5,157,687; 5,168,148; 5,168,149; 5,180,904; 5,216,232; 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; 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

Invention No. 55,358; 62,539; 69,060; 69,187 (Taiwan); No. 1,601,796; 1,907,875; 1,955,269 (Japan);
European Patent 367,298; 367,299; 367,300; 414,281; UK 2,072,832; France 81/03938; Italy 1,138,713

A61429-001

About This Document

Reference Documents

This reference guide refers to the following documents:

Part Number	**Document Title**
A61406-001	*Late Breaking News*
A61411-001	Intel® PRO/Wireless 2011B LAN *Access Point Quick InstallationGuide*
A61426-001	Intel® PRO/Wireless 2011B LAN *Site Survey AdministratorsGuide*
A61428-001	Intel® PRO/Wireless 2011B LAN *Adapter Product Reference Guide*
A61437-001	Intel® PRO/Wireless 2011B LAN *Power Injector Quick Reference Guide*
A61481-001	Intel® PRO/Wireless 2011B LAN *Regulatory Approval Guide*
A63056-001	Intel® PRO/Wireless 2011B LAN *Adapter Quick Reference 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 con**a**ventions 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.
Italics	indicates the first use of a term, book title, variable or menu title.
Bold	indicates important user information, license provisions or warranty conditions.
`Screen dialog`	indicates screen dialog and user input options, and the exact syntax of items.
`Screen text`	indicates text and data displayed in an application screen on a computer monitor.
`Terminal text`	indicates text shown in a radio terminal LCD screen.
URL	indicates a Uniform Resource Locator, such as a Web page address.

This document uses the following for certain conditions or information:

Note

indicates tips or special requirements.

Caution

indicates conditions that can cause equipment damage or data loss.

Warning

indicates a potentially dangerous condition or procedure that only Intel® PRO/Wireless 2011B LAN-trained personnel should attempt to correct or perform.

Contents

Chapter 1. Introduction to Wireless Networking

The Intel® PRO/Wireless 2011B LAN Access Point is an Intel® PRO/Wireless 2011B LAN network product. Intel® PRO/Wireless 2011B LAN network products are based on the IEEE 802.11b standard and connect computers together to form a wireless network.

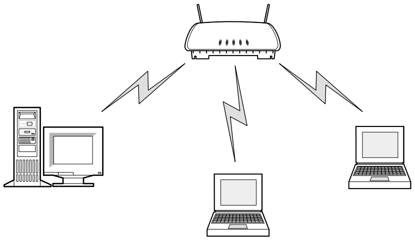
A Local Area Network (LAN) is a network in a central location. Users at that location share files, printers, and other services. In a LAN, a networked computers that request services are called clients, while servers in a LAN provide services. In a wireless LAN (WLAN), wireless adapters are installed in clients. A wireless client communicates with the WLAN without cables. Instead, wireless clients send and receive information through the air.

All Intel 802.11b compliant devices interoperate with other 802.11b compliant wireless devices from other vendors. The **WiFi** certification logo indicates that the wireless device has been tested by an independent organization and is 802.11b compliant.

A wireless client operates in either infrastructure mode or peer-to-peer mode.

1.1 Infrastructure Mode: A WLAN with Access Points

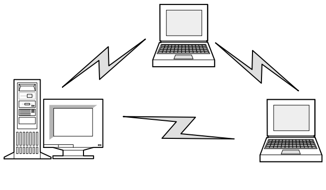
In infrastructure mode, wireless clients send and receive information through access points. When a wireless client communicates with another, it transmits to the access point. The access point receives the information and rebroadcasts it. Then the other device receives the information.



Access points are strategically located within an area to provide optimal coverage for wireless clients. A large WLAN uses multiple access points to provide coverage over a wide area. Access points can connect to a LAN through a wired Ethernet connection. Access points send and receive information from the LAN through this wired connection.

1.2 Peer-to-Peer Mode: A WLAN without Access Points

In peer-to-peer mode, also called Ad Hoc Mode, wireless clients send and receive information to other wireless clients without using an access point. In contrast to infrastructure mode, this type of WLAN only contains wireless clients.



You can use peer-to-peer mode to network computers in a home or small office, or to set up a temporary wireless network for a meeting.

1.3 Identifying a WLAN

All the devices on a WLAN use a Network Name, or Service Set Identifier (SSID) to identify the WLAN. There are several kinds of SSIDs, each having a slightly different meaning. In peer-to-peer mode, an Independent Basic Service Set Identifier (IBSSID) identifies a WLAN. In infrastructure mode, an Extended Service Set Identifier (ESSID) identifies a WLAN. For simplicity, this guide uses the term Network Name (SSID) in place of ESSID and IBSSID. Regardless of whether you are dealing with a infrastructure of peer-to-peer WLAN, the SSID indicates what WLAN you are communicating with. All the devices on a WLAN must use the same SSID to communicate with other wireless devices. When installing an access point or wireless adapter in a wireless client, the software asks you to specify an SSID.

1.4 Identifying Devices on a WLAN

A Basic Service Set Identifier (BSSID) uniquely defines each wireless device. The BSSID is the Ethernet Media Access Control (MAC) address of the wireless adapter installed in the wireless client. The MAC address is permanently set when the adapter is manufactured. 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:

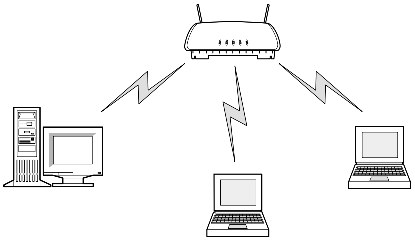
```
00:A0:F8:24:9A:C8
```

To view the MAC address of an Intel® PRO/Wireless 2011B LAN device, see the bottom of the device.

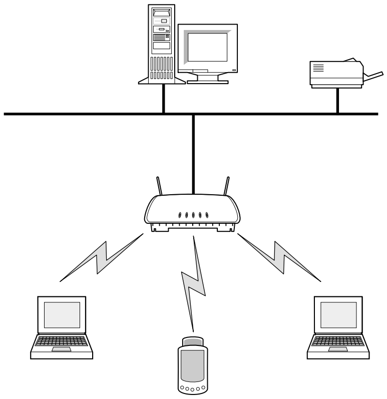
1.5 Wireless Network Options

You can use Intel® PRO/Wireless 2011B LAN Access Points in any of several network configurations depending on your networking needs and size. The following illustrations show simple wireless network configurations with access points:

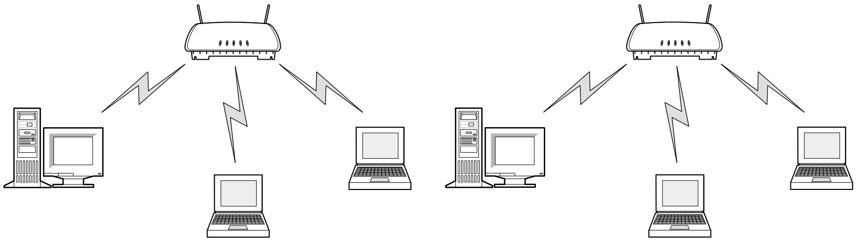
- A single access point forms a single-cell wireless network.



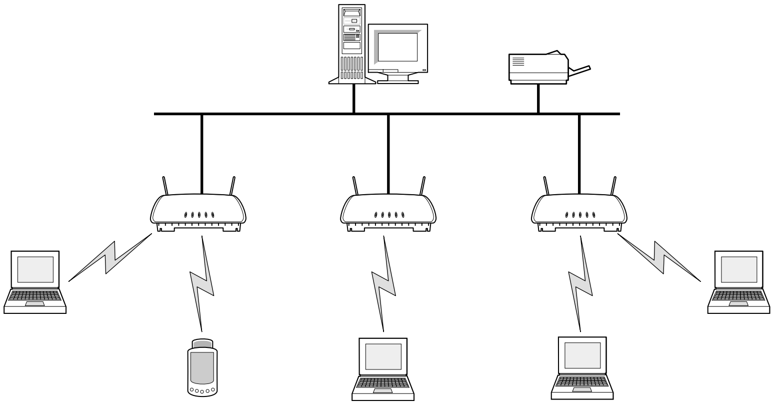
- A single access point can bridge between the Ethernet and wireless networks.



- Multiple access points can coexist as separate, individual networks at the same site using different network names (SSID). These separate wireless LANs can be configured to use different channel assignments to avoid RF interference.

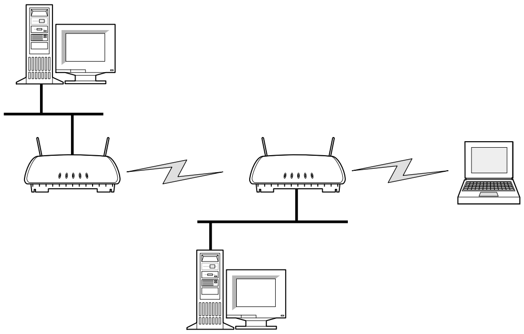


- Multiple access points wired together provide a network with a better coverage area and performance when using the same Network Names.

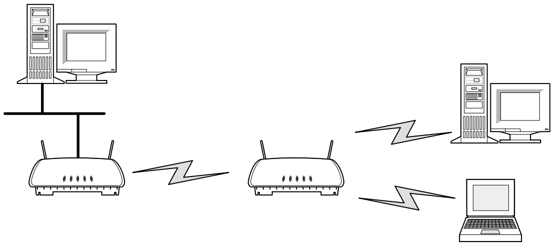


The following illustrations show possible options for access points operating in WLAP mode. In WLAP mode, an access point forwards data to another access point using the wireless connection rather than Ethernet cabling.

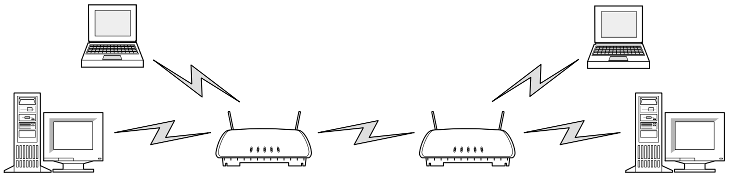
- Access points can bridge between two Ethernet networks.



- An access point can operate as a repeater to extend coverage area without additional network cabling.



- Multiple access points can form a stand-alone wireless network. Each access point can have connections with up to four other access points.



1.6 Wireless Security

Wireless networking devices transmit information through the air. Without implementing security, it is easy for an unauthorized person to intercept the information.

A common way of implementing security and protecting information is encryption. Before sending information, the wireless client or access point encrypts or scrambles information using an encryption key. The device receiving the information uses the same key to decrypt or unscramble the information. The information is only readable to wireless devices that have the correct encryption key.

The IEEE 802.11 wireless LAN standard specifies the Wired Equivalent Privacy (WEP) encryption and decryption algorithm. The standard includes two levels of security, using a 40-bit key or a 128-bit key. To implement WEP, use either one of these methods. For better security, use a 128-bit key. A 128-bit key has several trillion times as many possible combinations as a 40-bit key. For added security, change your keys often. Some vendors refer to 40-bit encryption as 64-bit. These are identical. A wireless device that claims to have 40-bit encryption interoperates with a device that claims to have 64-bit encryption.

The same device, host computer or front-end processor usually performs both encryption and decryption. The algorithm, like the pattern of a lock, is standardized and may be used by anyone, but the encrypted data is unreadable without the appropriate key, which is known only by the sender and receiver of the transmitted data. You should change your keys often for added security.

1.7 Radio Basics

IEEE 802.11 networking devices transmit and receive radio signals. Users communicate with the network by establishing radio links between mobile devices and access points, or between each other.

Warning

A minimum separation distance of 20 cm (8 inches) should be maintained between the radiating element of this product and nearby persons to comply with FCC rules for RF exposure.

IEEE 802.11 devices use frequency modulation (FM) to transmit digital data from one device to another. The radio signal propagates into the air as electromagnetic waves. The receiving device demodulates the signal, which results in the original digital data. The radio devices transmit in the 2.4 to 2.5 gigahertz frequency range, a license-free range throughout most of the world. The actual range is country-dependent.

1.7.1 Direct-Sequence Spread Spectrum

Broadband spread spectrum uses an algorithm to spread the transmission of a narrowband signal over a segment of the radio frequency band or spectrum. Direct-sequence spread spectrum (DSSS) is a spread spectrum technique in which the narrowband signal is combined with a “chipping sequence” to spread the radio signal sequentially across the entire frequency range specified by the channel of operation. The Intel® PRO/Wireless 2011B LAN access point uses direct-sequence spread spectrum for radio communication.

Note

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

1.7.2 Site Planning

For optimal performance, locate access points 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 access points in open areas or add access points as needed to improve coverage.

Site Survey

A site survey analyzes the installation environment and provides recommendations for equipment and its placement. For detailed information about conducting a site survey with the Site Survey Utility, see the Intel® PRO/Wireless 2011B LAN *Site Survey Administrators Guide*.

Intel 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.

Chapter 2. About the Intel® PRO/Wireless 2011B LAN Access Point

The Intel® PRO/Wireless 2011B LAN Access Point is an Intel® PRO/Wireless 2011B LAN network product. Intel® PRO/Wireless 2011B LAN network products are IEEE 802.11b wireless devices that operate between 2.4 and 2.5 gigahertz using direct-sequence spread spectrum (DSSS) technology. These products provide a high-capacity network using multiple access points within large or small environments.

An Intel® PRO/Wireless 2011B LAN:

- is an architecture that allows communication between both conventional wired and wireless clients and other devices.
- provides support for the IEEE 802.11b specification. This open architecture allows Intel® PRO/Wireless 2011B LAN devices to communicate with wireless devices from other vendors.
- allows wireless clients to roam throughout large facilities while remaining connected to the LAN.
- allows protocol firmware upgrades while devices remain operational.
- features antenna diversity. This feature allows devices to alternate between antennas with the best reception. A device with this capability receives data on one antenna and transmits on the other antenna, increasing overall performance.
- provides an 11 Mbps data rate for high-capacity, fast operation.
- operates within small or large environments using multiple access points.
- provides easy network scalability by adding access points.
- operates in a range of about 45 meters (150 feet).

The access point provides a bridge between Ethernet wired LANs and Intel® PRO/Wireless 2011B LAN networks. It provides connectivity between Ethernet wired networks and radio-equipped computers, including portable computers with Intel® PRO/Wireless 2011B LAN Adapters, terminals, bar-code scanners, and other mobile devices.

The access point provides an 11 Mbps data transfer rate on the radio network. It monitors Ethernet traffic and forwards appropriate Ethernet messages to computers over the Intel® PRO/Wireless 2011B LAN network. It also monitors wireless traffic and forwards packets to the Ethernet LAN.

The access point 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 Marking

The access point 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
- 10/100BaseT 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 clients
- data encryption
- multiple MIB support
- SNMP support
- Mobile IP support
- DHCP support
- HTTP Web server support
- short RF preamble
- wireless access point mode

The access point includes the following new features:

- Intelligent Queuing
- International Roaming
- Transmit Power Control
- BOOTP
- Antenna diversity transmit on primary only

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

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

Warning

A minimum separation distance of 20 cm (8 inches) should be maintained between the radiating element of this product and nearby persons to comply with FCC rules for RF exposure.

2.1 Physical Characteristics

Product Model	WEAP2011BWW
Dimensions	4.4 cm × 15.2 cm × 21.6 cm (1.75” × 6” × 8.5”)
Weight (w/power supply)	0.454 kg (1 lbs.)

Operating Temperature	–20º C to 55º C (–4º F to 131º F)
Storage Temperature	–40º C to 65º C (–40º F to 149º F)
Humidity	10% to 95% noncondensing
Shock	40 G, 11 ms, half-sine
ESD	meets Conformite Europeene (CE) Marking
Drop	withstands up to a 76 cm (30 inch) drop to concrete with possible surface marring

Warning

A minimum separation distance of 20 cm (8 inches) should be maintained between the radiating element of this product and nearby persons to comply with FCC rules for RF exposure.

2.1.1 Kinsington lock

You can attach a Kinsington lock and cable to the back of the access point to secure the device.

2.2 Power and data connections

2.2.1 Power Options

Standard 24 volt, 1 amp power supplyPart Number: 50-24000-024
115/230VAC, 50/60Hz.

- US line cord Part Number: 23844-00-00

2.2.2 Power Injector

You can use the optional Intel® PRO/Wireless LAN 2011B Power Injector to supply power to the Intel® PRO/Wireless 2011B LAN Access Point using the standard Ethernet data cable that connects to the access point. Typically, an Intel® 2011B LAN Access Point is connected to a LAN through a standard Ethernet cable. The access point's AC power supply also requires AC power.

The Intel® PRO/Wireless LAN 2011B Power Injector eliminates the need to install AC wiring to the access point, and lets you consolidate power management and control in the wiring closet. Rather than plugging the AC power supply directly into the access point, the power supply connects to the Power Injector. The Power Injector sends low-voltage DC power to the access point over the unused wires in a standard 4 pair Category 5 cable.

2.2.3 Network Connection

The RJ-45 connector on the access point can connect to an Ethernet network. The access point supports IEEE 802.3 specifications. The access point supports a 10Base-T connection to an Ethernet hub or switch.

When connecting the Intel® PRO/Wireless 2011 LAN access point to an Ethernet switch, make sure that switch port parameters are set to 10 Mbps Half Duplex. Severe performance degradation may result from mis-matched speed or duplex mode.

2.2.4 Serial Connection

The 9-pin, serial port provides a Point to Point Protocol (PPP) connection and basic management tools for the access point. The PPP provides a link between access points using a serial connection. The serial link supports direct serial or telephone-line connections. Connecting the access point to a computer requires a null modem cable and connecting the access point to a modem requires a straight-through cable.

2.2.5 Supported Modems

The access point uses the Hayes command set and is capable of working with various modems of 28,800 baud or faster. Intel does not support modems that Intel has not qualified.

The following modems qualify to work with the Intel® PRO/Wireless 2011B LAN 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

2.3 LED Indicators

The LED indicators provide a status display indicating transmission, and other activity.

📶	**Wireless LAN Activity**	Flickering indicates beacons and data transfers with wireless devices.
🖧	**Wired LAN Activity**	Flashing indicates data transfers on wired connection.
⏻	**Power**	Flashing indicates access point initialization. Steady Green during operation.

The unused LED indicators are reserved for future use.

2.3.1 WLAP mode LED display

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

1. After power up, system initialization begins:

LED	State
Status	Blinks
Wired LAN Activity	Blinks for activity
Wireless LAN Activity	Off

2. When a WLAP begins a full scan:

LED	State
Status	On
Wired LAN Activity	Off
Wireless LAN Activity	Blinks slowly

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

LED	State
Status	On
Wired LAN Activity	Off
Wireless LAN Activity	Blinks slowly

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

LED	State
Status	Blinks regularly
Wired LAN Activity	Blinks for activity
Wireless LAN Activity	Blinks slowly

5. When all WLAP connections are in Forward state:

LED	State
Status	Blinks regularly
Wired LAN Activity	Blinks for activity
Wireless LAN Activity	Blinks for activity

Special cases:

- If the WLAP manual BSSID is NOT set and no other WLAP is found, the WLAP goes to the functional state.
- If the WLAP manual BSSID is set and the specified WLAP not found, the WLAP remains in

FULL Scan state permanently. The LEDs have the following indicator status permanently:

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

- If the WLAP manual BSSID is set with the broadcast bit ON 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**
Status	On
Wired LAN Activity	Blinks slowly
Wireless LAN Activity	Off

2.4 Access Point Functional Features

The access point includes features for different interface connections and network management. The access point provides *MAC layer bridging* between its interfaces. The access point monitors traffic from its interfaces and, based on frame address, forwards the frames to the proper destination. The access point tracks frame sources and destinations to provide intelligent bridging as clients roam or network topologies change. The access point also handles broadcast and multicast message initiations and responds to client association requests.

2.4.1 MAC Layer Bridging

The access point 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 access point. The access point 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).

Each access point stores information on destinations and their interfaces to facilitate *forwarding*. When a user sends an Address Resolution Protocol (ARP) request packet, the access point 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 access point database keeps a record of the destination address along with the receiving interface. With this information, the access point forwards any directed packet to the correct destination. The access point forwards any packet for an unknown destination to the Ethernet interface. Transmitted ARP request packets echo back to other computers.

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

Filtering and Access Control

The access point provides facilities to limit the clients that send data packets through the access point. Filters provide network security or improve performance by eliminating broadcast/multicast packets from the radio network.

The Access Control List (ACL) lets you specify MAC addresses for clients allowed to associate with the access point. This provides security by preventing unauthorized access.

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

Depending on the setting, the access point can keep a list of frame types that it forwards or discards. The *Type Filtering* option prevents specific frames from being processed by the access point. These include certain broadcast frames from devices unimportant to the wireless LAN that take up bandwidth. Filtering out unnecessary frames can also improve performance.

2.4.2 Auto Fallback to Wireless Mode

The access point supports an Auto Fallback to Wireless mode if the wired Ethernet connection fails and the access point is in WLAP Mode. The access point resets itself and during initialization, attempts to associate with any other WLAP in the network. This allows the access point to communicate wirelessly with other access points.

To make this feature available, set the **WLAP Mode** to `Link Required`. See *3.4 Configuring System Parameters* on page 28 and *3.5.1 Wireless Operation Parameters* on page 36.

2.4.3 DHCP Support

The access point can use Dynamic Host Configuration Protocol (DHCP) to obtain a leased IP address and network configuration information from a DHCP server. An access point sends out a DHCP request searching for a DHCP server to acquire the network configuration and firmware filenames.

The access point can optionally download two files when a boot takes place, the firmware file and an HTML file. You can configure a DHCP or BOOTP server to transfer these two files when a DHCP request is made. Use these DHCP options for the specific file or information to download:

- Firmware and HTML file option 67
- ESSID file option 128
- Configuration file option 129
- ACL file option 130

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

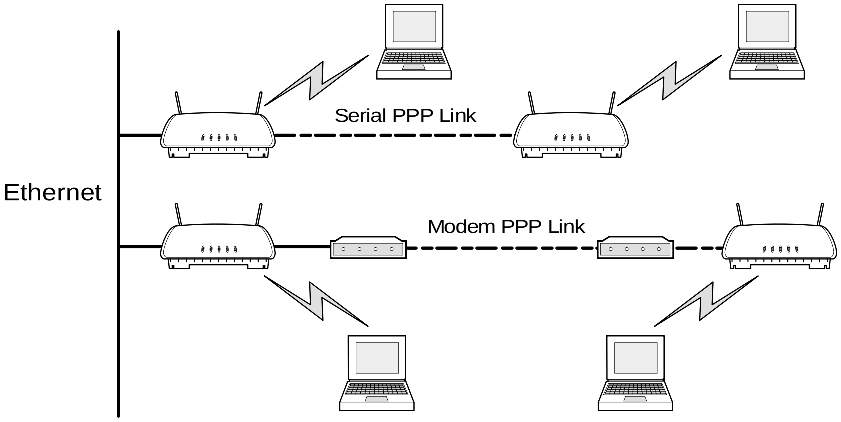
Note

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

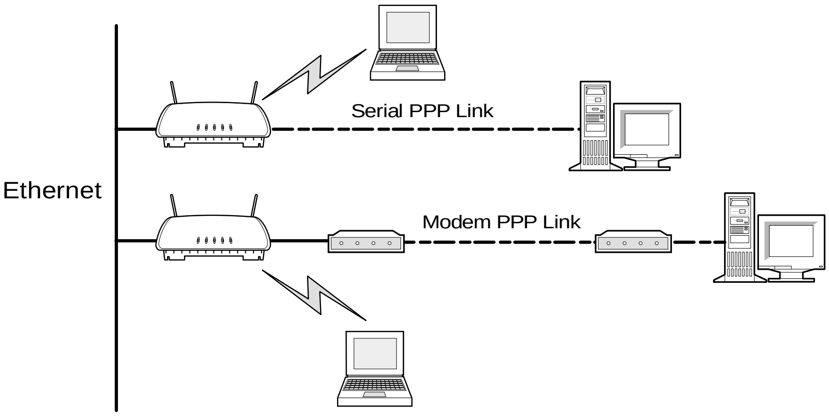
2.4.4 Bridging Support

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

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



- Internet Protocol bridging between an access point and a computer. To establish an Internet Protocol bridge with an access point, use a computer with the appropriate Telnet software with PPP and TCP/IP protocols. Using Telnet, a remote computer can connect to any access point 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 a wired Ethernet network.

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

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

The PPP implementation in the access point uses the Link Control Protocol (LCP) and Network Control Protocol (NCP). The access point database dynamically tracks computers and access points on the PPP interface.

Connecting two access points with a direct serial link requires a null-modem serial cable. Connecting two access points with modem devices requires straight-through cables between the access points and modems. Using modems requires a telephone line for as long as the link remains active.

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

2.4.5 Cellular Coverage

The access point establishes an average communication range with clients called a Basic Service Set (BSS) or cell. When in a particular cell, the client associates and communicates with the access point of that cell. Each cell has a Basic Service Set Identifier (BSSID). In IEEE 802.11, the access point MAC address is the BSSID. The client recognizes the associated access point from its BSSID. Adding access points to a LAN establishes more cells in an environment, creating a wireless network using the same Extended Service Set Identifier (ESSID).

Access points with the same ESSID, or SSID define a coverage area. The client searches for access points with a matching SSID and synchronizes with an access point to establish communications. This allows clients within the coverage area to move about or *roam*. As the client roams from cell to cell, it switches access points. The switch occurs when the client analyzes the reception quality at a location and determines the access point to communicate with based on the best signal strength and lowest client load distribution.

You configure the SSID. A valid SSID is an alphanumeric, case-sensitive identifier up to 32 characters. All nodes within one LAN must use the same SSID to communicate on the same LAN. Multiple wireless LANs can coexist in a single environment by assigning a different SSID for each access point and the clients that communicate with the corresponding access points.

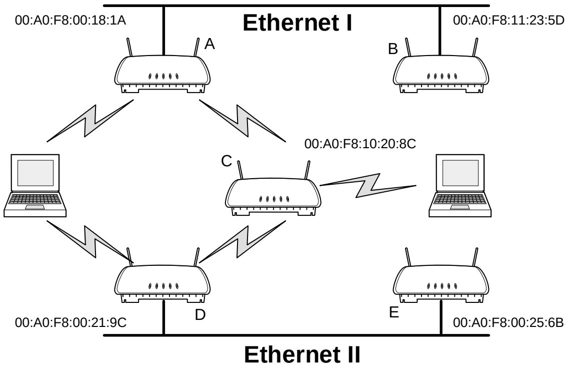
The Root Access Point and Association Process

By default, access points 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 access point and subsequently designated WLAPs.

Access points communicating wirelessly together require the same: Network Name (SSID), Encryption mode, Data Rate, and Short RF Preamble settings.

The root access point maintains the wireless connection among WLAPs by sending out beacons, sending and receiving configuration Bridge Protocol Data Unit (BPDU) packets between each designated WLAP. The WLAP with the lowest WLAP ID becomes the root access point. A concatenation of the WLAP Priority value and the MAC address becomes the WLAP ID.

WLAPs associated with the root access point use the root access point channel, Delivery Traffic Indication Message (DTIM) and Traffic Indication Map (TIM) interval.



In this configuration, the WLAP Priority value is the default `8000` Hex. On concatenating this value to the MAC addresses of the access points, access point A on Ethernet I has the lowest WLAP ID with `800000A0F800181A`, making it the root access point. Access point C uses the Access point A channel, DTIM and TIM interval.

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

To manually designate access point B as the root access point, assign it a WLAP Priority value of 8000. See *3.5 Configuring Radio Parameters* on page 33. Then assign a higher WLAP Priority value to all other access points.

2.4.6 Client Association Process

Access points recognize wireless clients as they associate with the access point. The access point keeps a list of the clients it services. Clients associate with an access point based on the following conditions:

- the signal strength between the access point and client
- clients currently associated with the access point
- the clients encryption and authentication capabilities and the type enabled
- the client supported data rate (1 Mbps, 2 Mbps, 5.5 Mbps or 11 Mbps).

Clients perform preemptive roaming by intermittently scanning for access points and associating with the best available access point. Before roaming and associating with access points, clients perform scans to collect access point statistics and determine the direct-sequence channel used by the access point.

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

Clients perform full scans at start-up. In a full scan, a client uses a sequential set of channels as the scan range. For each channel in range, the client tests for Clear Channel Assessment (CCA). When a transmission-free channel becomes available, the client broadcasts a probe with the Network Name (SSID) and the broadcast BSSID. An access point-directed probe response generates a client Acknowledgment (ACK) and the addition of the access point to the access point table with a proximity classification. An unsuccessful access point packet transmission generates another client probe on the same channel. If the client 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.

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

A client can roam within a coverage area by switching access points. Roaming occurs when:

- an unassociated client attempts to associate or reassociate with an available access point
- the supported rate changes or the client finds a better transmit rate with another access point
- the received signal strength indicator (RSSI) of a potential access point exceeds the current access point
- the ratio of good-transmitted packets to attempted-transmitted packets falls below a threshold.

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

The scanning and association process continues for active clients. This process allows the client to choose the best network connection available by finding new access points and discarding out-of-range or deactivated access points.

2.4.7 Data Encryption

The Intel® PRO/Wireless 2011B LAN uses the Wired Equivalent Privacy (WEP) encryption and decryption algorithm specified in Section 8 of the IEEE 802.11 wireless LAN standard. WEP uses the same key for both encryption and decryption, and provides security equivalent to that of a wired network, hence the “Wired Equivalent” portion of the name.

The IEEE 802.11 standard defines two types of authentication:

- **Open system authentication** is the default authentication service, in which all clients that request access to the network are accepted, with no actual verification. You should only use this system if it’s not necessary to positively validate the identity of the sender.
- **Shared key authentication** requires the exchange of an authentication key shared among all of the authentic access points and clients in the network. When a client requests access to the network, the access point sends a long random number encrypted with the shared key to the client. The client decrypts the number using the same key and sends it back to the access point, which only grants access to clients that return the correct number. The Intel® PRO/Wireless 2011B LAN Access Point supports both 40-bit and 128-bit shared key encryption.

Note

If you implement the shared key authentication mode, you must configure all access points and clients to use the same key.

To implement WEP on each access point, use either a 40-bit key or a 128-bit key. A 40-bit key consists of 10 hexadecimal numbers in two 5-digit groups, arrayed as follows.

```
10111 21314
```

A 128-bit key consists of 26 hexadecimal numbers in two 5-digit groups and four 4-digit groups, arrayed as follows.

```
10111 21314 1516 1718 191A 1B1C
```

2.4.8 Mobile IP

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

- The client changes its point of attachment without changing its IP address, causing forthcoming packets to become undeliverable.
- The client changes its IP address when it moves to a new network, causing it to lose connection.

Mobile IP enables a wireless client to communicate on the network using its home IP address after changing its point-of-attachment to another subnet.

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.

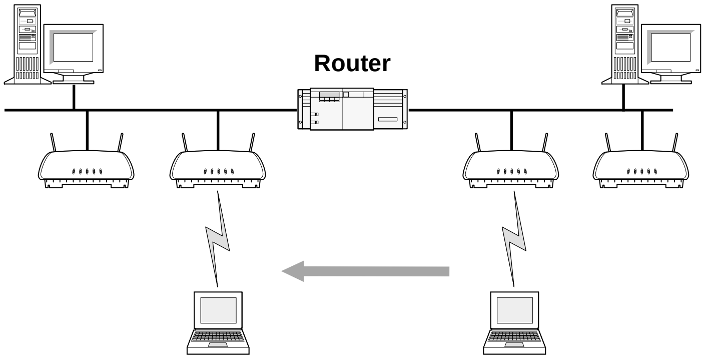
A tunnel is the path taken by the original packet encapsulated within the payload portion of a second packet to some destination on the network.

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

A *Foreign Agent* is an access point acting as a router at the client’s location on a foreign link. The foreign agent serves as the default router for packets sent out by the client connected on the same foreign link.

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

The following diagram illustrates Mobile IP:



When the client moves to an access point on another subnet, mobile IP allows it to continue to communicate as if it were on it’s original subnet.

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 client and access point share the *checksum*, called a *key*, to authenticate transmitted messages between them. The access point and client share the key while the client is visiting a foreign subnet. The client and access point have to use the same key. If not, the access point refuses to become the *Home Agent* for the client. The maximum key length is 13 characters. The access point allows all printable characters.

2.5 Management Options

Managing the Intel® PRO/Wireless 2011B LAN includes viewing network statistics and setting configuration options. Statistics track the network activity of associated clients and data transfers on the access point interfaces.

Web Browser Support

The Intel® PRO/Wireless 2011B LAN Access Point includes a Web server, which allows you to access the access point with a Java-compatible browser. You can use either NetScape Navigator† 4.5 or greater, or Microsoft Internet Explorer† 4.0 or greater to view and set configuration settings. You can browse to the IP address of the access point. If the access point is defined in DNS, you can browse to the DNS name of the access point. You can access configuration, performance, and diagnostic information for the access point. You can also change configuration settings and update the firmware in the access point.

Other management options

The access point also supports the following to perform custom management:

- a networked computer with a Telnet client
- terminal or computer with RS-232 connection and ANSI emulation
- Simple Network Management Protocol (SNMP)

  The access point 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 Intel proprietary Intel Management Information Base (MIB). The SNMP agent supports read-write, read-only or disabled modes. However, Intel does not recommend accessing the access point using this interface method. See to the MIB Browser documentation for usage. The access point supports traps that return to the SNMP manager when certain events occur. The Intel® PRO/Wireless 2011B LAN Installation Disk packaged with access points contains the Intel MIB.

Chapter 3. Configuring the Access Point

3.1 Configuration Options

To configure the Intel® PRO/Wireless 2011B LAN access point, you set up a connection to the access point and use one of the following methods:

Web Browser Browse to the access point built-in Web server from a Web browser using a wireless or Ethernet connection. See *3.1.2 Using a Web Browser* on page 21.

Telnet Client Telnet to the access point using a wireless or Ethernet connection. See *3.1.3 Using Telnet* on page 23.

Direct Serial Connection Use a terminal program on your computer with a null-modem serial cable connected to the access point.
See *3.1.4 Using a Direct Serial Connection* on page 23.

Dial Up Access Use a terminal program with a dial-up connection to the access point. The access point can connect to a Hayes-compatible modem. See *3.1.5 Using a Dial-Up Connection* on page 23.

Most of these access methods first require the configuration of an IP address. To access the access point to change the IP address, use the serial port and a terminal emulation program. Connect to the serial port using a null modem cable. Set your terminal emulation program for `19,200` bps, `8` bits, `NO` parity, `1` Stop Bit and `NO` flow control. Select the **AP Installation** screen, and enter the appropriate IP configuration parameters for your network.

3.1.1 Finding the IP Address of the Access Point

Before you can manage the access point using a Web browser or Telnet, you need to know the IP address of the access point. You can use the **AP Discovery** application to find access points on your network and determine the IP address of each. AP Discovery is installed from the Intel® PRO/Wireless 2011B LAN CD when you install the software on your computer. For installation instructions, see the Intel® PRO/Wireless 2011B LAN *Access Point Quick Installation Guide*.

To locate an access point, click **Start**, **Programs**, **Intel(R) PROWireless**, **Access Point Administration Utilities**, and then **AP Discovery**. If your are running Windows 95, click **Start**, **Programs**, **Intel(R) Wireless LAN**, **Intel WLAN Utilities**, and then **AP Discovery**.

If you do not have a DHCP server on your network, the access point uses the following default IP address:

```
192.0.2.1
```

If you cannot locate the access point on your network, you can use a direct serial connection to the access point and set an IP address for the access point. See *3.1.4 Using a Direct Serial Connection* on page 23.

To verify a connection, ping the access point. At the DOS prompt, type:

```
Ping -t
```

followed by the IP address of the access point. If the ping receives no response, verify that the hardware connections, IP address, gateway address and subnet mask are correct.

3.1.2 Using a Web Browser

The easiest way to manage the access point is to use a Web browser configured to browse the LAN. Your computer can be on the wired or wireless LAN. Your Web browser must be Internet Explorer† 4.0 or greater, or Netscape Navigator† 4.5 or greater.

Accessing the Main Menu

To use a Web browser to manage the access point, the Web browser must be configured to browse the LAN. The remote computer can be on the wired or wireless LAN.

To make sure the **Web Server** option is enabled for the access point:

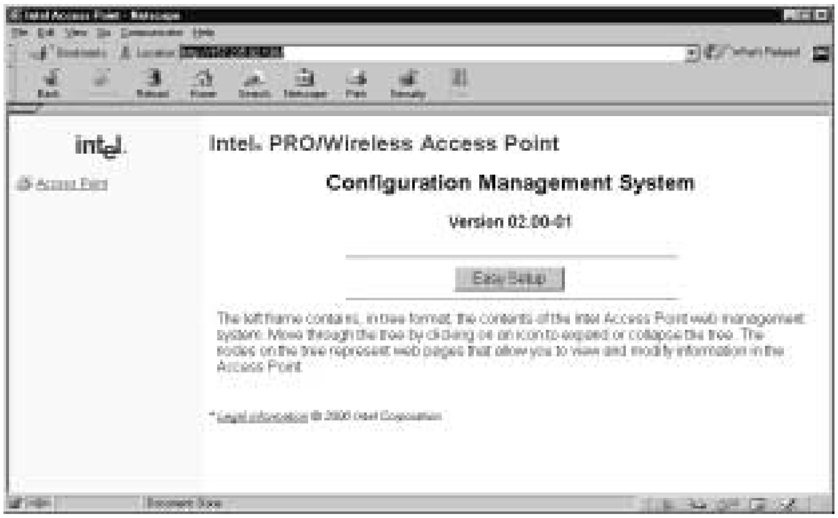
1. Access the management console using a Serial or Telnet connection.
2. Select the **System Configuration** screen.
3. Verify the **Web Server** option on the **System Configuration** screen is enabled.
4. Save the configuration by selecting **Save-[F1]**.

Reset the access point for changes to take effect.

1. Select the **Special Functions** screen.
2. Select **Reset AP**.

To access the access point using a Web browser from a computer:

1. Type the IP Address for the access point in the browser address window. The browser displays the **Configuration Management System** main page:



Intel® PRO/Wireless Access Point

Configuration Management System

Version 02.00-01

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

* Legal information © 2000 Intel Corporation

The Web pages differ from those for the console used for Telnet, Direct Serial or Dial-Up Connections, but the contents are the same. Access the different pages using the links located on the left.

To view configuration, function or option changes on the Web pages, turn off the caching function for your browser.

- — 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 access to the **Easy Setup** and **Configuration** pages:

1. Click **Easy Setup** and type the access point name.

   `Intel PRO/2011B Access Point`

2. Type the password. The default is:

   `Intel`

   Note that the password is case-sensitive.

Setup Network Web Server Help File Access

The Intel® PRO/Wireless 2011B LAN CD-ROM contains Help for the Access Point Configuration Management System web pages. You can view the Help on the CD or copy the files to a Web server on you network and make them available on the server.

To copy the Help files to a network Web server:

1. Create a directory on the network Web server for the Access Point Web Site Help Files to reside.
2. Copy the `*.gif` and `*.htm` files to this directory from the following directory on the Intel® PRO/Wireless 2011B LAN CD-ROM:

   `firmware\AP\AP Web Site\Help`

To browse to the Help, browse to `wlaaphlp.htm` in this folder.

To enable Help file access from the Web management pages on the access point, change the Help URL parameter:

1. Type the IP Address for the access point in the browser address window. The browser displays the **Configuration Management System** main page.
2. Select the **Special Functions** screen.
3. Use the **TAB** or **UP/DOWN ARROW** key to select the **Alter Filename(s)/HELP URL/TFTP Server/DHCP**.
4. Press Enter.
5. Use the **TAB** or **DOWN ARROW** key to select the **.HELP URL** field.
6. Type the IP address/URL 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.
7. Press **ENTER**.
8. Use the **TAB** or **DOWN ARROW** key to select **OK-[CR]** and press **ENTER**.
9. Save the new setting by selecting the **Save Configuration** option.

Reset the access point for changes to take effect.

1. Select the **Special Functions** screen.
2. Select **Reset AP**.

To access help from any management web page:

- Select the **Help** button located in the top right-hand corner of each page.

3.1.3 Using Telnet

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

To access the access point from the workstation:

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

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

2. At the prompt type the password. The default is:

```
Intel
```

Note that the password is case-sensitive.

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

— If the session is idle with 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.

3.1.4 Using a Direct Serial Connection

The access point supports a serial connection to the management console, through a 9-pin serial connector. Connecting the access point directly to a computer serial port requires a null modem cable. The factory-configured access point accepts a direct serial connection.

To make a serial connection:

1. Attach a null modem serial cable from the access point to the terminal or computer serial port.

2. From the computer, start the communication program, such as HyperTerminal† for Windows†.

3. Select the correct COM port along with the following parameters:

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

There is no password requirement.

4. Press **ESC** to refresh the view. The access point displays the **Main Menu**.

To terminate the session, exit the communication program.

3.1.5 Using a Dial-Up Connection

The access point supports a dial-up connection to the management console. The access point supports connection to a Hayes-compatible 28,800-baud or faster modem. This requires accessing the management console from a Web, Telnet, or a direct serial connection and changing the serial port configuration.

A dial-up connection requires a straight-through cable between the modem and the access point. The remote computer requires a modem and a communication program, for example the Microsoft Windows Terminal† program. For supported modems, see *2.2.5 Supported Modems* on page 10.

Configuring Serial Port

To enable and configure the serial port connection on the access point:

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 access point.

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 The access point sends a command to the modem to turn on/off the modem speaker. The default is `On`.

Inactivity Timeout The inactivity time on the management console that causes the access point 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 access point:

1. Attach a straight-through serial cable from the access point to the modem.
2. Make sure that the modem connects to the telephone line and has power.
3. From the remote terminal, start the communication program.
4. Select the correct serial port along with the following parameters.

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

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

Hanging Up

To hang up while connected:

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

3.2 Navigating the Management Console

The access point displays a Main Menu when you access the management console using Telnet or a serial connection:

```
Intel PRO/Wireless 2011 LAN
                        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 Access Control List
Show Ethernet Statistics            Set Address Filtering
Show RF Statistics                  Set Type Filtering
Show Misc. Statistics               Set SNMP Configuration
Show Event History                  Set Event Logging Configuration
Enter Admin Mode
```

The top line displays the **System Name** for the access point (default is `Intel PRO/2011B Access Point`) and the name of the configuration screen.

The access point 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 access point beeps and restores the original value.
- 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**.
- Press **ESC** to exit 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 nonvolatile memory (NVM). A reset command returns to previously saved settings.

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

Save ALL APs To save the *access point installation* configuration information to all access points with the same Network Name (SSID). This option saves the configuration changes for the current access point on the **Known APs** table to update their configuration and reset after the configuration has been modified. You can use this option only among the same hardware platforms and same firmware versions.

Cancel Does not register settings changed in a screen.

The dot in front of certain parameters, functions or options (`.Antenna Selection  Primary Only`) indicates these items update to all access points with the same Network Name (SSID) when choosing the **Save ALL APs-[F2]** option. You can perform this option only among the same hardware platforms and same firmware versions.

3.2.1 Entering Admin Mode

The access point defaults to *User* when in *Serial mode* allowing read-only access to the access points functions (e.g., view statistics). Entering *Admin* mode provides access to configuration menus and allows you to configure the access point.

Entering Admin mode requires the administration password.

1. Select **Enter Admin Mode** from the **Main Menu**.
2. Type the password. The default is:
   `Intel`

   Note that the password is case-sensitive.

   — If the password is correct, the access point displays the **Main Menu** with the **Enter Admin Mode** menu item changed to **Exit Admin Mode**.

   — If the password is incorrect, the access point continues to display the **Main Menu** with the **Enter Admin Mode** menu item.

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

3.2.2 Controlling Access to the Management System

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

To change Telnet access to the access point:

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]** and display the **Change System Passwords** screen.
3. 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 `Intel`.

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. The default password is `Intel`.

4. To register settings by writing changes to NVM, select **Save-[F1]**.

3.3 Changing Basic Settings

To change the basic parameters set during installation of the access point:

1. Select **AP Installation** from the **Main Menu**.
2. Change the following settings and select **Save**.

Country Config Set the country for the access point. This item displays a list of country names. Prior to setting the Country Config code certain features will not be available.

Unit Name The name of this access point.

IP Address The network-assigned Internet Protocol address of the access point.

Gateway IP Address IP address of a router the access point uses on the Ethernet default gateway.

Subnet Mask These values help divide a network into subnetworks and simplify routing and data transmission. The subnet mask defines the size of the subnet.

DNS IP Address Primary Domain Name Server IP address.

Additional DNS The IP address of the additional DNS servers available. A maximum of two additional DNS servers are available.

Net_ID (ESS) The unique 32-character, alphanumeric, case-sensitive network identifier of the access point.

Antenna Selection **Full Diversity**: The radio receives on the antenna that has the best signal and transmits on the last antenna it received on.

Primary Only: The radio transmits and receives on the primary antenna only.

Secondary Only: The radio transmits and receives on the secondary antenna only.

Rx Diversity: The radio receives on the antenna that has the best signal and transmits on the primary antenna.

Additiional Gateways The IP address of the additional gateways used.

DHCP/BOOTP **Enabled**: DHCP and BOOTP interoperate, server that responds first becomes the server allocating the information.

DHCP Only: Only DHCP responses will be accepted by the access point.

BOOTP Only: Only BOOTP responses will be accepted by the access point.

Disabled: Disables BOOTP and DHCP. IP configuration is manually entered.

3.4 Configuring System Parameters

The access point 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**.
2. Configure the direct-sequence channel settings.

Country	ID	Channels	
		First	Last
Argentina	AR	1	13
Australia	AU	1	13
Austria	AT	1	13
Bahrain	BH	1	13
Belarus	BY	1	13
Belgium - Indoor	BE	1	13
Belgium - Outdoor	BE	1	2
Brazil	BR	1	13
Bulgaria	BG	1	13
Canada	CA	1	13
Chile	CL	1	13
China	CN	1	13
Columbia	CO	1	13
Costa Rica	CR	1	13
Croatia	HR	1	13
Czech Republic	CZ	1	13
Denmark	DK	1	13
Finland	FL	1	13
France	FR	11	13

Country	ID	Channels	
		First	Last
Germany	DE	1	13
Greece	GR	1	13
Guatemala	GT	1	13
Hong Kong	HK	1	13
Hungary	HU	1	13
Iceland	IS	1	13
India	IN	1	13
Indonesia	ID	1	13
Ireland	IE	1	13
Israel	IL	5	8
Italy	IT	1	13
Japan	JP	1	14
Jordan	JO	1	13
Kuwait	KW	1	13
Liechtenstein	LN	1	13
Lithuania	LT	1	13
Luxembourg	LU	1	13
Malaysia	MY	1	13
Mexico	MX	11	13
Morocco	MA	1	13
Netherlands	NL	1	13
New Zealand	NZ	1	13
Norway	NO	1	13
Peru	PE	1	13
Panama	PA	1	13
Philippines	PH	1	13
Poland	PL	1	13
Portugal	PT	1	13
Qatar	QA	1	13
Romania	RO	1	13
Russian Federation	RU	1	13
Saudi Arabia	SA	1	13
Singapore	SG	10	13
Slovak Republic	SO	1	13
Slovenia	SI	1	13
South Africa	ZA	1	13
South Korea	KR	1	13
Spain	ES	1	13
Sri Lanka	LK	1	2
Taiwan	TW	1	13
Thailand	TH	1	13
Turkey	TR	1	13
UAE	UE	1	13
Ukraine	UA	1	13
UK	UK	1	13
USA	US	1	11
Venezuela	VE	1	13

3. Configure the access point system settings as required:

Auto Channel Select

Normally run once during initial installation.

1. Power up the AP and select Auto Channel Select (ACS).
2. The access point scans all channels and selects a non-overlapping channel with the fewest APs. The access point saves the channel in FLASH (the power LED flashes during this process) and turns off ACS. The access point flashes its LEDs as if powering up and returns to a STATUS-flashing state when complete.

Non-overlapping channels have 25Mhz separation beginning at the first allowed channel for the country (for the US and most of Europe, channels 1, 6 & 11 will be used). The channel selection process groups all wirelessly detected access points into non-overlapping bands and then compares the quantities of access points with received signal strengths above the average signal strength. Ties are broken based on the access point's MAC address.

Ethernet Timeout

Disables radio interface if no activity is detected on the Ethernet line after the seconds indicated (`30–255`).
The access point disassociates clients 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 access point, 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 access point clears the client computer table and disables the RF interface until the Ethernet connection comes up.

Telnet Logins

Specifies if the access point accepts or rejects Telnet Logins.
The default value is `Enabled`.

Encryption Admin 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.

Any allows anyone with admin privileges to change encryption keys using a Web browser, Telnet, or the serial port.

Serial: Limits changing encryption keys to access through the serial port.

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

PRO/2011B Mobile IP If enabled, this feature allows clients to roam across routers.

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

computer-computer Disallowed If enabled, clients associated with the same access point are not allowed to communicate with each other.

Web Server Enables the use of a Web browser to manage the access point instead of HyperTerminal or Telnet applications. An access point reset is required for this feature to take effect.

System Password Admin Allows you to change the passwords for the access point. This screen can be accessed only when the access point is in **Telnet** mode.

Serial mode provides read-only privileges and does not allow the anyone to view this screen.

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

Type Filtering Specifies filter type for packets received either Forward/ Discard or Disabled.

The default value is `Disabled`.

WNMP Functions Specifies if the access point can perform WNMP functions.

The default value is `Enabled`.

AP-AP State Xchg Specifies access point-to-access point communication exchanged.

4. To enable or disable interfaces on the access point, modify the following parameters:

Ethernet Interface Enables or disables wired Ethernet.

The default value is `On`.

PPP Interface Enables or disables serial PPP.

The default value is `Off`.

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

Default Interface Specifies the default interface (**Ethernet**, **PPP** or **WLAP**) that the access point forwards a frame to if the access point 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.
7. Select **Save ALL APs-[F2]** to save the **System Configuration** information to all access points with the same Network Name (SSID). This option saves the configuration changes for the current access point, and sends two messages to all other access points on the **Known APs** table to update their configuration and reset after the configuration has been modified. You can perform this option only among the same hardware platforms and same firmware versions.

3.4.1 System Password Administration

This screen allows you to configure the passwords for the access point. The user password allows the user to Telnet into the access point or use the serial port and have read-only privileges. While using the serial port in an Admin mode session, the session does not time-out.

Caution

Entering the **Admin** mode with both the **Telnet** and **Serial Port** menus active enables **Admin** mode on both interfaces. This can cause a security breach if a user without admin privileges Telnets into the access point while the admin security level is enabled, giving the user admin-level access.

1. To access and change the System Passwords, select **System Password Admin-[F4]** from the **System Configuration** menu to display the **Change System Passwords** screen.
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 `Intel`.

   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 `Intel`.

3. Select `Save` to register settings by writing changes to NVM.

3.5 Configuring Radio Parameters

The access point automatically configures most radio parameters. Only advanced users, Intel® PRO/Wireless 2011B LAN trained users or Intel® PRO/Wireless 2011B LAN representatives (http://www.intel.com/network) should adjust the radio parameters for the access point. Options in the **RF Configuration** screen fine-tune the radio and WLAP functions.

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

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

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

Reassembly timeout Sets the time in 0.5 ms units before a 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.

Max Retries (d) The maximum allowed retries before aborting a single data packet transmission. The default is 15. Do not change this setting.

Max Retries (v) The maximum allowed retries before aborting a single voice packet transmission. The default is 5. Do not change.

Multicast Mask (d) Supports broadcast download protocols for any client, 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.

Multicast Mask (v) Supports broadcast, or *party-line*, 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.

Beacon Interval The time between beacons in Kilo-microseconds. The default is 100. Avoid changing this parameter because it can adversely affect PSP-mode terminal performance.

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

computer inactivity Timeout Allows industry-standard device interoperability by specifying the time the access point allows for client inactivity. A PRO/2011B access point recognizes client activity through data packet transmission and reception, and through scanning. PRO/2011B clients conduct active scanning. Other industry-standard clients might conduct passive scans and a PRO/2011B access point can classify them as inactive.

Rate Control Defines the data transmission rate, the defaults are:

- **11 Mbps** - Optional
- **5.5 Mbps** - Optional
- **2 Mbps** - Required
- **1 Mbps** - Required.

The defaults allow the access point to automatically select 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.
Any combination of the data rates can be selected as **Optional**, **Required** or **Not Used**, but it is essential to set the lowest selected rate to Required. All IEEE 802.11 broadcast and management frames are sent out on the lowest required data rate.

RTS Threshold Request to send threshold (256 – 2347). Allows the access point to use Request To Send (RTS) on frames longer than the specified length. The default is 2347 Bytes.

CCA Mode Clear Channel Assessment (CCA) mode is the method used to detect transmissions from sources other than the access point. The default is Carrier Sense.

CCA Energy Threshold The energy threshold or level above which the airwaves are considered busy. The default is 60.

WEP (Privacy) Defines the WEP algorithm. Admin privileges are required to make changes to this parameter. The default is Disabled.

WEP Algorithm 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.

Encryption Key ID Change the **Active Key** number. Admin privileges are required to make changes to this parameter. The default key ID is `1`.
Reset the access point for the new key value to become the active key.

Encryption Key Maintenance Change the values for each encryption key. Admin privileges are required to make changes to this parameter.

Enable Strong Encryption 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 Intel Customer Support Center for a unique access code to enable this feature.

Short RF Preamble Determines whether the access point uses a short or long preamble. The preamble is approximately 8 bytes of the packet header generated by the access point 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 available on the Intel® PRO/Wireless 2011B LAN Access Point and other high rate DSSS hardware. Non-high rate DSSS hardware such as the BAY Stack 660 cannot enable the short preamble function and cannot see, receive or acknowledge messages from short preamble enabled in earlier versions of the hardware. Disable this feature in a mixed hardware network and use the long preamble. Clients and access points are required to have the same Short RF Preamble settings for interoperability. The default is `Enabled`.

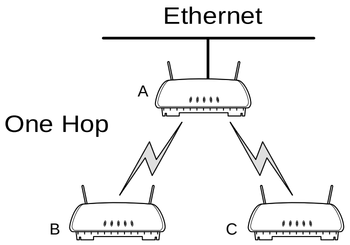
Tx Power Control Allows the you to reduce the coverage area while increasing the throughput. Available settings are: **Full** (default), **30mW**, **15mW**, **5mW** and **1mW**. These values are approximate.

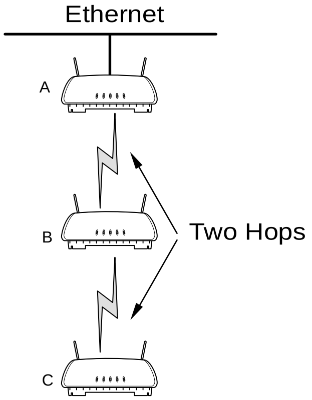
RTS Threshold, **CCA Mode** and **CCA Energy Threshold** are not configurable parameters.

3. Verify the values set reflect the network environment. Change them as needed.
4. Select **OK** or **Save** to register the settings by writing changes to NVM.
5. Select **Save ALL APs-[F2]** to save the **RF Configuration** information to all access points with the same SSID. This option saves the configuration changes for the current access point, and sends two messages to all other access points on the **Known APs** table to update their configuration and reset after the configuration has been modified. You can perform this option only among the same hardware platforms and same firmware versions.

3.5.1 Wireless Operation Parameters

The access point supports up to four WLAP interfaces. Intel recommends using one WLAP as an interface on high traffic networks. For low traffic networks use no more than two WLAPs. With multiple WLAPs, excessive channel contention causes the WLAP to miss beacons from the root access point shown in the example.

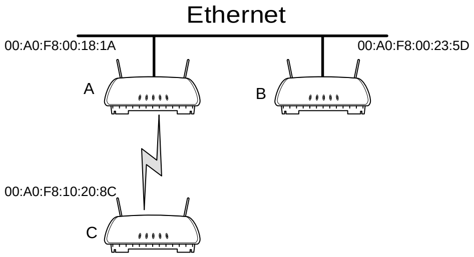




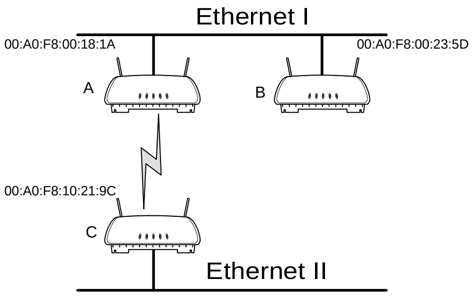
See *2.3 LED Indicators* on page 10 for indication of access point status. If more than two WLAPs operate in a repeater configuration, Intel recommends the WLAPs with the lowest WLAP IDs be placed on the wired network.

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 access point **A** to `Ethernet`.
2. Set the default interface for access point **B** to `Ethernet`.
3. Set the default interface for access point **C** to `WLAP`.
   This allows the clients to roam and transmit data between access point **B** and **C**.



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



To configure the access point for wireless operation:

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

WLAP Mode

Specifies the access point’s wireless-access point operation status.

Enabled, the access point sets up automatically for wireless operation. The access point can operate in any of these configurations: **Wireless**, **Repeater** or **Ethernet Bridge**.

Disabled, no wireless operation possible. Default setting.

Link Required. At power up:

- If the WLAP is the root access point, an Ethernet connection is required.
- If the WLAP is a designated WLAP, association to the root access point is required.

During normal operation:

- If the Ethernet connection is lost, the root access point resets.
- If the WLAP association is lost, the designated WLAP resets.

WLAP Priority

Set the Root and the designated WLAP in wireless operation. Concatenate the priority value as the most significant portion of the MAC address. An access point with a lower numerical value for priority is more likely to become the root access point. The default is `8000` hex from the `0` to `0xFFFF` range.

WLAP Manual BSS_ID

Specifies the BSSID of a particular WLAP and forces the current access point to associate only with that WLAP.

If setting the **WLAP Manual BSS_ID** to the current BSSID, the current access point jumps into **Functional State** immediately and waits for an Association Request from the other WLAP. See *4.8 Radio Statistics* on page 68. This feature speeds up the association process and minimizes confusion when more than two WLAPs try to associate with each other.

WLAP Hello Time

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

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

WLAP Max Age

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

The **WLAP Max Age** of the root access point overwrites the **WLAP Max Age** of designated WLAPs.

WLAP Forward Delay

Specifies the time, in seconds, to prevent an access point from forwarding data packets during initialization. The WLAPs involved and the wireless operation state, see *4.8 Radio Statistics* on page 68, 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 access point overwrites the **WLAP Forward Delay** of designated WLAPs.

3.5.2 Encryption Key Maintenance

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

This table shows the access point association capability with the selected WEP Algorithm.

Access Point Selected WEP Algorithm	Client Selected WEP Algorithm	Association Status
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

Intel provides a total of four Encryption Keys. Each key enables encryption between the access point and an associated client 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 access point and client to authenticate data transmission using encryption.

Example: An access point uses **Key 1** with a value of `1011121314`. The associated client 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 screens, contact the Intel Support Center (http://support.intel.com) or the Network Products division (http://www.intel.com/network) for the unique access code to enable this feature.

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

40 Bit Encryption

Each key has 40 bits available for configuration and are displayed in two 20-bit segments. The remaining 24 bits are factory set and not configurable.

1. Select the desired key and enter the value.
2. Select **OK** or **Save** to register the settings by writing changes to NVM.
3. Select **Save ALL APs-[F2]** to save the **Encryption Key Maintenance** information to all access points with the same SSID. This option saves the configuration changes for the current access point, and sends two messages to all other access points on the **Known APs** table to update their configuration and reset after the configuration has been modified. You can perform this option only among the same hardware platforms and same firmware versions.

128 Bit Encryption

Each key has 124 bits available to for configuration and are displayed in two 20-bit segments and four 16-bit segments. The remaining 24 bits are factory set and not configurable.

1. Select the desired key and enter the value.
2. Select **OK** or **Save** to register the settings by writing changes to NVM.
3. Select **Save ALL APs-[F2]** to save the **Encryption Key Maintenance** information to all access points with the same SSID. This option saves the configuration changes for the current access point, and sends two messages to all other access points on the **Known APs** table to update

their configuration and reset after the configuration has been modified. You can perform this option only among the same hardware platforms and same firmware versions.

Enabling 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. If you are eligible to use 128-bit strong encryption, you can contact Intel Support Center (http://support.intel.com/support/network/#Wireless_Ethernet_LAN **Top Technical Issues** page and **FAQ** document), or the Intel Networking and Communications Division (http://www.intel.com/network), to obtain the Access Code.

1. To enable Strong Encryption (128-bit encryption) select Enable Strong Encryption on the RF Configuration screen.
2. Enter the acquired access code in the space provided.
3. Select **OK** or **Save** to register settings by writing changes to NVM.
4. Select **Save ALL APs-[F2]** to save the **Enable Strong Encryption** access code to all access points with the same SSID. This option saves the configuration changes for the current access point, and sends two messages to all other access points on the **Known APs** table to update their configuration and reset after the configuration has been modified. You can perform this option only among the same hardware platforms and same firmware versions.

3.6 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.

3.6.1 PPP Direct

A direct null modem serial cable connection between two access points.

1. Select **Set Serial Port Configuration** from the **Main Menu**.
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 access point. Set the other access points **Connect Mode** to `Originate`.

3.6.2 Establishing Connection

To establish the PPP port connection on both access points:

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.

3.6.3 PPP with Modems

The PPP interface provides a connection using modems over a telephone line. Connect modems to the access points with straight-through serial cables. Designate one access point as the *Originating* access point and the other as the *Answering* access point. Configure the originating access point with dial-out information to the answering access point. The answering access point waits for the originating access point to dial into it

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

3.6.4 Originating Access Point

From the originating access point's **Main Menu**:

1. Select **Set Serial Port Configuration**.
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 access point (maximum 31 characters). This string matches what follows a typical Hayes Smartmodem `ATDT` command. Possible characters include pauses, numbers and letters. See the modem documentation.
6. Set the **Dialout Mode** to `Auto`.

7. Configure the other settings as required:

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

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

PPP Timeout Controls the time-out between issuing a PPP packet and expecting a reply, 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.

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

3.6.5 Answering Access Point

From the answering access point's **Main Menu**:

1. Select **Set Serial Port Configuration**.
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 access point.

3.6.6 Initiating a Modem Connection

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

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

The access point dials out and attempts to make connection according to parameters set in **Serial Port Configuration**. If dial-out fails, the access point 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 access point LEDs flash as if powering up and then returns to a STATUS-flashing state.

To hang up:

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

3.7 Configuring the SNMP Agent

An SNMP manager application gains access to the access point SNMP agent if it has the access point IP address. An access point can be accessed through the SNMP Trap Manager to configure settings and parameters, Intel does not recommend this process.

Configuring the encryption Keys using the SNMP Trap Manager overrides the Key values for the access points accessed by the SNMP Trap Manager.

The agent configures as **read-only**, **read-write** or **disabled** to provide security when using SNMP. The access point sends specific traps for some conditions. Ensure the SNMP trap manager recognizes how to manage these traps.

For specific entries, see the Intel MIB on the Intel® PRO/Wireless 2011B LAN Installation Disk in the `DMI-SNMP\Win32` directory.

The access point supports SNMP Version 1, a limited feature set of SNMP Version 2, the IEEE 802.11 MIB-II and the INTEL.MIB.

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

SNMP Agent Mode defines the SNMP agent mode:

Disabled disables SNMP functions.

Read-only allows get and trap operations.

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

Read-Only Community A password string up to 31 characters for users with read-only privileges.

Read/Write Community A password up to 13 characters for users with read/write privileges.
Ensure that the password used matches the **Admin Password** used to gain access to the **System Password Administration** screen.

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

Cold Boot Send a trap to manager when the access point cold boots.
The default value is `Disabled`.

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

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

Access Cntrl Violation Send a trap to manager when an Access Control List (ACL) violation occurs. The default value is `Disabled`.

Trap Host1 IP Address The **Trap Host1** manager IP address.
The default is `0.0.0.0`.

Trap Host2 IP Address The **Trap Host2** manager IP address.
The default is `0.0.0.0`.

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

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

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

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

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.
5. Select **Save ALL APs-[F2]** to save the **SNMP Configuration** information to all access points with the same SSID. This option saves the configuration changes for the current access point, and sends two messages to all other access points on the **Known APs** table to update their configuration and reset after the configuration has been modified. You can perform this option only among the same hardware platforms and same firmware versions.

3.8 Configuring the Access Control List

The Access Control List (ACL) contains MAC addresses for clients allowed to associate with the access point. This provides security by preventing unauthorized access. The ACL supports adding client computer 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**.

3.8.1 Setting a Range of Allowed Clients

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** and change the values as needed.
6. To delete a range of wireless clients, select **Delete-[F1]**.
7. To add a range of wireless clients, select **Add-[F2]**.
8. Select **Save ALL APs-[F3]** to save the **Ranges of Allowed Mobile Units** information to all access points with the same SSID. This option saves the configuration changes for the current access point, and sends two messages to all other access points on the **Known APs** table to update their configuration and reset after the configuration has been modified. You can perform this option only among the same hardware platforms and firmware versions.

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

3.8.2 Adding Allowed Clients

The **Access Control List** screen provides a facility to add clients 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 access point prompts for a MAC address.

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

4. Enter the MAC address. You can enter MAC addresses without colons.
5. Select **Save ALL APs-[F3]** to save the **Access Point Installation** configuration information to all access points with the same SSID. This option saves the configuration changes for the current access point, and sends two messages to all other access points on the **Known APs** table to update their configuration and reset after the configuration has been modified. You can perform this option only among the same hardware platforms and firmware version.

3.8.3 Removing Allowed Clients

The *A***llowed Mobile Units** screen provides a facility to remove clients from the ACL.

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

3.8.4 Enabling or Disabling the Access Control List

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.

3.8.5 Removing All Allowed Clients

The access point provides a facility to remove all clients from the ACL.

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

3.8.6 Loading an Access Control List from the Computer List

This option from the **Special Functions** menu takes all associated clients and creates an ACL from them. This builds an ACL without having to manually type addresses. Then you can edit the ACL using the add and delete functions.

To add addresses of associated clients to the ACL:

1. Select **Special Functions** from the **Main Menu**.
2. Select **Load ACL from Computer List**.

3.8.7 Loading an Access Control List from File

This option from the **Special Functions** menu creates an ACL from a user defined ACL file (`AP_ACL.TXT` the file name) entered on the secondary screen of the **Special Functions** Menu. The following is an example of the `AP_ACL.TXT` file.

```
[ACLIndividual]
Add    00:A0:F8:FF:01:FB
Add    00:A0:F8:FF:01:FC
Add    00:A0:F8:FF:01:FD
Add    00:A0:F8:FF:01:FE
Add    00:A0:F8:FF:01:FF
;Delete00:A0:F8:FF:00:0A
;Delete00:A0:F8:FF:00:1A
;Delete00:A0:F8:FF:00:2A

[ACLRange]
Add      00:A0:F8:FD:01:00    00:A0:F8:FF:01:20
Add      00:A0:F8:FD:02:00    00:A0:F8:FD:02:20
Add      00:A0:F8:FD:03:00    00:A0:F8:FD:03:20
Add      00:A0:F8:FD:04:00    00:A0:F8:FD:04:20
Add      00:A0:F8:FD:08:00    00:A0:F8:FD:08:20
;Delete  00:A0:F8:FD:05:00    00:A0:F8:FD:05:20

[AddressFilter]
Add      00:A0:F8:FF:00:03
Add      00:A0:F8:FF:00:04
Add      00:A0:F8:FF:00:05

[TypeFilter]
Add      807e
Add      6006
Add      8001
```

Select **Special Functions** from the **Main Menu**.

Select **Load ACL from File** to load site specific ACL.

3.9 Configuring Address Filtering

The access point can keep a list of MAC addresses of the clients 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 clients to access points. If no entries have been made for the ACL, the maximum number of entries is `512`. This is the total number of entries available to both ACL and Disallowed Address Filtering entries.

- Select **Set Address Filtering** from the **Main Menu**.

3.9.1 Adding Disallowed clients

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

1. Select **Add -[F2]**. The access point prompts for a MAC address.

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

2. Enter the MAC address. You can enter MAC addresses without colons.

3.9.2 Removing Disallowed Clients

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

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

3.10 Configuring Type Filtering

Type Filtering prevents the access point from forwarding specific frames, including certain broadcast frames from devices unimportant to the wireless LAN that take up bandwidth. Filtering out unnecessary frames can improve performance. Packet types supported for the type filtering function include the 16-bit DIX Ethernet types. The list can include up to 16 types.

3.10.1 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.

3.10.2 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-[F1]**.

3.10.3 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 thespian **BAR** to toggle between the **Forward**, **Discard** or **Disable** type filtering and press **ENTER** to confirm the choice.
4. To save the **Type Filtering Setu***p* information to all access points with the same SSID, select **Save ALL APs-[F2]**. You can perform this option only among the same hardware platforms and firmware versions. You can only enable one type filtering option at a time.

3.11 Manually Updating the Access Point Configuration

You can manually update the configuration of an access point by editing the `AP_CFG.TXT` file and using one of the following options to transfer the file:

- Telnet to the access point from a TFTP host computer using an Ethernet connection.
- Transfer the file with **Xmodem** file transfer protocol from a computer using a null modem serial cable.

Xmodem transfers require more time than TFTP transfers.

Before you update the access point, edit the `AP_CFG.TXT` file to match your site specific network settings.

Example AP_CFG.TXT file:

```
[APInstallation]
;UnitName              testhost.intel.com     ;up to 31 chars
;IPAddress             157.235.101.33        ;comment out if DHCP enabled
Gateway1               157.235.101.1
Gateway2               157.235.101.2
SubNetMask             255.255.255.0
NetID                  Engineering            ;up to 32 chars
AntennaSelect          Primary Only           ;"Full Diversity"
                                              ;"Primary Only"
                                              ;"Secondary Only"
                                                         ;"Rx Diversity"

DHCP                   Enabled                ; "Disabled"
                                              ; "Enabled"
                                              ; "DHCP Only"
                                              ; "BOOTP Only"
DNSServer1             157.235.101.1
DNSServer2             157.235.101.2
DNSServer3             157.235.101.3

[SpecialFunction]
FWFileName             intl3_fw.bin           ;up to 30 chars
HTMLFileName           intl3_htm.bin          ;up to 30 chars
ConfigFileName         ap_cfg.txt             ;up to 30 chars ***New***
ACLFileName            ap_acl.txt             ;up to 30 chars ***New***
;HelpURL               www.intel.com          ;up to 30 chars
TFTPServer             tftp.apfw.intel.com    ;ip address or name

[SystemConfig]
Channel                2                      ; 1 - 11
AutoChannelSelect      Disabled               ; "Disabled", "Enabled"
EthernetTimeOut        0                      ; 0: disabled,
                                              ; 1: hw detection,
                                              ; 2,3,4: WLAP detection,
                                          ; 30 - 255 seconds: sw detection
TelnetLogins           Enabled                ; "Disabled", "Enabled"
AgentAdInterval        0                      ; 0 - 1200 seconds
S24MobileIP            Disabled               ; "Disabled", "Enabled"
MobileHomeMD5Key       Intel                  ; up to 13 chars
InternationalMode      Disabled               ; "Disabled", "Enabled"
WebServer              Enabled                ; "Disabled", "Enabled"
AccessControl          Disabled               ; "Disabled", "Allowed",
"Disallowed"
```

```
TypeFiltering          Disabled               ; "Disabled", "Forward",
"Discard"

WNMPFunctions          Enabled                ; "Disabled", "Enabled"
APAPStateExchange     Enabled               ; "Disabled", "Enabled", "1",
"4"
TypeFiltering          Disabled               ; "Disabled", "Forward",
"Discard"
WNMPFunctions          Enabled                ; "Disabled", "Enabled"
APAPStateExchange     Enabled               ; "Disabled", "Enabled", "1",
"4"
EthernetInterface      On                     ; "Off", "On"
RFInterface            On                     ; "Off", "On"
DefaultInterface       Ethernet               ; "Ethernet",
MUMUDisallowed         Off                    ; "Off", "On"
;AdminPassword         Intel                  ; up to 13 chars
;UserPassword          Intel                  ; up to 13 chars
InactivityTimeout      5                      ; 0 - 9999
ModemConnected         No                     ; "No", "Yes"
Kerberos               Disabled               ; "Disabled", "Enabled"
KDCName                krbtgt                 ; up to 128 chars
KSSName                ksssrv                 ; up to 128 chars
KSSPort                34567                  : 0 - 99999
RealmName              apfw.intel.com         ; up to 128 chars
KerberosUserID         KerberosTest           ; up to 32 chars
KerberosPassword       Intel                  ; up to 32 chars
TimeZone               PST                    ; GMT, BST, IST, WET, WEST,
                                             ; CET, CEST, EET, EEST, MSK,
                                              ; MSD, AST, ADT, EST, EDT,
                                              ; CST, CDT, MST, MDT, PST,
                                              ; PDT, HST, AKST, AKDT, WST
ClockSkew              300                    ; 0 - 99999

[RFConfig]
DTIMInterval           10                     ; 1- 255
BCMCQMax               100                    ; 0 - 100
ReassemblyTimeout      9000                   ; 0 - 9999
MaxRetriesData         15                     ; 0 - 32
MaxRetriesVoice        5                      ; 0 - 32
MulticastMaskData      09000E00
MulticastMaskVoice     01005E00
BeaconInterval         100                    ; 20 - 1000
AcceptBroadcastESSID   Disabled               ; "Disabled", "Enabled"
MUInactivityTimeout    60                     ; 3 - 600
TransmitRate1          Required               ; "NotUsed", "Optional",
"Required"
TransmitRate2          Required               ; "NotUsed", "Optional",
"Required"
TransmitRate5.5        Optional               ; "NotUsed", "Optional",
"Required"
```

```
TransmitRate11         Optional               ; "NotUsed", "Optional",
"Required"
FragmentationThreshold 572                    ; 256 - 2346
RTSThreshold           100                    ; 0 - 2347
WLAPMode               Disabled               ; "Disabled",
                                              ; "Enabled",
                                              ; "LinkRequired"
WLAPPriority           8000                   ; 0 - FFFF
WLAPManualBSSID        00:A0:F8:00:B8:B9
WLAPHelloTime          20                     ; 0 - 9999
WLAPMaxAge             100                    ; 0 - 9999
WLAPForwardDelay       5                      ; 0 - 9999
WEPPrivacy             Disabled               ; "Disabled", "Enabled"
WEPAlgorithm           40BitSharedKey         ; 40BitSharedKey
                                              ; 128BitSharedkey"
EncryptionKeyID        1                      ;  1 - 4
EncryptionKey1         1011121314
EncryptionKey2         2021222324
EncryptionKey3         3031323334
EncryptionKey4         4041424344
TxPowerControl         Full                   ; "Full", "30mW", "15mW",
"5mW", "1mW"

[SNMPConfig]
AgentMode              ReadOnly               ; "Disable",
                                              ; "ReadOnly",
                                              ; "ReadWrite"
TrapHost1              157.235.101.101        ; ip address or name
TrapHost2              157.235.101.102        ; ip address or name
ReadOnlyCommunity      public                 ; up to 31 chars
ReadWriteCommunity     admin                  ; up to 13 chars
AllTraps               Enabled                ; "Disabled", "Enabled"
ColdBoot               TrapHost2Only          ; "Disabled",
                                              ; "TrapHost1Only"
                                              ; "TrapHost2Only"
                                              ; "AllTrapHosts"
AuthenticationFailure  TrapHost1Only          ; "Disabled",
                                              ; "TrapHost1Only"
                                              ; "TrapHost2Only"
                                              ; "AllTrapHosts"
RadioRestart           TrapHost2Only          ; "Disabled",
                                              ; "TrapHost1Only"
                                              ; "TrapHost2Only"
                                              ; "AllTrapHosts"
AccessViolation        AllTrapHosts           ; "Disabled",
                                              ; "TrapHost1Only"
                                              ; "TrapHost2Only"
                                              ; "AllTrapHosts"
MUStateChange          TrapHost1Only          ; "Disabled",
                                              ; "TrapHost1Only"
                                              ; "TrapHost2Only"
                                              ; "AllTrapHosts"
WLAPConnectionChange   TrapHost2Only          ; "Disabled",
                                              ; "TrapHost1Only"
                                              ; "TrapHost2Only"
                                              ; "AllTrapHosts"
DHCPChange             AllTrapHosts           ; "Disabled",
                                              ; "TrapHost1Only"
                                              ; "TrapHost2Only"
                                              ; "AllTrapHosts"
KerberosError          TrapHost2Only          ; "Disabled",
                                              ; "TrapHost1Only"
                                              ; "TrapHost2Only"
                                              ; "AllTrapHosts"

[EventLogConfig]
AnyEventLogging        Enabled                ; "Disabled","Enabled"
SecurityViolation      Disabled               ; "Disabled","Enabled"
MUStateChanges         Enabled                ; "Disabled","Enabled"
WNMPEvents             Enabled                ; "Disabled","Enabled"
SerialPortEvents       Enabled                ; "Disabled", "Enabled"
APAPMessages           Disabled               ; "Disabled","Enabled"
TelnetLogins           Enabled                ; "Disabled","Enabled"
SystemEvents           Enabled                ; "Disabled","Enabled"
EthernetEvents         Disabled               ; "Disabled","Enabled"
```

3.11.1 Updating Configuration with TFTP

The Ethernet TFTP update method requires a connection between the access point and a computer on the same Ethernet segment. Make sure the computer 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 update method requires a connection between the access point and a TFTP server. The TFTP server can be running on an Intel® PRO/Wireless 2011B LAN device.

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

To update the access point configuration:

1. Copy the configuration file `AP_CFG.TXT` to the terminal or computer hard disk.
2. Telnet to the access point using its IP address.
3. At the prompt enter the password. The default is:

   `Intel`

   Note that the password is case-sensitive. You can change password in **System Passwords** in the **Set System Configuration** screen.

   The access point displays the **Main Menu.**
4. Select *S***pecial Functions** from the **Main Menu** and press enter.
5. Press **F3** to view the **Special Functions update** page.
6. Select **Alter Filename(s)/HELP URL/TFTP Server** and press **ENTER.**

7. Enter the configuration file name in the **Config. Filename** field. Change this only if the network administrator requires a new File name. The default is `AP_CFG.TXT`. Verify the path accuracy for the File name. See step one.
8. Enter the TFTP Server IP address or name in the **TFTP Server** field**.**
9. Press **F1** to save settings and type `Y` to confirm.

Caution

Do not use the **Use XMODEM to Update Access Point's Firmware** option on the access point's **Telnet** menu. This option causes the access point to reset and look for the configuration file over the serial interface.

10. Under the function heading **Use TFTP to Update Access Points**, select **Config**.
11. Press **ENTER** and type `Y` to confirm. This ends the Telnet session.

    Note that the Wired LAN Activity light on the access point does NOT flash during the transfer.

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

    The access point resets when the file transfer completes.

To verify that the network settings are correct:

1. Telnet to the access point using its IP address.
2. At the prompt enter the password:

    `Intel`

    Note that the password is case-sensitive. The access point displays the **Main Menu.**
3. View the network settings on the **System Summary** screen.
4. Press **CTRL+D** to end Telnet session.

3.11.2 Updating Configuration with Xmodem

The **Xmodem** upgrade method requires a direct connection between the access point and a computer using a null modem serial cable and using software like HyperTerminal for Windows 95.

Before you update the access point:

1. Copy the configuration file `AP_CFG.TXT` to the computer hard disk of the computer that you will use to transfer the file to the access point.
2. Attach a null modem serial cable from the access point to the computer serial port.

Note

The instructions below describe using Hyper Terminal on a computer running Windows.

To update the access point configuration:

1. On the computer connected to the access point, start the **Hyper Terminal** communication program.
2. Type a name for the session and click **OK**.
3. Select the correct communication port and set the following parameters:

emulation	ANSI
bits per second	19200

data bits	8
stop bits	1
parity	none
flow control	none

4. Click **OK** and press **ENTER** to display the access point **Main Menu**.
5. Select **Enter Admin Mode** and enter the password. The default is:
   `Intel`
   Note that the password is case-sensitive.
6. Enter the **Special Functions** screen**.**
7. Press **F3** to view the **Special Functions update** page.
8. Under **Use XMODEM to Update Access Points,** select **Config.**
9. Press **ENTER** and type `Y` to confirm downloading the file `AP_CFG.TXT`.

Caution

Make sure the file is correct before sending. An incorrect file can render the access point inoperable.

10. From the **Hyper Terminal Transfer** menu, click **Send File**.
11. Click the **Browse** button and locate the file `AP_CFG.TXT`.
12. Select the **XModem** protocol from the drop down list.
13. Click the **Send** button.

Hyper Terminal displays the transfer process through a progress bar. The download is complete when the terminal screen displays:

```
Download Successful
Updating AP
Set Successful
```

If the transfer fails, the access point displays an error message indicating the cause.

The access point automatically resets after the file transfer completes. Exit the communication program to terminate the session.

3.12 Clearing Clients from the Access Point

You can clear the client computer association table for diagnostic purposes. Clear clients from the access point if the access point has many client associations no longer in use. Use this option to make sure that clients associating with the access point are active.

To clear clients associated with the access point:

1. Select **Special Functions** from the **Main Menu**.
2. Select **Clear MU Table**. The access point removes the clients associated with it. Clients cleared from the access point try to reassociate with the access point or another nearby access point.

3.13 Setting Logging Options

The event log kept by the access point allows you to log important events. You can select the events that you want to log.

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

Any Event Logging	Logs all events listed in the screen.
Security Violations	ACL filter or administrative password access violations.
MU State Changes	Allows logging all client computer state changes.
WNMP Events	WNMP events such as computers using WNMP.
Serial Port Events	Serial port activity.
AP-AP Msgs	Access point-to-access point communication.
Telnet Logins	Telnet sessions for monitoring and administration.
System Events	Internal use only.
Ethernet Events	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.
5. Select **Save ALL APs-[F2]** to save the **Event Logging Configuration** information to all access points with the same SSID. This option saves the configuration changes for the current access point, and sends two messages to all other access points on the **Known APs** table to update their configuration and reset after the configuration has been modified. You can perform this option only among the same hardware platforms and firmware versions.

3.14 Manually Updating Access Point Firmware

Options for manually updating the firmware:

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

The files required for firmware updates are `DSAP_FW.BIN` and `INTL_HTM.bin`.

3.14.1 Updating Firmware with TFTP

The Ethernet TFTP upgrade method requires a connection between the access point and computer on the same Ethernet segment. Verify that the computer 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 access point and a TFTP server. The TFTP server can be running on an Intel® PRO/Wireless 2011B LAN device.

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

To update the access point firmware:

1. Copy the Firmware files `DSAP_FW.BIN` and `INTL_HTM.bin` on the terminal or computer hard disk.
2. Telnet to the access point using its IP address.
3. At the prompt type the password. The default is:

   `Intel`

   Note that the password is case-sensitive.

   The access point 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.

   The defaults are `DSAP_FW.BIN` and `INTL_HTM.bin`. Make sure you use these names unless you changed the filename. Also make sure the path for the file is correct. (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 access point through an Ethernet interface, do not use the **Use XMODEM to Update Access Point's Firmware** option. This option causes the access point to reset and look for the firmware file over the serial interface.

10. Select **Special Functions** from the **Main Menu**.
11. Under the heading **Use TFTP to Update Access Point**, select **Firmware HTML** or **Both** and press **ENTER**.
12. Press **Y** to confirm. This ends the Telnet session.

    Note that the Wired LAN Activity light on the access point does NOT flash during the transfer.

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

    The access point resets when the file transfer and FLASH programming completes.

To verify the accuracy of the firmware version number:

1. Telnet to the access point using its IP address.
2. At the prompt enter the password. The default is:

   `Intel`

   Note that the password is case-sensitive.

   The access point displays the **Main Menu.**
3. View the version number on the **System Summary** screen.
4. Press **CTRL+D** to end Telnet session.

3.14.2 Updating Firmware with Xmodem

The **Xmodem** upgrade method requires a direct connection between the access point and computer using a Null modem serial cable and software like HyperTerminal for Windows 95[†]. Xmodem supports file transfers between terminal emulation programs and the access point.

Before you update the access point:

1. Copy the configuration file AP_CFG.TXT to the computer hard disk of the computer that you will use to transfer the file to the access point.
2. Attach a null modem serial cable from the access point to the computer serial port.

The instructions below describe using Hyper Terminal on a computer running Windows.

To update the access point configuration:

1. On the computer connected to the access point, start the **Hyper Terminal** communication program.
2. Type a name for the session and click **OK**.
3. Select the correct communication port and set the following parameters:

emulation	ANSI
bits per second	19200
data bits	8
stop bits	1
parity	none
flow control	none

4. Click OK and press **ENTER** to display the access point **Main Menu**.
5. Select **Enter Admin Mode** and enter the password:

```
Intel
```

   Note that the password is case-sensitive.

6. Enter the **Special Functions** screen.
7. Under the function heading **Use XMODEM to Update Access Points**, select **Firmware HTML**. Selecting **Both** downloads the `DSAP_FW.BIN` and `INTL_HTM.bin` files separately. Make sure that both files are located in the same directory before the download begins.
8. Press **ENTER**.
9. At the confirmation prompt, press **Y** to display:

```
Downloading firmware using XMODEM.
Send firmware with XMODEM now ...
```

Make sure the file is correct before sending. An incorrect file can render the access point inoperable.

10. From the **Hyper Terminal Transfer** menu, click **Send File**.
11. Select the **Browse** button and locate the one files, `DSAP_FW.BIN` or `INTL_HTM.bin`.
12. Select the **XModem** protocol from the drop down list.
13. Click the **Send** button.

Hyper Terminal displays the transfer process through a progress bar. The download is complete when the terminal screen displays:

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

If the transfer fails, the access point displays an error message indicating the cause.

If you are downloading both files, repeat the steps beginning at step 10 to download the next file and avoid a transfer time-out error.

The access point automatically resets after the file transfer completes. Exit the communication program to terminate the session.

3.15 Auto Update All Access Points Through Messaging

The **Use TFTP to update ALL Access Points** option upgrades or downgrades the firmware of all associated access points with the same Network Name (SSID) on the same subnet and includes all recognized hardware platforms regardless of firmware version. The initiating access point sends the correct file name for each Intel platform. The initiating access point does not send update commands to non-Intel platforms.

You can find the specific access points that will have their firmware upgraded or downgraded on the **Known APs** screen. The time interval between the update firmware commands for updating each access point is two seconds. This interval prevents more than one access point from accessing the TFTP server and causing network congestion.

The Ethernet TFTP upgrade method requires a connection between the access point and computer on the same Ethernet segment. Verify that the computer has a TFTP server running on it. Running the server requires third party software such as FTP PC/TCP† for DOS† or OnNet† for Windows†.

The wireless TFTP upgrade method requires a connection between the access point and a TFTP server. The TFTP server can be running on an Intel® PRO/Wireless 2011B LAN device.

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

To update the access point firmware:

1. Copy the Firmware files `DSAP_FW.BIN` and `INTL_HTM.bin` on the terminal or computer hard disk.
2. Telnet to the access point using its IP address.
3. At the prompt type the password. The default is:

   `Intel`

   Note that the password is case-sensitive.

   The access point 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 intl_htm.bin`

Caution

Make sure the file name is `DSAP_FW.BIN` and `INTL_HTM.bin` unless the you changed the filename.

7. Type the TFTP Server IP address in the **TFTP Server** field and press **ENTER**.

8. Select **Save Configuration** to save settings.
9. Select **Special Functions** from the **Main Menu**.
10. Select **Use TFTP to update ALL Access Points** and press **ENTER**.
11. Press **Y** to confirm. This ends the Telnet session.

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

The access point resets when the file transfer and FLASH programming completes.

To verify the accuracy of the firmware version number:

1. Telnet to the access point using its IP address.
2. At the prompt enter the password. The default is:

   `Intel`

   Note that the password is case-sensitive. The access point displays the **Main Menu.**
3. View the version number on the **System Summary** screen.
4. Press **CTRL+D** to end Telnet session.

3.16 Performing Pings

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

Note

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

No pings returned or fewer pings returned than sent can indicate a communication problem between the access point and the other station.

To ping another station:

1. Select the **Show Mobile Units** screen from the **Main Menu**.
2. Select **Regular** from the **Show Mobile Units** screen.
3. Press the **TAB** key to highlight the MAC address of the station to ping.
4. Select **Ping-[F1]** to display the **Packet Ping Setup** screen:
5. 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`).
6. Select **Start-[CR]** to begin. The access point dynamically displays packets transmitted and received.

3.17 Mobile IP Using MD5 Authentication

You can achieve authentication by using the *MD5 algorithm* with a shared key configured into the access point and its client. 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. The message-digest is the authentication checksum of a message from a mobile client to an access point during the Home Agent registration process.

The purpose of the MD5 algorithm is to prevent an outside computer or entity from impersonating an authenticated client. You can think of the message-digest as a *fingerprint* of the original message that is computed using a mathematical formula, or algorithm. The probability of an outside entity reproducing the MD5 message-digest is similar to the remote chance that two people will have the same fingerprints.

3.18 Saving the Configuration

The access point keeps only saved configuration changes after a reset.

To make configuration changes permanent:

1. Select **Special Functions** from the **Main Menu**.
2. From the **Special Functions** menu, 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. You 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 *3.20 Restoring the Factory Configuration* on page 60.

3.19 Resetting the Access Point

Resetting an access point clears statistics and restores the last saved configuration. If You make unsaved changes, the access point clears those changes and restores the last saved configuration on reset.

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

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

3.20 Restoring the Factory Configuration

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

DHCP Disabled all access point configuration and statistics are reset, except the **Access Point Installation** screen

DHCP Enabled all access point configuration and statistics are reset

To restore factory configuration:

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

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

3.21 Troubleshooting

If you have problems with your wireless network, check the following before contacting the Intel Support Center:

- Verify access point operation:
  - — If the access point does not power up, make sure the power supply is plugged into an AC outlet with power, and connected to the access point.
  - — After the access point 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 access point resets. The LEDs turn off sequentially as each test passes.
- Identify wired network problems:
  - — Check access point configuration through Telnet, PPP or Web browser. Review procedures for Ethernet and serial connection of the access point. Review access point 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. Make sure that no other device responds to that address.
  - — If the access point is powered on but has no connection to the wired network, check connections for proper wiring.
- Check network wiring and topology for proper configuration:
  - — Check that the cables used have proper pinouts and connectors.
  - — Check router configuration and filtration settings.
  - — Make sure that network use does not exceed 37% of bandwidth.
  - — Check client operations.
  - — Confirm access point and client SSID.
  - — Make sure that the radio driver loaded properly.
  - — Make sure that the client computer `PROTOCOL.INI` or `NET.CFG` file is compatible with the network operating system.
- If performance is slow or erratic:
  - — Check client computer and RF communications range.
  - — Check antenna, connectors and cabling.
  - — Make sure the access point antenna diversity setting is appropriate.
    `Full Diversity`: The radio receives on the antenna that has the best signal and transmits on the last antenna it received on.
    `Primary Only`: The radio transmits and receives on the primary antenna only.
    `Secondary Only`: The radio transmits and receives on the secondary antenna only.
    `Rx Diversity`: The radio receives on the antenna that has the best signal and transmits on primary antenna.
  - — Make sure network traffic does not exceed 37% of bandwidth.
  - — Check to see that the wired network does not exceed 10 broadcast messages per second.
  - — Make sure wired network topology and configuration.

For more troubleshooting information, browse the Intel customer support web site (http://support.intel.com).

Chapter 4. Monitoring Statistics

The access point 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.

4.1 System Summary

The *Show System Summary* screen displays information about the access point's configuration.

To view information about the access point configuration, select *Show System Summary* from the *Main Menu*.

Unit Name Identifies the access point name.

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

IP Address Identifies the network-assigned Internet Protocol address.

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

Channel Identifies the direct-sequence channel used by the access point. The channel used is within the range required for the operating country.

Country Identifies access point country code that in turn determines the access point direct-sequence channel range.

Antenna Selection Indicates if the access point is configured for single or dual antenna mode.

WEP (Privacy) Defines the WEP algorithm. Admin privileges are required to make changes to this parameter. The default is `Disabled`.

WEP Algorithm 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`.

Current computers Specifies the current number of associated clients.

Total Assoc Specifies the total client associations handled by this access point.

System Up Time Specifies how long the system has been operational. **System Up Time** resets to zero after `119,304` hours.

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

WLAP Mode Specifies if wireless access point operation status is enabled.

If enabled, the access point sets up automatically for wireless operation. This feature is `Disabled` by default.

Model Number Identifies the model number.

Serial Number States the access points unique identifier.

Hardware Revision Specifies the hardware version.

AP Firmware Ver Specifies the firmware version.

RF Firmware Ver	Specifies the Radio firmware version.
HTML File Ver	Specifies the HTML file version.
Start Flashing All LEDs	Begins a test routine to check the LED functionality and allows you to determine the access point location.
Reset AP	Clears the access points statistics and restores the last saved configuration.

4.2 Interface Statistics

The **Interface Statistics** screen provides:

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

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

- Select *I***nterface Statistics** from the **Main Menu**.
  - — 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.

4.3 Forwarding Counts

Forwarding Counts provides information on packets transmitted from one interface to another (**Ethernet**, **PPP**, **RF**, **AP**). Forwarding Counts also displays the broadcast packets transmitted from the access point.

- Select **Forwarding Counts** from the **Main Menu**.
  - — Select **Refresh** at the status display to update the values manually.
  - — Select **Timed** to automatically update the display every two seconds.
  - — Press **ESC** to return to the previous menu.

4.4 Client Statistics

Mobile Units statistics provide information on clients associated with the access point. The statistics include information on data sent and received, activity and association. A client shows only in the **Home/Foreign Agent Table** screens when a client has roamed to another access point on a different subnet. Once a client has roamed, the client *IP Address* displays on the **Home Agent Table** screen of the client “home” access point with the IP Address of the *Foreign Agent* to tell the “home” access point where to forward packets.

The client IP Address is also shown in the **Foreign Agent Table** and **Regular** screens of the new “foreign” access point to tell the new access point where to expect packets from for newly associated clients. The access point **Regular** screen shows the clients associated locally on the same subnet.

- Select **Show Mobile Units** from the **Main Menu**.

Use the **TAB** or arrow keys to select your choice and press **ENTER**.

- Select **Regular** from the **Mobile Units** prompt.

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

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

where:

addr client MAC address in `xx:xx:xx:xx:xx:xx` format

p clients power mode: `P` for PSP, `C` for CAM. An unassociated client does not display any character.

i client location on access point interfaces. `R` for radio, `P` for PPP. Clients with an `A` were associated with the access point in the past, but no longer associate with it at time of verifying status.

Access point current Radio transmit rate for the messages sent to this client: `11` for 11 Mbps.

e Encryption is enabled for this device.

V Indicates an Intel Voice enabled device.

- To bring up the **Packet Ping Setup** screen, press **TAB** to highlight the client and select **Ping**. This allows the access point to ping a client. See *3.16 Performing Pings* on page 59.
  - — Select **Refresh** at the status display to update the values manually.
  - — Select **Next** to display the next screen.
  - — Press **ESC** to return to the previous menu.
- To bring up detailed information on a client, press **TAB** to highlight the client computer and select **Information**.

Displayed information includes:

Interface The access point interface shows the client connection as: **RF**, **Ethernet**, **PPP** or **AP**.

State The connection state between the access point and the client:

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

Power Mode The client power mode: CAM, PSP or N/A.

Station ID The IEEE 802.11 specification requires that each access point assign a station ID to all associated clients, regardless of the client power mode. (PSP or CAM)

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

Supported Rates Data transmission rates the station supports.

Current Xmt Rate The current rate the access point transmits data to the station.

Priority Indicates whether the client is a voice or data type device. **Voice** indicates packet delivery is time critical and a high priority. `Normal` indicates packet delivery is not time critical.

Encryption client encryption support: `On` or `Off`.

Packets Sent The packets sent by the access point to the client.

Packets Rcvd The packets received by the access point from the client.

Bytes Sent The bytes sent by the access point to the client.

Bytes Rcvd The bytes received by the access point from the client.

Discard Pkts/CRC The packets discarded because of data error.

Last Activity The time in hours, minutes and seconds since the last communication with the client.

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

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

4.5 Mobile IP

The following tables display the mapping of clients to mobility agents. See *2.4.7 Data Encryption* on page 17.

- Select **Home Agent** from the **Show Mobile Units** prompt.
- Select **Foreign Agent** from the **Show Mobile Units** prompt.

4.6 Known Access Points

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

Note

The **Save All APs** function from the **Special Functions Menu** updates and configures access point firmware and HTML code for all access points shown in the **Known APs** menu. You can perform this option only among the same hardware platforms and firmware versions. See *3.4 Configuring System Parameters* on page 28.

- Select *Known APs* from the *Main Menu*.

The access point displays the following for each known access point:

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

IP Address the network-assigned Internet Protocol address

DS Channel The direct-sequence channel used by the access point.

computerS The clients associated with the access point.

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

FW_Ver the firmware version used by the specified access point

Away Determines if the access point functions as a part of the network or *away*. Away indicates the last known transmission took place 12 or more seconds before.

4.7 Ethernet Statistics

The access point keeps Ethernet performance statistics including packet transmission and data retries until reset.

- Select **Ethernet Statistics** from the **Main Menu**.

Packet display for Ethernet statistical units:

Packets Seen packets received on Ethernet interface

Packets Forwarded packets forwarded from Ethernet interface to other interfaces

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

Discarded/Forced packets discarded because of the applied address filters

Discarded/Buffer packets discarded because insufficient buffers in access point

Discarded/CRC packets discarded because of data errors

Broadcast/Multicast total broadcast or multicast packets received

Individual Address packets received with designated individual addresses

Packets Sent total packets sent out

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

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

4.8 Radio Statistics

The access point keeps radio performance statistics including packet and communication information.

To view RF statistics:

- Select **Show RF Statistics** from the **Main Menu**.

Radio performance statistics include:

Data Packets Sent	total data packets transmitted
Data Bytes Sent	total data packets transmitted in bytes
BC/MC Packets Sent	broadcast/multicast user data packets successfully transmitted
BC/MC Bytes Sent	broadcast/multicast user data bytes successfully transmitted
Sys Packets Sent	system packets successfully transmitted
SBC/MC Packets Sent	broadcast/multicast system packets successfully transmitted
Succ Frag Packets	fragmented packets successfully transmitted
Unsucc Frag Packets	fragmented packets unsuccessfully transmitted
Fragments Sent	packet fragments transmitted
Packets w/o Retries	transmitted packets not affected by retries
Packets w/ Retries	transmitted packets affected by retries
Packets w/ Max Retries	transmitted packets affected by the maximum limit of retries
Total Retries	retries occurring on the interface. A retry occurs if the device fails to receive an *acknowledgment (ACK)* from a destination
Data Packets Rcvd	total data packets received
Data Bytes Rcvd	total data packets received in bytes
BC/MC Packets Rcvd	broadcast/multicast user data packets successfully received
BC/MC Bytes Rcvd	broadcast/multicast user data bytes successfully received
Sys Packets Rcvd	system packets successfully received
SBC/MC Packets Rcvd	broadcast/multicast system packets successfully received
Succ Reass Packets	packets successfully reassembled
Unsucc Reass Packets	packets unsuccessfully reassembled
Fragments Rcvd	packet fragments received
Rcv Duplicate Pkts	Duplicate packets received by the access point. This indicates the access point sent an ACK, but the client did not receive it and transmitted the packet again.
Undecryptable Pkts	total data packets that could not be decrypted

Rcv CRC Errors Packets received that contained *Cyclic Redundancy Check* (*CRC*) errors. A client transmitted a corrupt data packet and failed to pass the CRC verification. Make sure that any acknowledgment of the data packet contains the correct CRC word. An incorrect CRC causes the access point to discard the data packet.

Rcv ICV Errors Packets received containing Identity Check Value (ICV) errors. A client 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** to update the values manually at the status display.

— Select **Timed** to automatically update the display every two seconds.

— Press **ESC** to return to the previous menu.

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

Current # WLAP Itf the current Wireless access point interfaces in use in a `1` to `4` range

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

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

The *1.7.2 Site Planning* on page 6 provides an explanation of a root access point.

Priority the WLAP priority value assigned to the access point under *3.5 Configuring Radio Parameters* on page 33.

Root Interface the interface leading to the root access point

Root Priority the priority value of the root access point

Root MAC Address the MAC address of the root access point

Root Path Cost the hops between the current WLAP and the root access point

Itf ID Identifies the wireless interface the access point uses to communicate with another device.

WLAP Itf MAC Addr States the MAC address of the associated WLAP.

Itf State identifies the state of the interface:

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

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

Designated Root ID An ID designated by the root access point. Access points in WLAP mode negotiate the position of Root access Point at power up. The access point with the lowest Root ID, path and WLAP ID becomes the root access point. 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 access point.

Designated Cost a path cost designated by the root access point

Designated WLAP ID a WLAP ID assigned by the root access point

Designated Itf ID an ID assigned by the root access point

— Select **Refresh** to update the values manually at the status display.

— Select **Timed** to automatically update the display every two seconds.

— Press **ESC** to return to the previous menu.

4.9 Miscellaneous Statistics

The access point 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**.

WNMP statistics include:

Echoes echo requests received by the access point

Pings ping requests received by the access point

Passthrough Echoes echoes for clients associated with the access point

SNMP statistics include:

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

Filter statistics include:

ACL Violations	attempts by client, not in ACL list to associate with this access point
Address	packets discarded by address filter
Type	packets discarded by type filter

Modem statistics for the serial port include:

Number of Dialouts	dial-out attempts by the access point
Dialout Failures	dial-out failures by the access point
Number of Answers	answer attempts by the access point
Current Call Time	current connection session length in seconds
Last Call Time	last connection session length in seconds

Mobile IP statistics include:

Agent Ad Sent	number of agent advertisements sent from the access point
Reg Request Received	number of Mobile IP registration requests received
Reg Reply Sent	number of Mobile IP registration replies sent

— Select **Refresh** to update the values manually at the status display.

— Select **Timed** to automatically update the display every two seconds.

— Press **ESC** to return to the previous menu.

4.9.1 Analyzing Channel Use

The access point 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**.

   The display shows counters for the packets sent, received and retries for each channel.
3. Press any key to continue.

4.9.2 Analyzing Retries

The access point 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**.

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

4.10 Event History

The access point 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 access point powered up or reset. The type of event logged follows the time stamp.

4.11 Clearing Statistics

To clear statistics:

1. Select **Special Functions** from the **Main Menu**.

2. Select **Clear All Statistics**. The access point zeroes all statistics.

Resetting the access point also clears statistics.

Chapter 5. Customer Support

5.1 Intel Automated Customer Support

You can reach Intel automated support services 24 hours a day, every day at no charge. The services contain the most up-to-date information about Intel products. You can access installation instructions, troubleshooting information, and product information.

5.1.1 User Guide on Your Product CD-ROM

For more information about installing drivers or troubleshooting other topics, see the online User Guide. To view the guide, insert the Intel CD in your drive and wait for the Autorun to display. Click the **User Guide** button to view the guide. Note that a web browser is required to view the guide.

5.1.2 Web and Internet Sites

• Support:	http://support.intel.com
• Network Products:	http://www.intel.com/network
• Corporate:	http://www.intel.com
• Newsgroups:	news://cs.intel.com
• FTP Host:	ftp://download.intel.com
• FTP Directory:	`/support/network/<device>/`

5.1.3 Customer Support Technicians

U.S. and Canada

If you are using this product in conjunction with Intel® PRO/Wireless 2011B LAN hardware in a business or office environment and want customer support, please call +1 916-377-7000 (7:00 – 17:00 M–F Pacific Time). You can also visit the Intel customer support web site (http://support.intel.com).

Worldwide Access

Intel has technical support centers worldwide. Many of the centers are staffed by technicians who speak the local languages. For a list of all Intel support centers, the telephone numbers, and the times they are open, refer to the Customer Support Phone Numbers web site (http://www.intel.com/support/9089.htm).

5.2 Intel Software License Agreement

IMPORTANT - READ CAREFULLY BEFORE COPYING, INSTALLING OR USING.

Do not use or load this software and any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

LICENSES

- If you are a network administrator, the "Site License" below shall apply to you.
- If you are an end user, the "Single User License" shall apply to you.

Site License

You may copy the Software onto your organiation's computers for your organization's use, and you may make a reasonable number of back-up copies of the Software, subject to these conditions:

1. **This Software is licensed for use only in conjunction with Intel component products. Use of the Software with non-Intel component products is not licensed hereunder.**
2. You may not copy, modify, rent, sell, distribute or transfer any part of the Software except as provided in this Agreement, and you agree to prevent unauthorized copying of the Software.
3. You may not reverse engineer, decompile, or disassemble the Software.
4. You may not sublicense or permit simultaneous use of the Software by more than one user.
5. The Software may include portions offered on terms in addition to those set out here, as set out in a license accompanying those portions.

Single User License

You may copy the Software onto a single computer for your personal, noncommercial use, and you may make one back-up copy of the Software, subject to these conditions:

1. **This Software is licensed for use only in conjunction with Intel component products. Use of the Software with non-Intel component products is not licensed hereunder.**
2. You may not copy, modify, rent, sell, distribute or transfer any part of the Software except as provided in this Agreement, and you agree to prevent unauthorized copying of the Software.
3. You may not reverse engineer, decompile, or disassemble the Software.
4. You may not sublicense or permit simultaneous use of the Software by more than one user.
5. The Software may include portions offered on terms in addition to those set out here, as set out in a license accompanying those portions.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS

Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You may not remove any copyright notices from the Software. Intel may make changes to the Software, or to items referenced therein, at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITED MEDIA WARRANTY

If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

EXCLUSION OF OTHER WARRANTIES

EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED “AS IS” WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the Software.

LIMITATION OF LIABILITY

IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

TERMINATION OF THIS AGREEMENT

Intel may terminate this Agreement at any time if you violate its terms. Upon termination, you will immediately destroy the Software or return all copies of the Software to Intel.

APPLICABLE LAWS

Claims arising under this Agreement shall be governed by the laws of California, excluding its principles of conflict of laws and the United Nations Convention on Contracts for the Sale of Goods. You may not export the Software in violation of applicable export laws and regulations. Intel is not obligated under any other agreements unless they are in writing and signed by an authorized representative of Intel.

GOVERNMENT RESTRICTED RIGHTS

The Software is provided with “RESTRICTED RIGHTS.” Use, duplication, or disclosure by the Government is subject to restrictions as set forth in FAR52.227-14 and DFAR252.227-7013 et seq. or its successor. Use of the Software by the Government constitutes acknowledgment of Intel’s proprietary rights therein. Contractor or Manufacturer is Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95052.

5.3 Limited Hardware Warranty

Intel warrants to the original owner that the hardware product delivered in this package will be free from defects in material and workmanship. This warranty does not cover the product if it is damaged in the process of being installed. Intel recommends that you have the company from whom you purchased this product install the product. Intel reserves the right to fill your order with a product containing new or remanufactured components.

THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF NON-INFRINGEMENT OF INTELLECTUAL PROPERTY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

This warranty does not cover replacement of hardware products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing.

If the hardware product is found to be otherwise defective, Intel, at its option, will replace or repair the hardware product at no charge except as set forth below, provided that you deliver the hardware product along with a Return Material Authorization (RMA) number (see below) either to the company from whom you purchased it or to Intel (North America only). If you ship the hardware product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge.

Intel may replace or repair the hardware product with either new or remanufactured product or parts, and the returned hardware product becomes Intel’s property. Repaired or replaced products will be returned at the same revision level as received or higher, at Intel’s option. Intel reserves the right to replace discontinued product with an equivalent current generation product.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this hardware product are covered by Intel’s limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

5.3.1 Returning a Defective Product

From North America

Before returning any hardware product, contact Intel Customer Support to obtain an RMA number by calling +1 916-377-7000.

If the Customer Support Group verifies that the hardware product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the hardware product. Intel cannot accept any product without an RMA number on the package.

All Other Locations

Return the hardware product to the place of purchase for a refund or replacement.

5.3.2 Limitation of Liability and Remedies

INTEL’S SOLE LIABILITY HEREUNDER SHALL BE LIMITED TO DIRECT, OBJECTIVELY MEASURABLE DAMAGES. IN NO EVENT SHALL INTEL HAVE ANY LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL, AND SPECIAL DAMAGES) INCLUDING, BUT NOT LIMITED TO, INFRINGEMENT OF INTELLECTUAL PROPERTY, REPROCUREMENT COSTS, LOSS OF USE, BUSINESS INTERRUPTIONS, LOSS OF GOODWILL, AND LOSS OF PROFITS, WHETHER ANY SUCH DAMAGES ARISE OUT OF CONTRACT, NEGLIGENCE, TORT OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES. NOTWITHSTANDING THE FOREGOING, INTEL’S TOTAL LIABILTIY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENIAL LIABLITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations may not apply to you.

Critical Control Applications

Intel specifically disclaims liability for use of the hardware product in critical control applications (including, for example only, safety or health care control systems, nuclear energy control systems, or air or ground traffic control systems) by you or your customers, and such use is entirely at the user’s risk. You agree to defend, indemnify, and hold Intel harmless from and against any and all claims arising out of use of the hardware product in such applications by you or your customers.

Software

Software provided with the hardware product is not covered under the hardware warranty described above. See the applicable software license agreement which shipped with the hardware product for details on any software warranty.

5.4 Product Registration

The Beginning of a Valuable Relationship…

Register Your Product Today!

As a registered customer, you stay connected and informed by receiving:

- Access to Intel’s outstanding technical support for optimum performance.
- Advance notice of product upgrades and new products to give you a competitive edge.
- Information updates to keep you current.
- Special offers for savings on products and evaluation units.

There are three easy ways to register:

- Browse the Intel product registration web site (http://www.intel.com/product/register).
- Mail the attached postage prepaid registration card.
- Fax the attached registration card to +1 608-757-1727.

Chapter 6. Regulatory Compliance Information

For U.S. and international regulatory compliance information for the Intel® PRO/Wireless 2011B LAN, please see the Regulatory Specifications posted at the Intel customer support web site (http://support.intel.com).

Important Regulatory Compliance Instructions

If your country is listed on the regulatory labels included with the Intel® PRO/Wireless 2011B LAN hardware, remove the label for your country and attach it to the bottom of the device in the space provided. Failure to apply the label for the appropriate country constitutes a breach of law.

Warning

A minimum separation distance of 20 cm (8 inches) should be maintained between the radiating element of this product and nearby persons to comply with FCC rules for RF exposure.

Index