SAP2315A
802.11b/g Access Point

Management Guide

Management Guide

802.11b/g Access Point

IEEE 802.11b/g Wireless Access Point

SAP2315A
E062006-EK-R01
FEGFT2315000E

Table of Contents

Chapter 1: Initial Configuration **1-1**

Logging into the Web Interface 1-1
Using the Setup Wizard 1-2

Chapter 2: System Configuration **2-1**

Information 2-3
System 2-3
Client 2-4
Network 2-5
Event Log 2-6
System Settings 2-7
Administration 2-7
Operation Mode 2-8
Reboot System 2-8
Wireless VAP Settings 2-10
Basic 2-10
Channel Setting 2-11
WEP Security 2-11
WPA-PSK Security 2-12
Network Settings 2-14
DHCP Client 2-14
DHCP Server/NAT 2-15
PPPoE 2-17
Time and Log 2-18
Updating Firmware 2-20
Upgrade via the Web Page 2-20
Upgrade via a Remote Server 2-20

Appendix A: Troubleshooting **A-1**

Glossary

Index

Chapter 1: Initial Configuration

The Access Point offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 5.0 or above).

The initial configuration steps can be made through the web browser interface using the Setup Wizard. It is recommended to make the initial changes by connecting a PC directly to the access point before installing it in its intended location. The access point has a default IP address of 192.168.1.20 and a subnet mask of 255.255.255.0. If your PC has an IP address on the same subnet (that is, the PC and access point addresses both start 192.168.1.x), you can connect immediately to the web interface. Otherwise, you must first change your PC's IP address to be on the same subnet as the access point.

Logging into the Web Interface

In the web browser's address bar, type the default IP address: http://192.168.1.20. The web browser displays the access point's login page.

The User ID is fixed as "admin." There is no default password, so just leave the Password box blank and click LOGIN.

Note: It is strongly recommended that you configure a password. If a password is not configured, the management interface is not protected and anyone that can connect to the access point may be able to compromise your network security. For information on configuring a password, see "Administration" on page 2-7.

Figure 1-1. Login Page

The home page displays the Main Menu. There are two options available, you can configure the basic features of the access point using the Setup Wizard's simple steps, or you can configure all features in detail using the Advanced Setup menu.

Figure 1-2. Home Page

Using the Setup Wizard

There are only a few basic steps you need to set up the access point and provide a connection for your Wi-Fi phone and network access for other wireless stations.

The Setup Wizard takes you through configuration procedures for the general network settings, such as IP configuration, wireless network name (Service Set Identifier), and wireless security. Follow these steps:

1. **Launch the Setup Wizard** – Click "Start with Setup Wizard" on the home page.

2. **Operation Mode Setting** – Select an operation mode according to how your divice will function.

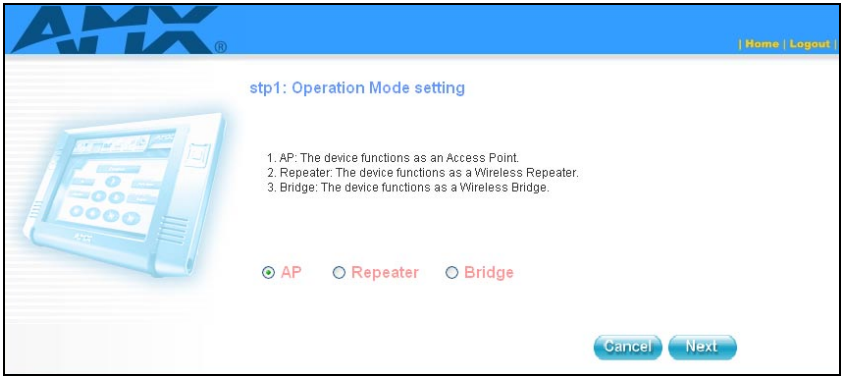


Figure 1-3. Setup Wizard - Network Setting (AP)

There are three operation modes:

- **AP** — Set the device as an Access Point.
- **Repeater** — Set the device as a Wireless Repeater to relay messages between subnetworks that use different protocols or cable types. The Root AP MAC Address can be assigned manually or selected after click “Scan”.

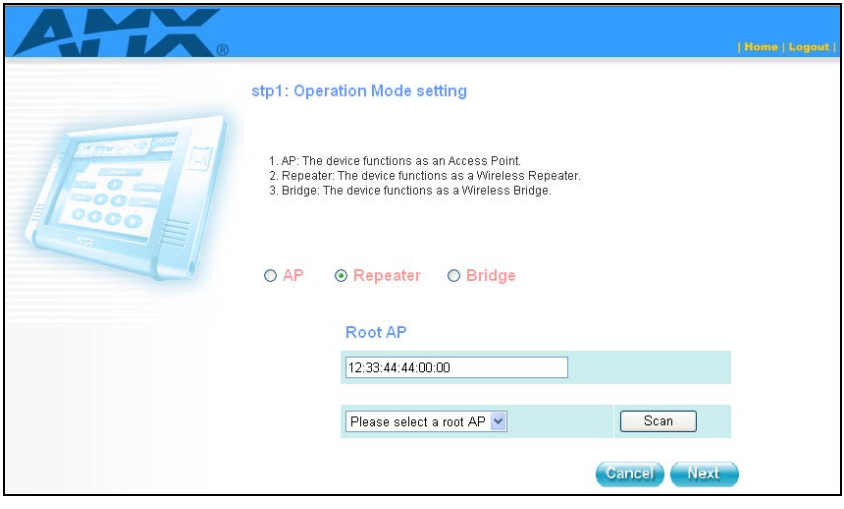


Figure 1-4. Setup Wizard - Network Setting (Repeater)

- **Bridge** — Set the device as a Wireless Bridge to connect two local-area networks (LANs), or two segments of the same LAN that use the same protocol. The Bridge Nodes need to be assigned manually by the user.

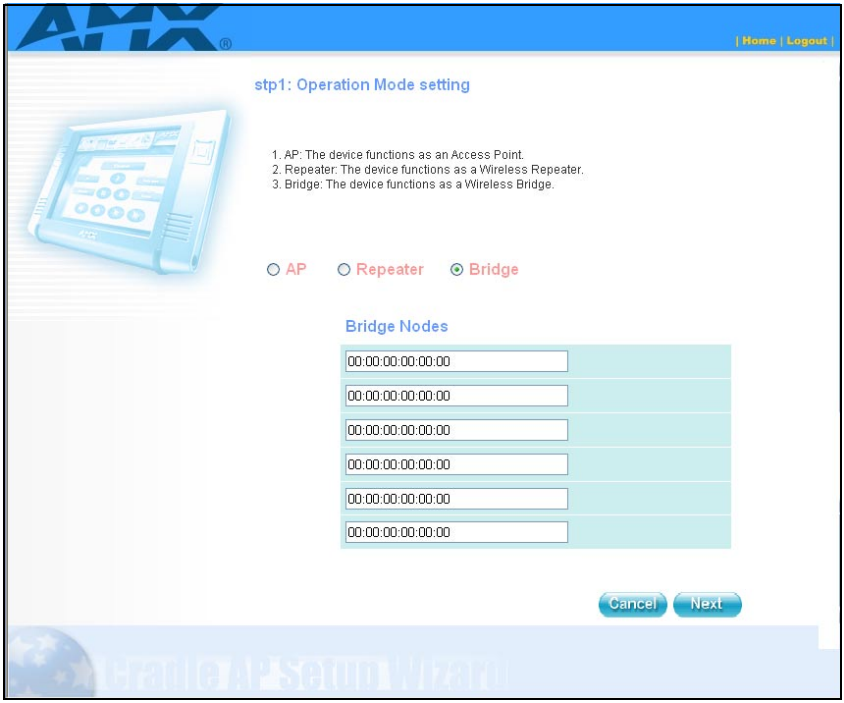


Figure 1-5. Wizard - Network Setting (Repeater)

3. **Network Setting** – Sets the access point's IP address assignment method and configures the local Dynamic Host Configuration Prototcol (DHCP) server and Network Address Translation (NAT) settings.

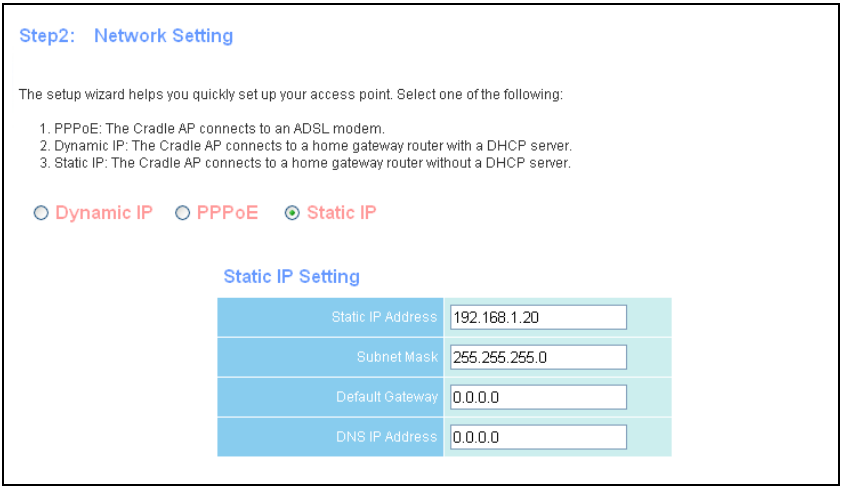


Figure 1-6. Setup Wizard - Network Setting

There are three basic methods for configuring the access point's IP address:

- **Dynamic IP** — The IP address is assigned automatically from a home gateway router or other device that has a DHCP server feature.
- **PPPoE** — The IP address is assigned automatically from an Internet service provider (ISP) through an ADSL modem using Point-to-Point Protocol over Ethernet (PPPoE). If your ISP has provided you with a user name and password, enter these in the corresponding text boxes under PPPoE Setting.
- **Static IP** — The IP address is assigned manually by the user. This may be required if your access point is connected to a home gateway router or other device that does not support a DHCP server.

If you select Static IP, enter an appropriate IP address and subnet mask that are compatible with your existing network. If a management station exists on another network segment, then you must enter the IP address for a Default Gateway that can route traffic between these segments. Also enter the IP address for the Domain Name Server (DNS) to be used for host-name to IP address resolution.

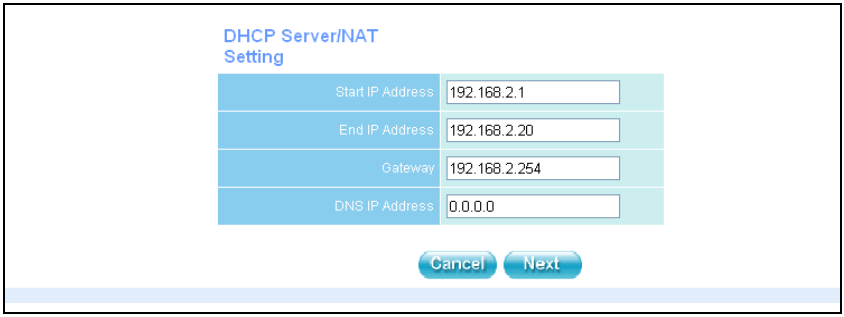


Figure 1-7. Setup Wizard - DHCP Server and NAT Settings

DHCP Server/NAT Setting — This access point includes a DHCP server that can assign IP addresses to any wireless station or Wi-Fi phone requesting the service. Addresses are assigned from a common address pool configured on the access point. You can configure the address pool by specifying start and end IP addresses.

NAT is a standard method of mapping multiple “internal” IP addresses to one “external” IP address on devices at the edge of a network. For the access point, the internal (local) IP addresses are the IP addresses assigned to wireless clients by the DHCP server, and the external IP address is the IP address assigned to the access point itself. Note that the access point IP address is always in a different subnet from the DHCP server pool. The access point uses the NAT IP settings to route traffic from the wireless interface to the Ethernet network.

4. **Wireless VAP #1 Setting** – Sets the wireless Service Set Identifier (SSID) and wireless security encryption key for the VAP#1 network. Note that it is recommended to restrict one VAP network for only Wi-Fi phones and let all other wireless stations use the other VAP network.

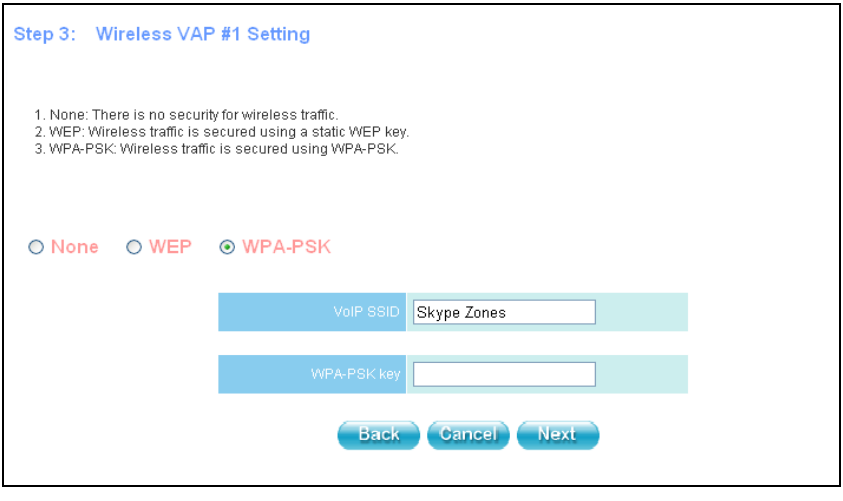


Figure 1-8. Setup Wizard - Setting the VAP#1 SSID and Security

Enter the SSID, or wireless network name, which all wireless stations must use to associate with the access point. The SSID is case sensitive and can consist of up to 32 alphanumeric characters (Default: Skype Zones).

The access point offers two wireless security options; Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access Pre-shared Key (WPA-PSK). Select the security you want to use and enter the appropriate encryption key, or select “none” for no security.

- **WEP Key** — Enter 10 hexadecimal digits (0 to 9 and A to F) or 5 alphanumeric characters for 64 bit keys, 26 hexadecimal digits or 13 alphanumeric characters for 128 bit keys, and 32 hexadecimal digits or 16 alphanumeric characters for 152 bit keys.
- **WPA-PSK Key** — Enter as an easy-to-remember form of letters and numbers. The key must be from 8 to 63 characters, which can include spaces.

Note: All wireless devices must be configured with the same WEP or WPA-PSK Key values to communicate with the access point.

5. **Wireless VAP #2 Setting** – Sets the wireless Service Set Identifier (SSID) and wireless security encryption key for the VAP#2 wireless network.

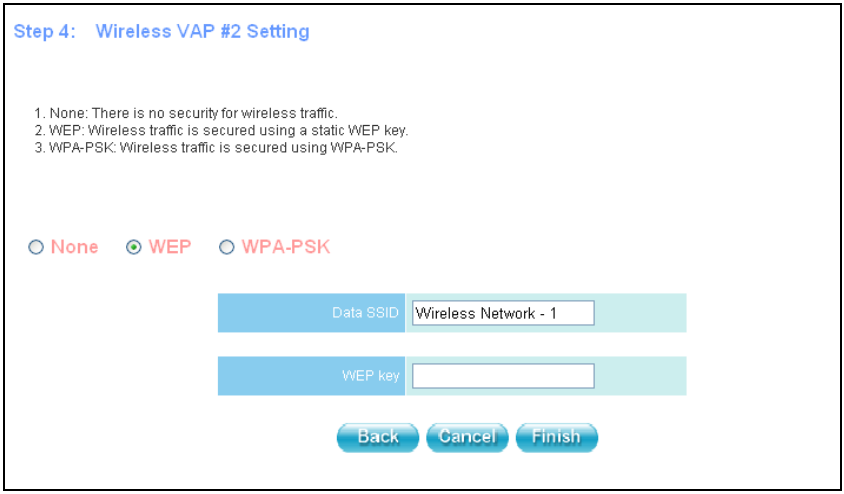


Figure 1-9. Setup Wizard - Setting the VAP#2 SSID and Security

Enter the SSID, or wireless network name, which all wireless stations must use to associate with the access point. The SSID is case sensitive and can consist of up to 32 alphanumeric characters (Default: Wireless Network - 1).

The access point offers two wireless security options; Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access Pre-shared Key (WPA-PSK). Select the security you want to use and enter the appropriate encryption key, or select “none” for no security.

- **WEP Key** — Enter 10 hexadecimal digits (0 to 9 and A to F) or 5 alphanumeric characters for 64 bit keys, 26 hexadecimal digits or 13 alphanumeric characters for 128 bit keys, and 32 hexadecimal digits or 16 alphanumeric characters for 152 bit keys.
- **WPA-PSK Key** — Enter as an easy-to-remember form of letters and numbers. The key must be from 8 to 63 characters, which can include spaces.

Note: All wireless devices must be configured with the same WEP or WPA-PSK Key values to communicate with the access point.

6. Click Finish.

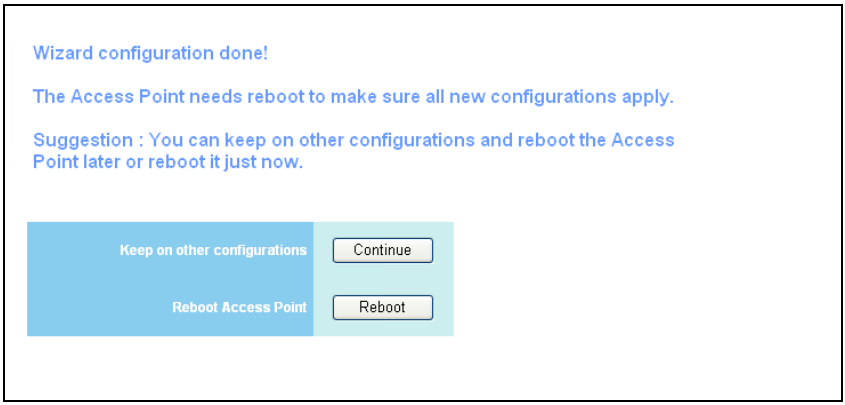


Figure 1-10. Setup Wizard - Finish

7. Click the Reboot button to restart the access point.

   Note that the access point will start using any configured new IP settings, which must be used to access the web management interface.

Chapter 2: System Configuration

The access point's basic settings can be configured using the Setup Wizard, as described in the previous chapter, "Initial Configuration." However, for some installations, you may need to configure specific settings that are not available in the Setup Wizard. The Advanced Setup menu provides access to all the unit's settings for complete control of the access point's features.

To access the Advanced Setup menus, follow these steps:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.1.20 or the IP address set through the Wizard.
2. Log into the access point management interface by leaving the password blank (the default), and click "LOGIN."
3. When the home page displays, click on Advanced Setup. The following page displays.

Figure 2-1. Advanced Setup

The information in this chapter is organized to reflect the structure of the web management screens for easy reference. However, it is recommended that you first configure a password to control access to the management interface. For details, see "Administration" on page 2-7.

The Advanced Setup pages include the options in the table below. For details on configuration for each feature, see the corresponding page number.

Table 2-1. Configuration Options

Menu	Description	Page
Information		
System	Displays a summary of access point settings	2-3
Client	Displays information on stations associated to the access point	2-4
Network	Displays DHCP client, server, NAT, and PPPoE settings	2-5
Event Log	Displays the system message log	2-6
System		
Administration	Configures the password for management access	2-7
Operation	Sets the device function	2-8
Reboot System	Restarts the system and resets configuration settings to factory defaults	2-8
Wireless VAP 1, 2		
Basic	Enables the VAP interface and sets the SSID	2-10
Channel	Sets the radio channel	2-11
WEP	Configures WEP security	2-11
WPA-PSK	Configures WPA-PSK security	2-12
Network		
DHCP Client	Enables DHCP client or manually sets an IP address	2-14
DHCP Server/NAT	Enables DHCP server and configures NAT settings	2-15
PPPoE	Configures PPPoE settings	2-17
Time & Log		
SNTP	Sets the system clock using SNTP	2-18
Update		
Upgrade via the Web Page	Upgrades system software from a local file	2-20
Upgrade via a Remote Server	Upgrades system software from a file on an FTP or TFTP server	2-20

Information

The system information pages display details on the current configuration and status of the access point, including associated wireless stations and event log messages.

System

The system information page displays basic system configuration settings, as well as the settings for each wireless interface. The displayed settings are for status information only and are not configurable on this page.

AP System Configuration	
System Up Time	Day 0, 1:08:18
MAC Address	00-12-CF-21-CD-73
IP Address	192.168.1.20
IP default-gateway	0.0.0.0
HTTP Server	Enabled
HTTP Server Port	80
VLAN	Disabled
Version	v1.0.3.3
Wireless VLAN #1 SSID Configuration	
SSID	Skype Zones
Channel	6
Radio Status	Enabled
Encryption	Enabled
Authentication Type	WPA2-PSK
Multicast Cipher	Auto
Wireless VLAN #2 SSID Configuration	
SSID	Wireless Network - 1
Radio Status	Enabled
Encryption	Enabled
Authentication Type	WPA2-PSK
Multicast Cipher	Auto

Figure 2-2. System Information

The displayed items on this page can be described as follows:

AP System Configuration – Displays basic system configuration settings:

- **System Up Time** – Length of time since the access point was powered on.
- **MAC Address** – The physical layer address for the access point's Ethernet port.
- **IP Address** – The IP address configured on the access point.
- **IP Default Gateway** – The IP address of the gateway router between the access point and management stations that exist on other network segments.

- **HTTP Server** – The status of the web management server.
- **HTTP Server Port** – The TCP port used by the web management server.
- **Version** – The version number of the current access point software.

Wireless Data #1/#2 SSID Configuration – The AP Wireless Configuration table displays the wireless interface settings listed below.

- **SSID** – The service set identifier for this wireless group.
- **Channel** – The radio channel through which the access point communicates with wireless clients.
- **Encryption** – The key size used for data encryption.
- **Authentication Type** – Shows if open system or shared key authentication is used.
- **Multicast Cipher** – The encryption used for broadcast and multicast data.

Client

The client information page displays details on wireless devices currently associated to the access point. The displayed settings are for status information only and are not configurable on this page.

802.11 Station

Station Address	Authenticated	Associated	Encryption	Cipher	SSID	RSSI
00:12:CF:21:7A:F0	TRUE	TRUE	Disabled	None	Skype Zone	65

Figure 2-3. Client Information

The displayed items on this page can be described as follows:

- **Station Address** – The MAC address of the wireless client.
- **Authenticated** – Shows if the client has been authenticated. The two basic methods of authentication supported for 802.11 wireless networks are “open

system” and “shared key.” Open-system authentication accepts any client attempting to connect to the access point without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to clients before attempting authentication.

- **Associated** – Shows if the client has been successfully associated with the access point. Clients can associate with the access point only after authentication has completed.
- **Encryption** – Indicates if encryption is being used by the client; either Enabled or Disabled.
- **Cipher** – Indicates the encryption cipher capability being advertised by the client; WEP, TKIP, AES, or None.
- **SSID** -- The VAP interface that the client is associated with.
- **RSSI** -- The received signal strength of the client.

Network

The network information page displays the current Dynamic Host Configuration Protocol (DHCP) client, DHCP server, and Point-to-Point Protocol over Ethernet (PPPoE) status. The basic settings are also configurable on this page.

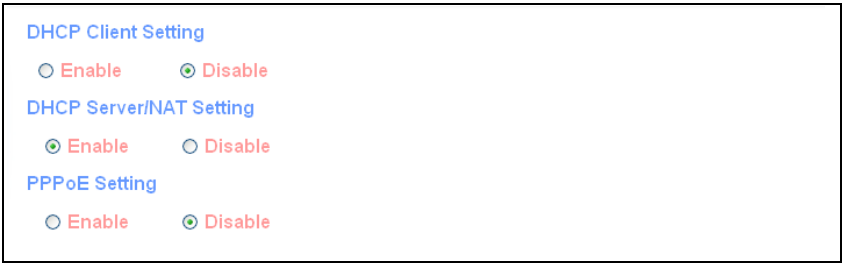


Figure 2-4. Network Information

The displayed items on this page can be described as follows:

- **DHCP Client Setting** – Enables the access point to automatically obtain an IP address from a DHCP server. When disabled, or if a response is not received from the DHCP server, the access point uses the configured static IP settings on the Network > DHCP Client page. (Default: Disabled)
- **DHCP Server/NAT Setting** – Enables or disables the DHCP server on the access point. The access point DHCP server can assign IP addresses to any wireless client requesting the service. Addresses are assigned to clients from a common address pool configured on the Network > DHCP Server/NAT page. (Default: Enabled)
- **PPPoE Setting** – Enables a connection to an Internet service provider using PPPoE. The PPPoE access user name and password can be set on the Network > PPPoE page. (Default: Disabled)

Event Log

The Event Log page displays system messages generated during system operation. The logged messages can serve as a valuable tool for isolating access point and network problems.

Event Log

1 Information: wlan0 vap1: Default Key set to key Index 3

2 Information: wlan0 vap1: Cipher set to WEP

3 Information: wlan0 vap1: Encryption set to enabled

4 Information: SNTP Server set to enabled

Figure 2-5. Event Log

The Event Log page displays the last 128 messages logged in chronological order, from the newest to the oldest. Log messages saved in the access point's memory are erased when the device is rebooted.

System Settings

The system settings pages allow you to change the management access password and restart the access point.

Administration

Management access to the access point is controlled through a single password.

To protect access to the management interface, you need to configure an Administrator password as soon as possible. If the password is not configured, then anyone having access to the access point may be able to compromise access point and network security.

Note: Pressing the reset button on the back of the access point for more than five seconds resets the user name and password to the factory defaults.

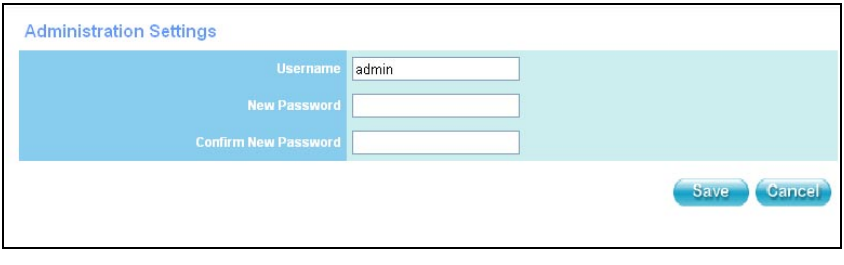


Figure 2-6. Administration Password

The displayed items on this page can be described as follows:

- **Username** – The name of the user. The default name is “admin.” The user name is not configurable.
- **New Password** – The password for management access. (Length: 0-32 characters, case sensitive)
- **Confirm New Password** – Enter the password again for verification.

Operation Mode

The device can be set as an access point, a wireless repeater or a wireless bridge according to user's need.

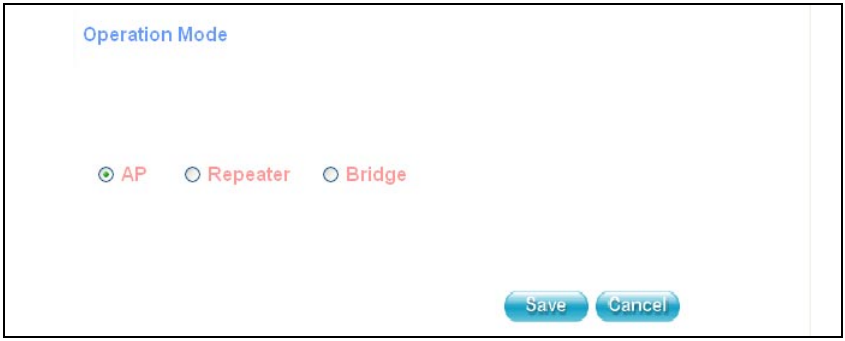


Figure 2-7. Administration Password

There are three operation modes:

- **AP** — Set the device as an Access Point.
- **Repeater** — Set the device as a Wireless Repeater to relay messages between subnetworks that use different protocols or cable types. The Root AP MAC Address can be assigned manually or selected after click "Scan".
- **Bridge** — Set the device as a Wireless Bridge to connect two local-area networks (LANs), or two segments of the same LAN that use the same protocol. The Bridge Nodes need to be assigned manually by the user.

Reboot System

The Reboot System page allows you to restart the access point software and restore factory default settings.

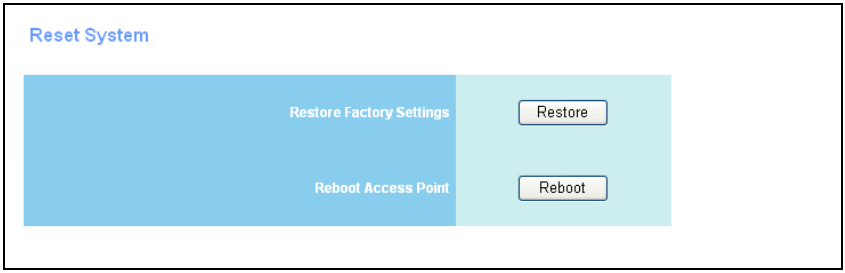


Figure 2-8. Reboot System

The displayed items on this page can be described as follows:

- **Restore Factory Settings** – Click the Restore button to reset the configuration settings for the access point to the factory defaults and reboot the system. Note that all user configured information will be lost. You will have to use the default IP address to re-gain management access to the access point.
- **Reboot Access Point** – Click the Reboot button to reboot the system.

Note: If you have upgraded the system software, then you must reboot the access point to implement the new code.

Wireless VAP Settings

The Wireless VAP #1 Setting and Wireless VAP #2 Setting pages include configuration options for radio signal characteristics and wireless security features on the access point.

The following sections apply to both Wireless VAP #1 Setting and Wireless VAP #2 Setting pages.

Note: it is recommended to restrict one VAP network for only Wi-Fi phones and let all other wireless stations use the other VAP network.

Basic

The Basic Setting page allows you to enable the VAP radio interface and define the Service Set IDentifier (SSID).

The access point includes an IEEE 802.11g radio for wireless communications. The IEEE 802.11g standard operates within the 2.4 GHz band at up to 54 Mbps. Note that because the IEEE 802.11g standard is an extension of the IEEE 802.11b standard, it allows clients with 802.11b wireless network cards to associate to an 802.11g access point.

The SSID is a recognizable text string that identifies the wireless network service provided by the VAP interface. Wireless clients that want to connect to the network must set their SSIDs to match that of the VAP interface.

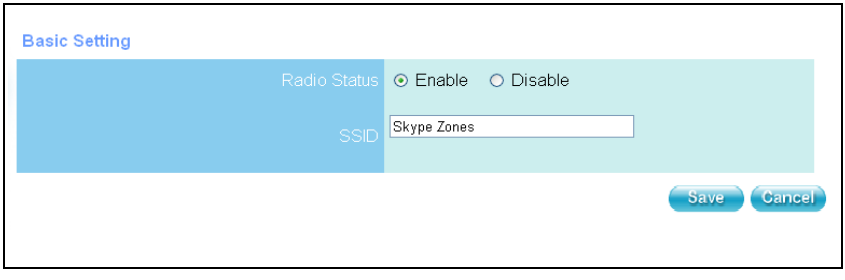


Figure 2-9. Basic Wireless Settings

The displayed items on this page can be described as follows:

- **Radio Status** – Enables radio communications for the VAP interface. (Default: Enabled)
- **SSID** – The name of the wireless network service provided by the VAP. Clients that want to connect to the network must set their SSID to the same as that of the VAP interface. (Defaults: Skype Zones," VAP #2 "Wireless Network - 1"; Range: 1-32 characters)

Channel Setting

The access point uses one radio channel in the 2.4 GHz band to communicate with its clients. The radio channel may be set manually by the user or automatically by the system, which selects the channel with the least radio interference.

Note: If you experience poor performance, you may be encountering interference from another wireless device. Try changing the channel, as this may eliminate interference and increase performance. Channels 1, 6, and 11, as the three non-overlapping channels in the 2.4 GHz band, are preferred.

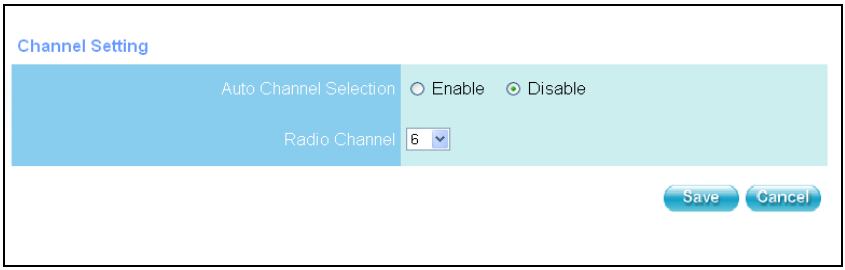


Figure 2-10. Wireless Channel Setting

The displayed items on this page can be described as follows:

- **Auto Channel Selection** – Enables the access point to automatically select an interference-free radio channel. (Default: Disabled)
- **Radio Channel** – The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the access point to which it is linked. (Range: 1-11; Default: 6)

WEP Security

The access point is configured by default as an “open system,” which broadcasts a beacon signal including the configured SSID. Wireless clients with a configured SSID of “any” can read the SSID from the beacon and automatically set their SSID to allow immediate connection to the access point. To secure the wireless network, you have to implement user authentication and wireless data encryption.

Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

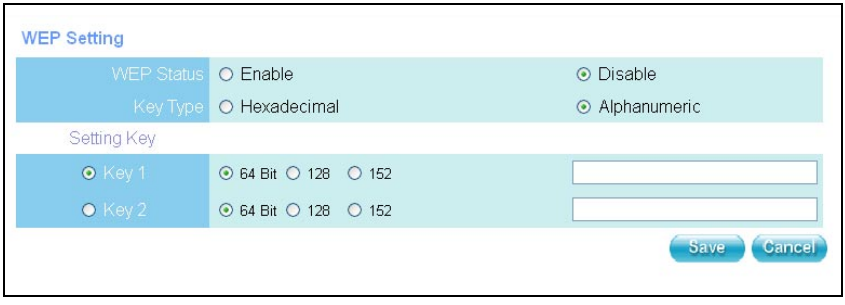


Figure 2-11. WEP Wireless Security

The displayed items on this page can be described as follows:

- **WEP Status** – Enables the access point to use WEP shared keys. If enabled, you must configure at least one key for the VAP interface and all its clients.
- **Key Type** – Select the preferred method of entering WEP encryption keys on the access point.
  - **Hexadecimal**: Enter keys as hexadecimal digits (0 to 9 and A to F).
  - **Alphanumeric**: Enter keys as alphanumeric characters.
- **Setting Key** – Sets WEP key values for one or two keys. At least one key must be specified. Each WEP key has an index number. Index numbers 1 and 2 apply to VAP #1 interface and numbers 3 and 4 apply to VAP #2 interface. The selected key is used for authentication and encryption on the VAP interface.

  Enter key values that match the key type and length settings. Select 64 Bit, 128 Bit, or 152 Bit key length. Note that the same size of encryption key must be supported on all wireless clients. (Default: 64 Bit)
  - **64 Bit**: Enter keys as 5 alphanumeric characters or 10 hexadecimal digits.
  - **128 Bit**: Enter keys as 13 alphanumeric characters or 26 hexadecimal digits.
  - **152 Bit**: Enter keys as 16 alphanumeric characters or 32 hexadecimal digits.

Note: Key index and type must match that configured on all clients.

WPA-PSK Security

Wi-Fi Protected Access (WPA) employs a combination of technologies to provide an enhanced security solution for wireless networks. The WPA Pre-shared Key (WPA-PSK) mode for small networks uses a common password phrase that must be manually distributed to all clients that want to connect to the network.

WPA2 is a futher security enhancement that includes the now ratified IEEE 802.11i wireless security standard. Both WPA and WPA2 provide very robust security through the support of the Advanced Encryption Standard (AES) and Temporal Key Integrity Protocol (TKIP) encryption ciphers.

Note: The computationally intensive operations of AES encryption requires hardware support on client devices. Before implementing AES in the network, be sure that wireless client hardware is AES or WPA2 compliant.

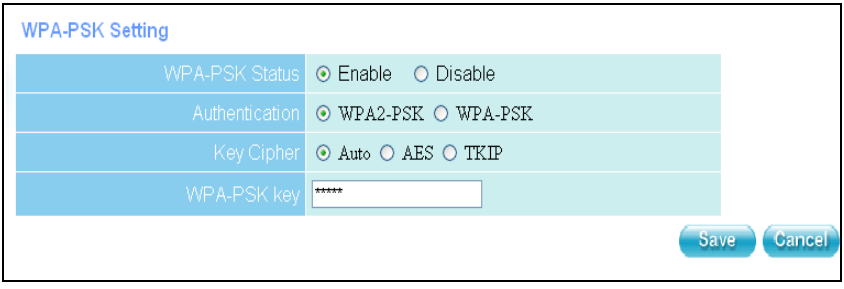


Figure 2-12. WPA-PSK Wireless Security

The displayed items on this page can be described as follows:

- **WPA-PSK Status** – Enables WPA-PSK or WPA2-PSK security on the VAP interface. When enabled, WEP clients are not supported. (Default: Enabled).
- **Authentication** – Selects WPA-PSK or WPA2-PSK security.
- **Key Cipher Mode** – Selects the encryption cipher to use for multicast and unicast data traffic:
  - **Auto** – Uses TKIP for the multicast cipher and TKIP or AES for the unicast cipher depending on the capability of associated clients.
  - **AES** – Uses AES keys for both multicast and unicast encryption.
  - **TKIP** – Uses TKIP keys for both multicast and unicast encryption.
- **WPA-PSK Key** – Enter a key as an easy-to-remember form of letters and numbers. The key must be from 8 to 63 characters, which can include spaces. All wireless clients must be configured with the same key to communicate with the VAP interface.

Network Settings

The access point supports DHCP client, DHCP server and Network Address Translation (NAT). Point-to-Point Protocol over Ethernet (PPPoE) is also supported for users that have an IP address assigned automatically from an Internet service provider (ISP) through an ADSL modem.

DHCP Client

Configuring the access point with an IP address enables you to manage the access point from any PC in the attached network. A number of access point features depend on IP addressing to operate.

Note: You can connect to the web browser interface to access IP addressing only if the access point already has an IP address that is reachable through your network.

By default, the access point is configured with the IP address 192.168.1.20, with the DHCP client disabled.

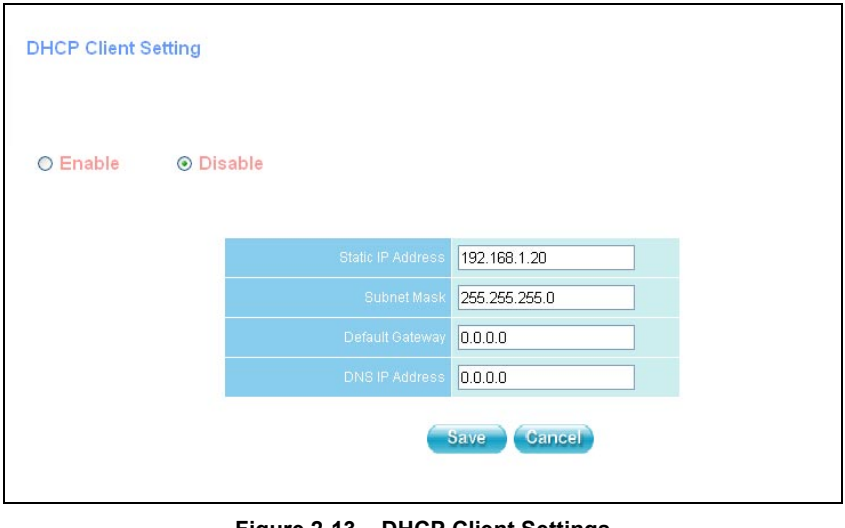


Figure 2-13. DHCP Client Settings

The displayed items on this page can be described as follows:

- **DHCP Client Setting** – Enables the access point to automatically obtain an IP address from a DHCP server. If a response is not received from the DHCP server, the access point uses the fixed IP settings as configured on this page. When set to disabled, a static IP address can be manually configured.
- **Static IP Address** – The IP address of the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

- **Subnet Mask** – The mask that identifies the host address bits used for routing to specific subnets.
- **Default Gateway** – The default gateway is the IP address of the router for the access point, which is used if the requested destination address is not on the local subnet. If you have management stations located on another subnet, type the IP address of the default gateway router in the text field provided. Otherwise, leave the address as all zeros (0.0.0.0).
- **DNS IP Address** – The IP address of a Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

  If you have a DNS server located on the local network, type the IP address in the text field provided. Otherwise, leave the address as all zeros (0.0.0.0).

DHCP Server/NAT

The access point includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to wireless clients requesting the service.

Addresses are assigned to clients from a common address pool configured on the access point. Configure an address pool by specifying start and end IP addresses. Be sure not to include the access point's IP address in the address pool range.

Network Address Translation (NAT) is a standard method of mapping multiple "internal" IP addresses to one "external" IP address on devices at the edge of a network. For the access point, the internal (local) IP addresses are the IP addresses assigned to wireless clients by the DHCP server, and the external IP address is the IP address assigned to the Ethernet port. When enabled, the access point's wireless interface uses the NAT IP settings to access the Ethernet network.

Note: When the DHCP server is enabled, NAT is also enabled.

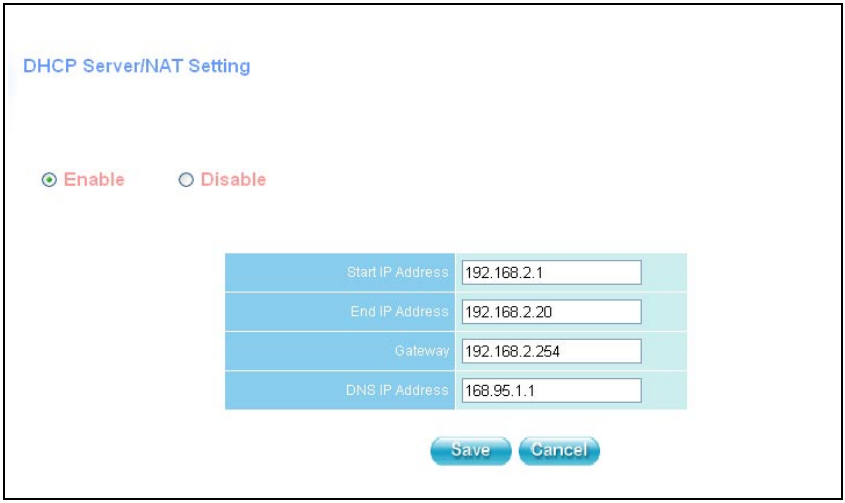


Figure 2-14. DHCP Server/NAT Settings

The displayed items on this page can be described as follows:

- **DHCP Server/NAT Setting** – Enables or disables the DHCP server and NAT on the access point. (Default: Enabled)
- **Start/End IP Address** – Specifies the start/end IP address of a range that the DHCP server can assign to DHCP clients. You can specify a single address or an address range.
- **Gateway** – The IP address of the gateway router for the access point, which is used if the requested destination address is not on the local subnet.
- **DNS IP Address** – The IP address of a Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

PPPoE

Many Internet service providers (ISPs) use the Point-to-Point Protocol over Ethernet (PPPoE) to automatically assign an IP address to users with a DSL modem. The PPPoE page provides the settings needed for this service.

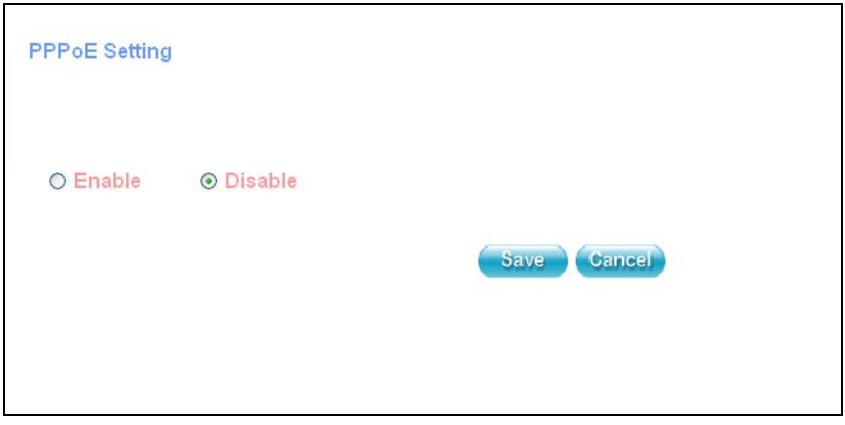


Figure 2-15. PPPoE Settings

The displayed items on this page can be described as follows:

- **PPPoE Setting** — Enables the access point IP address to be assigned automatically from an Internet service provider (ISP) through an ADSL modem using PPPoE.
- **Username** — If your ISP has provided you with a PPPoE user name, enter it in the corresponding text box.
- **Password** — If your ISP has provided you with a PPPoE password, enter it in the corresponding text box.

Time and Log

Simple Network Time Protocol (SNTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables all system log messages to be stamped with the correct time and date. If the clock is not set, the access point only records the time from the factory default set at the last bootup.

The access point acts as an SNTP client, which periodically sends time synchronization requests to a specific time server. SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display the time corresponding to your local time, you must also indicate the number of hours your time zone is located before or after UTC/GMT.

Figure 2-16. SNTP Settings

The displayed items on this page can be described as follows:

- **SNTP Server** Setting — Configures the access point to operate as an SNTP client. When enabled, the time server IP address must be specified.
- **Primary Server**: The IP address of an SNTP or NTP time server that the access point attempts to poll for a time update.
- **Time Zone** — Sets the number of hours your local time zone is located before or after UTC/GMT. (Default: GMT+00)

- **Daylight Saving** — The access point provides a way to automatically adjust the system clock for Daylight Savings Time changes. To use this feature you must define the month and date to begin and to end the change from standard time. During this period the system clock is set back by one hour.

Updating Firmware

You can upgrade new access point software from a local file on the management workstation, or from an FTP or TFTP server.

After upgrading to new software, you must reboot the access point to implement the new code. Until a reboot occurs, the access point will continue to run the software it was using before the upgrade started.

Upgrade via the Web Page

This web page allows you to download a new software code file from the local web management station to the access point using HTTP.

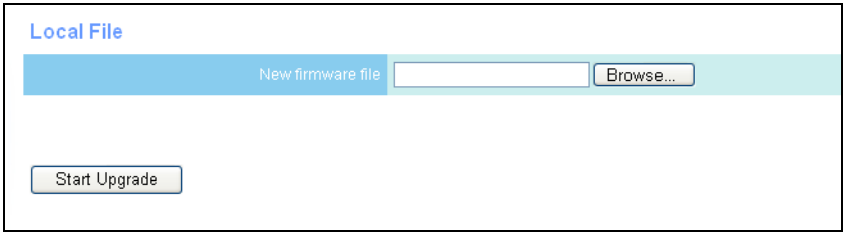


Figure 2-17. Web Page Upgrade

The displayed items on this page can be described as follows:

- **New Firmware File** — Specifies the name of the code file on the local web management station. You can use the Browse button to locate the image file locally on the management station.
- **Start Upgrade** — Starts the download process. Be sure to allow enough time for the download to complete before rebooting the access point.

Upgrade via a Remote Server

This web page allows you to download a new software code file from a remote server to the access point using FTP or TFTP.

When using an FTP or TFTP server, be sure to first obtain the IP address of the server and note the correct file path where the access point software is stored. If upgrading from an FTP server, also make sure that you have a user account configured on the server with a user name and password.

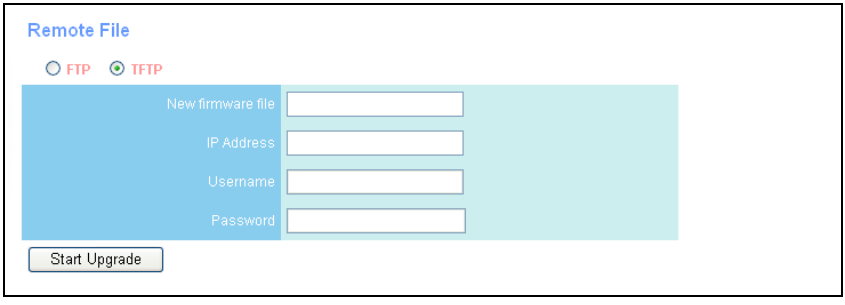


Figure 2-18. Remote Server Upgrade

The displayed items on this page can be described as follows:

- **Remote File** — Specifies a software code file download from a remote FTP or TFTP server.
- **New firmware file** — Specifies the name of the code file on the server. A path on the server can be specified using "/" in the destination file name, providing the path already exists. Other than to indicate a path, the file name must not contain any slashes (\ or /), the leading letter cannot be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters or 32 characters for files on the access point. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- **IP Address** — IP address or host name of the FTP or TFTP server.
- **Username** — The user ID used for login to an FTP server.
- **Password** — The password used for login to an FTP server.
- **Start Upgrade** — Starts the download process. Be sure to allow enough time for the download to complete before rebooting the access point.

Note: When you have downloaded the software file, you must reboot the access point to implement the new code.

Appendix A: Troubleshooting

Check the following items before you contact local Technical Support.

1. If wireless clients cannot access the network, check the following:
   - Be sure the access point and the wireless clients are configured with the same Service Set ID (SSID).
   - If authentication or encryption are enabled, ensure that the wireless clients are properly configured with the appropriate authentication or encryption keys.
2. If the access point cannot be configured using a web browser:
   - Be sure to have configured the access point with a valid IP address, subnet mask and default gateway.
   - If you are connecting to the access point through the wired Ethernet interface, check the network cabling between the management station and the access point. If you are connecting to access point from a wireless client, ensure that you have a valid connection to the access point.
3. If you forgot or lost the password:
   - Set the access point to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Connect to the web management interface using the default IP address 192.168.1.20. Then use the default user name “admin” and a null password to access the management interface.
4. If all other recovery measure fail, and the access point is still not functioning properly, take any of these steps:
   - Reset the access point’s hardware using the web interface or through a power reset.
   - Reset the access point to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Connect to the web management interface using the default IP address 192.168.1.20, then use the default user name “admin” and a null password.

Glossary

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

Access Point

An internetworking device that seamlessly connects wired and wireless networks. Access points attached to a wired network, support the creation of multiple radio cells that enable roaming throughout a facility.

Ad Hoc

A group of computers connected as an independent wireless network, without an access point.

Advanced Encryption Standard (AES)

An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.

Authentication

The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

Backbone

The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Beacon

A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

Broadcast Key

Broadcast keys are sent to stations using dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

Dynamic Host Configuration Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Encryption

Data passing between the access point and clients can use encryption to protect from interception and evesdropping.

Ethernet

A popular local area data communications network, which accepts transmission from computers and terminals.

File Transfer Protocol (FTP)

A TCP/IP protocol used for file transfer.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard used to transmit and receive all data over the World Wide Web.

IEEE 802.11b

A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11g

A wireless standard that supports wireless communications in the 2.4 GHz band using using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

Infrastructure

An integrated wireless and wired LAN is called an infrastructure configuration.

Local Area Network (LAN)

A group of interconnected computer and support devices.

MAC Address

The physical layer address used to uniquely identify network nodes.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Open System

A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

Orthogonal Frequency Division Multiplexing (ODFM)

OFDM/ allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

Service Set Identifier (SSID)

An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

Session Key

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Shared Key

A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Temporal Key Integrity Protocol (TKIP)

A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Wi-Fi Protected Access

WPA employs 802.1X as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.

Wired Equivalent Privacy (WEP)

WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

WPA Pre-shared Key (WPA-PSK)

WPA-PSK can be used for small office networks with a limited number of users that may not need a high level of security. WPA-PSK provides a simple security implementation that uses just a pre-shared password for network access.

Index

A
authentication
  type 2-11

C
configuration settings, saving or restoring 2-9
configuration, initial setup 1-1

D
DHCP 2-14
  server 2-15
DNS 2-15, 2-16
Domain Name Server *See* DNS
downloading software 2-20

F
factory defaults
  restoring 2-9
firmware
  upgrading 2-20

G
gateway address 2-15, 2-16

I
IEEE 802.11g
  configuring interface 2-10
  radio channel 2-11
initial setup 1-1
IP address
  configuring 1-5, 2-14

M
multicast cipher 2-13

O
open system 2-11

R
radio channel
  802.11g interface 2-11
reset 2-9
reset button 2-9
resetting the access point 2-9
restarting the system 2-9

S
security, options 2-11
SNTP 2-18
  enabling client 2-18
  server 2-18
software
  displaying version 2-3, 2-20
  downloading 2-20
SSID
  configuring 1-7, 1-8
system clock, setting 2-18
system software, downloading from server 2-20

T
troubleshooting A-1

U
upgrading software 2-20
user name, manager 2-7
user password 2-7

W
WEP
  configuring 2-11
WPA
  pre-shared key 2-13

Index

SAP2315A
E062006-EK-R01
FEGFT2315000E

SAP2315A
802.11b/g Access Point
Quick Installation Guide

SAP2315A
E062006-EK-R01
FEGFT2315000E

INTRODUCTION

Package Checklist

The 802.11b/g Access Point package includes:

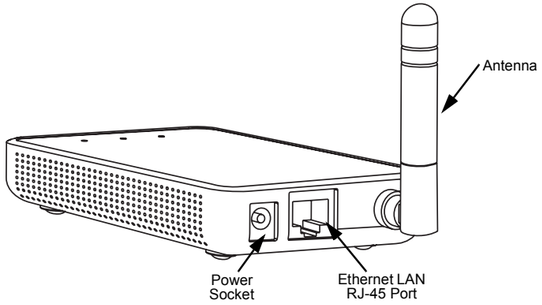
- Access Point
- One Category 5 network cable
- One AC power adapter
- This Installation Guide
- Management Guide CD

Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it.

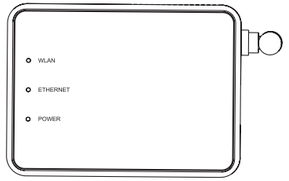
Power Connector

The access point does not have a power switch. It is powered on when connected to the AC power adapter, and the power adapter is connected to a power source. The power adapter automatically adjusts to any voltage between 100-240 volts at 50 or 60 Hz. No voltage range settings are required.

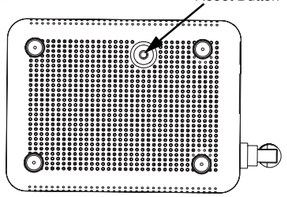
Hardware Description



Top Panel

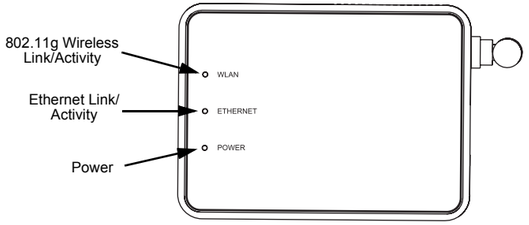


Bottom Panel



LED Indicators

The access point includes three status LED indicators, as described in the following figure and table.



LED	Status	Description
POWER	On Green	Indicates that the system is working normally.
WLAN	On/Flashing Green	Indicates the 802.11g radio is enabled and transmitting or receiving data through wireless links. The flashing rate is proportional to network activity.
	Off	Indicates the 802.11g radio is disabled.
ETHERNET	On/Flashing Green	Indicates a valid link on the Ethernet port and that the access point is transmitting or receiving data. The flashing rate is proportional to network activity.
	Off	The Ethernet port has no valid link.

INTRODUCTION

Ethernet Port

The access point has one 10BASE-T/100BASE-TX RJ-45 port that can be attached directly to 10BASE-T/100BASE-TX LAN segments. These segments must conform to the IEEE 802.3-2005 specifications.

This port supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs.

Reset Button

The Reset button is used to restart the access point or restore the factory default configuration. If you hold down the button for less than 5 seconds, the access point will perform a hardware reset. If you hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the access point.

HARDWARE INSTALLATION

To install the Access Point, follow these steps:

1. **Select a Site** – Choose a proper place for the access point. In general, the best location is at the center of your wireless coverage area, within line of sight of all wireless devices. For optimum performance, consider these points:
   - Mount the access point as high as possible above any obstructions in the coverage area.
   - Avoid mounting next to or near building support columns or other obstructions that may cause reduced signal or null zones in parts of the coverage area.
   - Mount away from any signal absorbing or reflecting structures (such as those containing metal).
   - Avoid radio interference by mounting away from other 2.4 GHz devices, such as other 802.11b or g wireless devices, regular cordless phones, and microwave ovens.
2. **Mount the Access Point** – The access point is designed to be mounted on any horizontal surface, such as a desktop.
3. **Connect the Power Cord** – Connect the power adapter to the access point, and plug the power adapter into an AC power outlet.

Caution: Use ONLY the power adapter supplied with the access point. Otherwise, the product may be damaged.

4. **Observe the Indicator LEDs** – When you power on the access point verify that the POWER LED turns on and that the other LED indicators start functioning as described under ”LED Indicators”.
5. **Connect the Ethernet Cable** – The access point can be connected to any 10 or 100 Mbps Ethernet network device, such as a hub or a switch. Connect your network to the RJ-45 port on the back panel using category 3, 4, or 5 UTP Ethernet cable. When the access point and the connected device are powered on, the ETHERNET LED should turn on indicating a valid network connection. If the ETHERNET LED fails to turn on, refer to “Troubleshooting”.

Note: The RJ-45 port on the access point supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs.

Access Point Configuration

The access point can be configured by connecting a PC to its Ethernet port and accessing the web interface. The default IP address of the access point is 192.168.1.20, with login user name “admin” and no default password.

For more information, refer to the *Management Guide*.

TROUBLESHOOTING

Diagnosing Access Point Indicators

Troubleshooting Chart	
Symptom	**Action**
POWER LED is Off	• AC power adapter may be disconnected. Check connections between the access point, the power adapter, and the wall outlet.
ETHERNET LED is Off	• Verify that the access point and attached device are powered on. • Be sure the cable is plugged into both the access point and corresponding device. • Verify that the proper cable type is used and its length does not exceed specified limits. • Check the cable connections for possible defects. Replace the defective cable if necessary.

For information on troubleshooting wireless connectivity issues, refer to the *Management Guide*.

COMPLIANCES

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Japan VCCI Class B

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると受信障害を引き起こすことがあります。
取り扱い説明書に従って正しい取り扱いをして下さい。

EC Conformance Declaration CE

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950-1 (IEC 60950-1) - Product Safety
- EN 300 328 - Technical requirements for 2.4 GHz radio equipment
- EN 301 489-1, EN 301 489-17 - EMC requirements for radio equipment

This device is intended for use in the following European Community countries:

- Austria
- Finland
- Italy
- Norway
- Switzerland
- Greece
- Belgium
- France
- Luxembourg
- Spain
- United Kingdom
- Ireland
- Denmark
- Germany
- Netherlands
- Sweden
- Portugal
- Iceland

Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below:

- In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

CABLES AND PINOUTS

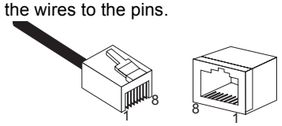
Twisted-Pair Cable Assignments

For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Caution: Each wire pair must be attached to the RJ-45 connectors in a specific orientation. (See “Crossover Wiring” and “Crossover Wiring” for an explanation.)

Caution: DO NOT plug a phone jack connector into the RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

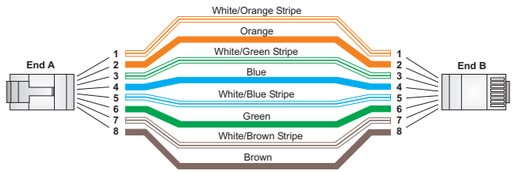
The following figure illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



Straight-Through Wiring

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through.

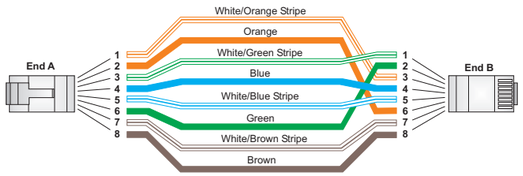
EIA/TIA 568B RJ-45 Wiring Standard
10/100BASE-TX Straight-through Cable



Crossover Wiring

If the twisted-pair cable is to join two ports and either both ports are labeled with an “X” (MDI-X) or neither port is labeled with an “X” (MDI), a crossover must be implemented in the wiring.

EIA/TIA 568B RJ-45 Wiring Standard
10/100BASE-TX Crossover Cable



SPECIFICATIONS

Maximum Channels
FCC/IC: 1-11
ETSI: 1-13
France: 10-13
MKK: 1-14
Taiwan: 1-11

Maximum Clients
32 per VAP interface

Data Rate
802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel
802.11b: 1, 2, 5.5, 11 Mbps per channel

Modulation Type
802.11g: CCK, BPSK, QPSK, OFDM
802.11b: CCK, BPSK, QPSK

Network Configuration
Infrastructure

Operating Frequency
2.4 ~ 2.4835 GHz (US, Canada, ETSI)
2.4 ~ 2.497 GHz (Japan)
2.400 ~ 2.4835 GHz (Taiwan)

Wireless Output Power
802.11b: 18 dBm (typical)
802.11g: 17 dBm @ 6 Mbps, 14dBm @ 54 Mbps

Wireless Receive Sensitivity
802.11b: -90 dBm @ 1 Mbps, -84 dBm @ 11 Mbps
802.11g: -86 dBm @ 6 Mbps, -68 dBm @ 54 Mbps

AC Power Adapter
Input: 100-240 VAC, 50-60 Hz
Output: 5 VDC, 2 A

Unit Power Supply
DC Input: 5 VDC, 2 A maximum
Power Consumption: 6.5 W maximum

Physical Size
14.7 x 9.0 x 2.8 cm (5.79 x 3.54 x 1.1 in)

Weight
300 g (10.6 oz)

LED Indicators
POWER (Power), ETHERNET (Ethernet Link/Activity), WLAN (Wireless Link/Activity)

Network Management
Web-browser

Temperature
Operating: 0 to 50 °C (32 to 122 °F)
Storage: -20 to 70 °C (32 to 158 °F)

Humidity
15% to 95% (non-condensing)

Compliances
FCC Part 15B Class B
VCCI ClassB
EN 55022 Class B
EN 55024
EN61000-3-2
EN61000-3-3

Radio Signal Certification
FCC Part 15C 15.247, 15.207 (2.4 GHz)
EN 300-328
EN 301 489-1
EN 301 489-17
ARIB STD-T66
ARIB STD-33

Safety
UL 60950-1
EN 60950-1
IEC 60950-1 (CB)

Standards
IEEE 802.3-2005 10BASE-T, 100BASE-TX
IEEE 802.11b, g
Wi-Fi 11b/g, WPA, WPA2, WMM