Wireless Concurrent Dual Band PoE Access Point

AP25N01

User Manual

Version 1.0 (June 2012)

© Copyright 2012 AIR802

Disclaimer

AIR802 makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. AIR802 may make improvements and/or changes to the product and/or specifications of the product described in this manual without prior notice. AIR802 reserves the right to revise this manual and to make changes from time to time in the contents without obligation to notify any person of such changes.

TABLE OF CONTENTS

SAFETY AND REGULATORY NOTICES

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, for which the user may be required to take adequate measures.

FCC 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 or more of the following measures:

1. Reorient or relocate the receiving antennas.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a different circuit different from the one to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

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.

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.
2. This device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTICE:
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 minimum distance 20cm (8 inches) between the antenna and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Industry Canada Notice

This class B digital apparatus complies with Canadian ICES-003.

Declaration of Conformity

AIR802, Inc., declares the following:

Product Name: Wireless Concurrent Dual-Band Access Point with PoE

Model No.: AP25N01 conforms to the following product standards:

This device complies with the Electromagnetic Compatibility Directive (89/336/EEC) issued by the Commission of the European Community. Compliance with this directive implies conformability to the following European Norms (the equivalent international standards are shown in brackets).

Electromagnetic Interference (Conduction and Radiation): EN 55022 (CISPR 22)

Electromagnetic Immunity: EN 55024 (IEC 61000-4-2, 3, 4, 5, 6, 8, 11)

Low Voltage Directive: EN 60950: 1992+A1: 1993+A2: 1993+A3: 1995+A4: 1996+A11: 1997.

Therefore, this product is in conformity with the following regional standards:
FCC Class B, following the provisions of FCC Part 15 directive; **CE Mark**, following the provisions of the EC directive.

AIR802, Inc. also declares that:

The wireless card in this product complies with the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following:

EMC Standards: FCC: 47 CFR Part 15, Subpart B, 47 CFR Part 15, Subpart C (Section 15.247); CE: EN 300 328-2, EN 300 826 (EN 489-17)

Therefore, this product is in conformity with the following regional standards:
FCC Class B, following the provisions of FCC Part 15 directive; **CE Mark**, following the provisions of the EC directive.

Product Introduction

AIR802 is an innovative company providing a variety of high quality networking products, including this Wireless Concurrent or Simultaneous Dual Band PoE Access Point (AP25N01). Embedded with a Qualcomm Atheros chipset, it offers network stability, robustness and wide network coverage at up to 300Mbps under the IEEE 802.11n standards.

It has been designed for deployment in enterprise networks or for public wireless access in locations such as:

- Airports

- Coffee shops

- Convention centers

- Education (K-12, college and universities)

- Hospitals

- Hotels

- Manufacturing plants

- Medical offices

- Military facilities

- Office buildings

- Restaurants

Features

- Housed in a steel enclosure, it is fully plenum rated for installation above drop ceilings where return airflows must meet strict fire codes.

- Two radios, 2.4 GHz and 5.1 to 5.8 GHz, support concurrent or simultaneous operations to IEEE 801.11b/g/n on the 2.4 GHz band and 802.11a/n on the 5.1 to 5.8 GHz band.

- Includes an AC power supply or may be powered via Power over Ethernet (PoE), and supports both IEEE 802.3af and passive non 802.3af PoE technology.

- Four external antennas with RP-SMA connectors support dual-band MIMO 2 x 2 spatial multiplexing.

- External ground lug for electro static discharge (ESD) prolongs product life and provides stability.

- High RF output power up to 400mW and excellent receiver sensitivity.

- Multiple SSIDs support up to four virtual access points per radio.

- Five wireless modes: station (client), station WDS, access point, access point WDS, repeater WDS.

- Two network modes: bridge or router.

- Built-In interference analyzer.

- VLAN operations.

- Management and configuration support for HTTP / HTTPS (web interface), Telnet, SSH and SNMP V2c.

PACKING LIST

Before you start to install the AP25N01, make sure the package contains the following items:

- AIR802 AP25N01 Concurrent Dual-Band PoE Access Point

- Four dual-band 2dBi dipole antennas with RP-SMA connectors

- Power adapter

- User manual CD

- Quick Installation Guide

- Ethernet patch cable

PRODUCT OVERVIEW

Front View

	Feature	Status and Indications
1	Power LED	On: Power is supplied to the device. Off: Power is not supplied to the device.
2	Ethernet Port LED	On: Connection has been established between the device and the network. Flashing: network is active. Off: No network connection.
3	Signal Strength Indicators	The four LEDs turn on at various levels to indicate the RSSI signal strength.

Rear View
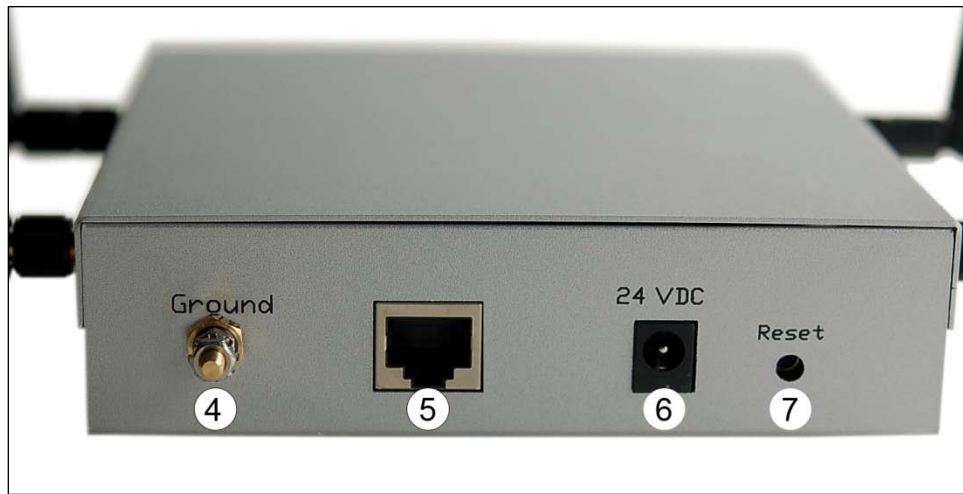
	Feature	Status and Indications
4	Ground connection	
5	Ethernet port	
6	Power supply input	For power input. 24V – 48 Vdc.
7	Reset button	To reboot, press and release.
		To reset the password, press and hold the button for 5 seconds then release.
		To restore the factory default settings, press and hold the button for 8 seconds then release.

Wireless Operational Modes

Wireless Operation Modes	Function
Station (Client)	Wireless client to the Access Point (root AP)
Station WDS	Wireless Client via WDS *both ends should be same product*
Access Point	Basic bridged link between wireless and wired network
Access Point WDS	Point-to-point or multipoint bridged links with Station WDS
Repeater WDS	Create relay access points to regenerate the received signal.

Station Mode

In station mode, the AP25N01 functions as a wireless client. In other words, it is a client to another access point (like a wireless card in a computer is a client to an access point). When connected to an access point, it creates a network link between the Ethernet network connected at this client device and the wireless Ethernet network connected at the access point. This mode translates all data packets that pass though the device to its own MAC address, which results in a lack of transparency.

In the example below, the workgroup PCs on the Ethernet network connected to the Bridge can access the printer across the wireless connection to the Station Mode client where the printer is connected.
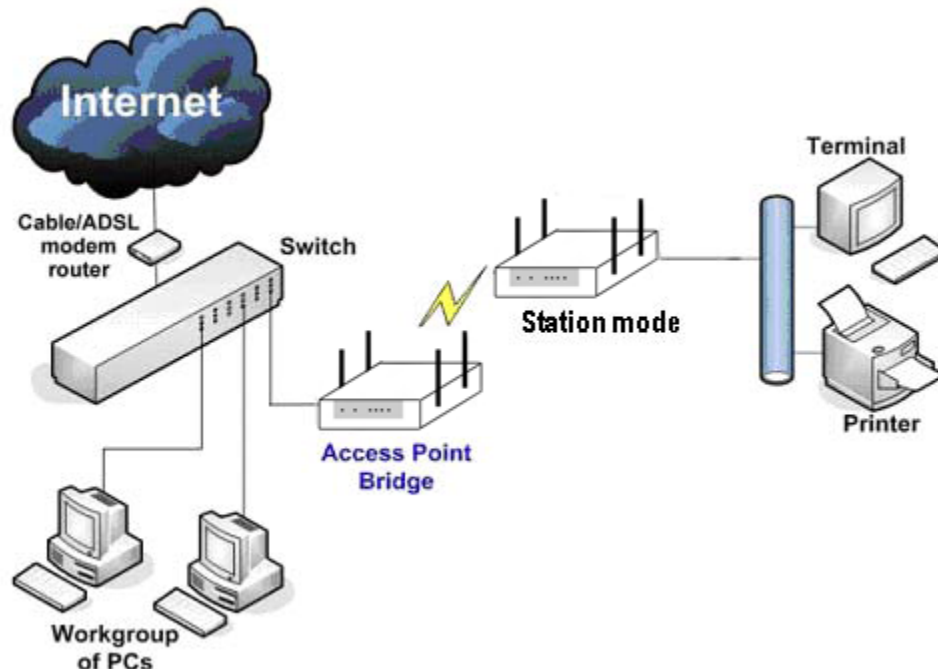
Station WDS

Station WDS (Wireless Distribution System) mode is similar to Station mode. The difference is that Station WDS must connect to an access point that has been configured to Access Point WDS (or Root AP) mode. WDS is a means of interconnecting two or more access points in a wireless network that maintains the MAC addresses across the links between access points. It is fully transparent.

It should be noted that WDS is not defined as a standard by the IEEE or other standards bodies, therefore it often results in incompatibility between different manufacturer's products. Also a disadvantage of WDS is that it reduces the throughput.

Station WDS is most commonly used for point to point or point to point to multipoint connections between two or more buildings or locations, sometimes miles apart.
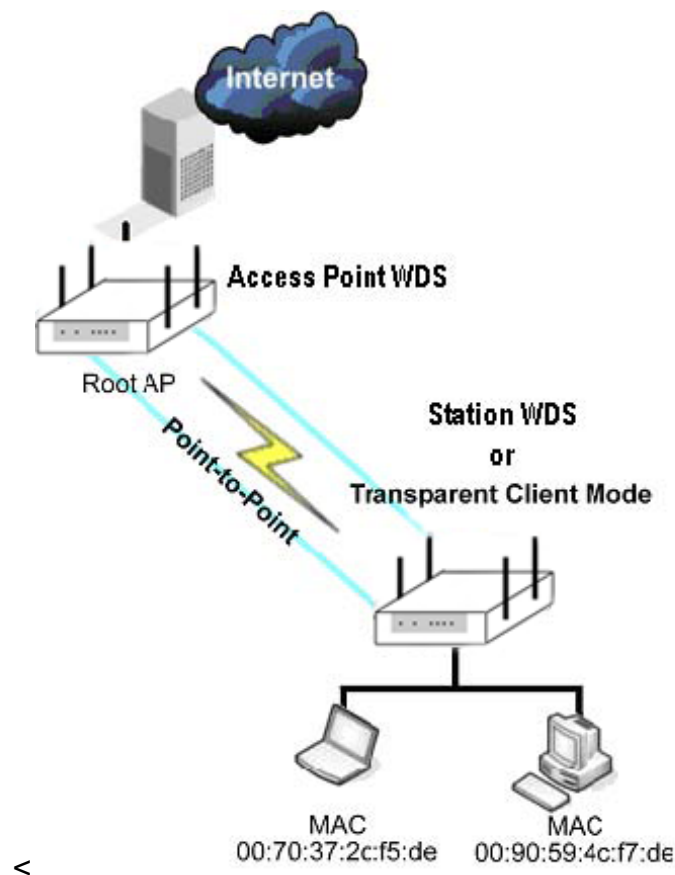
Access Point

This is the default mode, which enables a bridged path between any wireless clients and the wired network infrastructure. It provides a transparent link between the wireless clients and the wired network.

The diagram below depicts a typical example.
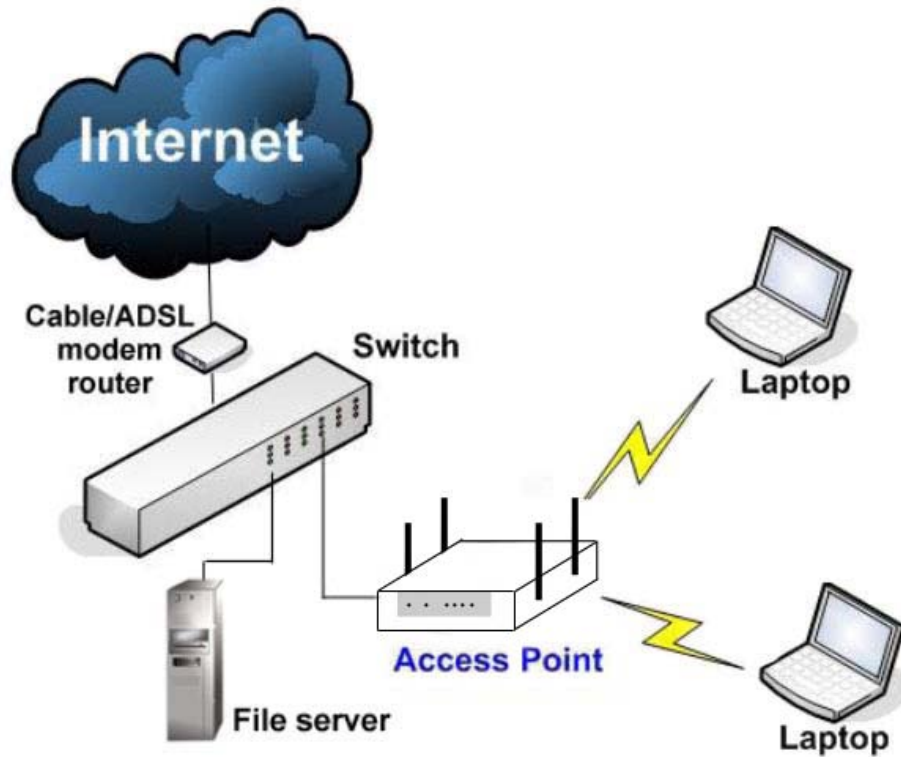
Access Point WDS

This mode can be used in either point to point or point to multipoint configurations or topology. This mode is generally used with Station WDS mode, where the Access Point WDS acts as the root AP and the other AP configured as Station WDS mode functions in transparent client mode to the root AP (Access Point WDS).
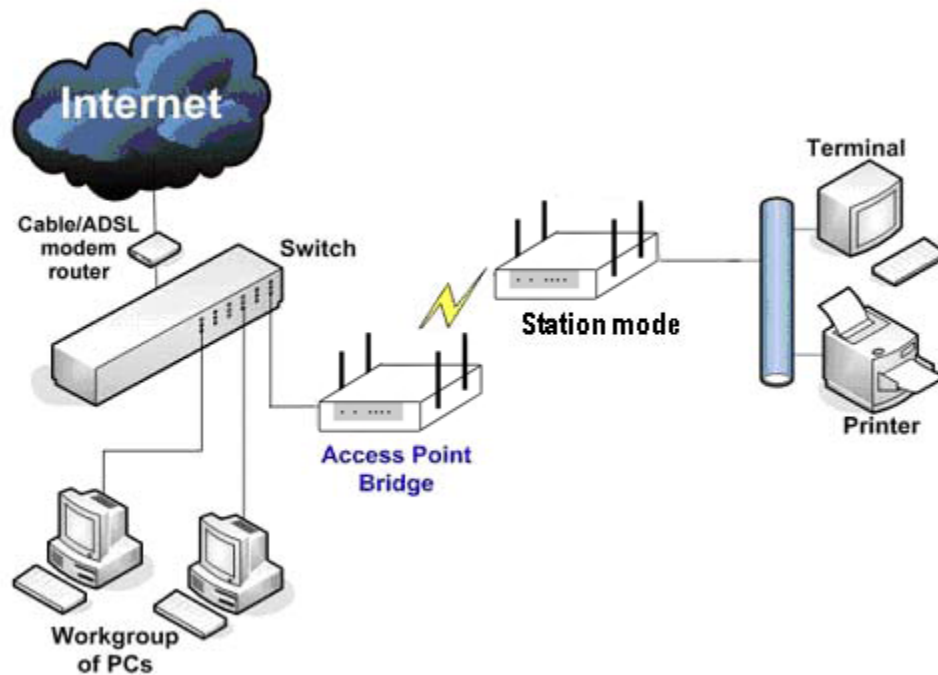
Repeater WDS

This mode allows one or more repeaters to operate between an access point configured as access point WDS (root AP) and an access point configured as Station WDS. This extends the range of a wireless network. Essentially, a device operating in this mode acts as a relay, receiving and retransmitting signals. The channel used is the same on all of the devices and the ESSID must be the same on the root AP (Access Point WDS) and the remote AP (Station WDS).
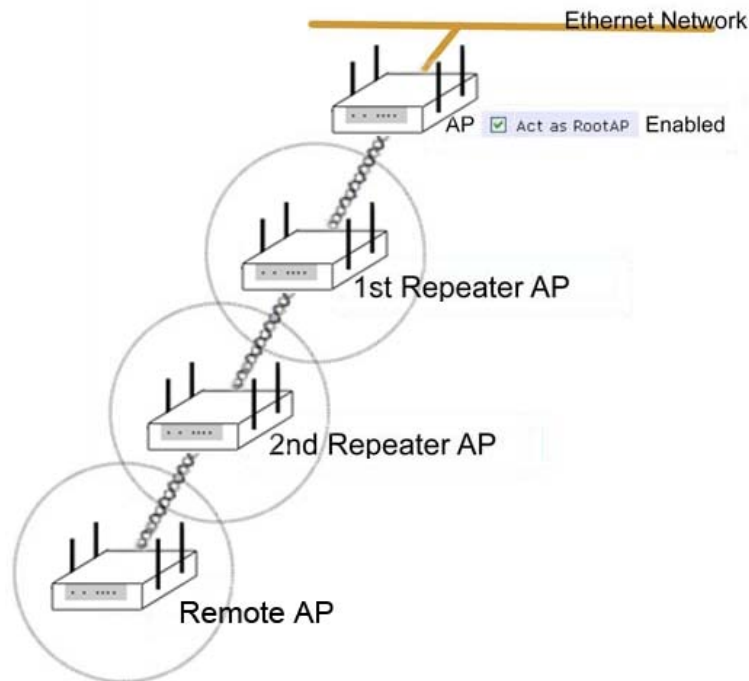
Network Modes

Network Mode	Function
Bridge	Extends data from wired to wireless network
Router	Routing of two separate subnets

Bridge

In bridge mode, the network operates at Layer 2 of the OSI model. Ethernet frames are seamlessly passed from the wireless to the wired network.

<insert diagram ….need to create>

Router

In router mode, the network operates at Layer 3 of the OSI model. Data packets are routed from the wireless network to the wired network. Either the wireless or wired Ethernet interface can be setup as the WAN (wide area network) connection. If the WAN is wireless, the appropriate wireless and network mode would be Station + Router (wireless routed client). For wired Ethernet as the WAN the appropriate mode would be AP + Router (sometimes called Gateway mode).
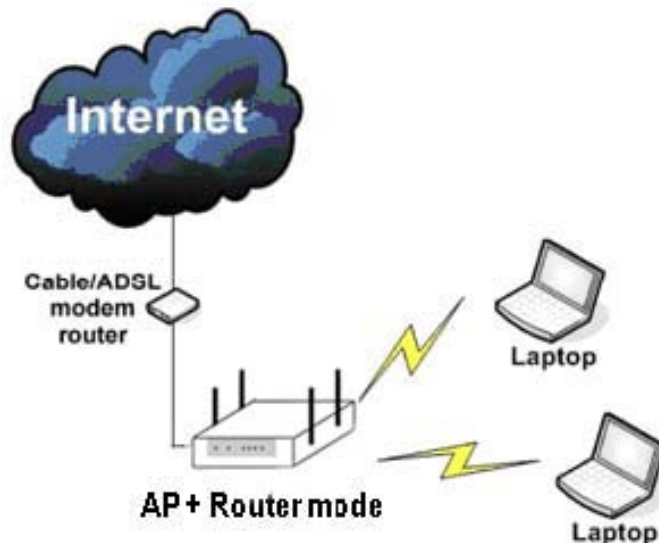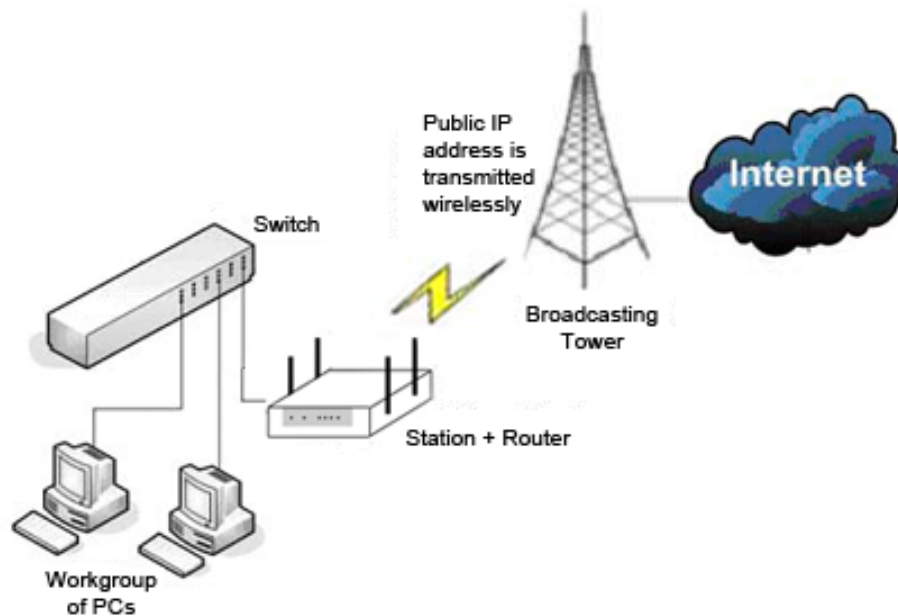
HARDWARE INSTALLATION

Physical Placement

The access point may be placed in a rack, above a ceiling, on a desk or shelf, or it may be wall mounted. The bottom of the case includes rubber feet and slots for wall mounting screws.

Wall mount slots

Feet

Grounding

The 5.1 to 5.8 GHz radio has been designed with electro static discharge (ESD) circuitry to protect the radio. In order for this to be effective, a ground cable must be secured between the ground lug in the rear of the access point and a ground source to dissipate any static electrical charge buildup. Ideally it should be grounded to electrical ground, a cold water pipe (copper only), or a ground rod. A connection to building structural steel, while not truly a proper ground would be better than no ground.

Ground lug

Antenna Installation

NOTE: It is not recommended to power up a wireless access point without antennas terminated into the antennas connectors.

Four dual-band antennas are supplied with the access point. Connect one to each of the four RP-SMA antenna connectors on the sides of the access point.

Alternatively, there are several installation options available from AIR802:

- If the device is located above a drop or false ceiling tile, the AIR802 Universal Ceiling Antenna Mount (UCAM) is recommended for maximum flexibility. This permits the antennas to be installed below the ceiling tiles, providing superior signal propagation.

- Short pigtail cables can be used between the top of the UCAM and the access point.

- For aesthetic matching, white antennas that can be attached to the bottom side of the UCAM are also available.

- Antenna cables can be used to connect to other styles and types of antennas located elsewhere, even outdoors.

NOTE: Always use a coaxial surge protection device if installing antennas on the exterior of a building.

Powering Options and Network Connectivity

Method 1 – Using the power adapter (supplied) to power the access point. A power outlet must be available nearby.

Method 2 – Using a PoE midspan injector, when no PoE switch is available or a power outlet is not located nearby.

Method 3 – Using a PoE switch.

Method 4 – Using an AIR802 dc to dc converter with PoE output. This is used when you have a voltage source of 9 to 36 Vdc available, such as a solar panel or vehicle battery, and need the voltage converted to 48vdc (IEEE 802.3af compliant).

NOTE: Direct connection between the access point and a computer is recommended for initial configuration of the access point.

Method 1: Power Adapter

1. Connect one end of an Ethernet patch cable to the Ethernet port in the rear of the AP25N01 access point and the other end to a computer, switch or router.

2. Insert the DC plug of the supplied power adapter into the power supply connector at the rear of the AP25N01 access point.

3. Connect the power adapter to a power outlet.
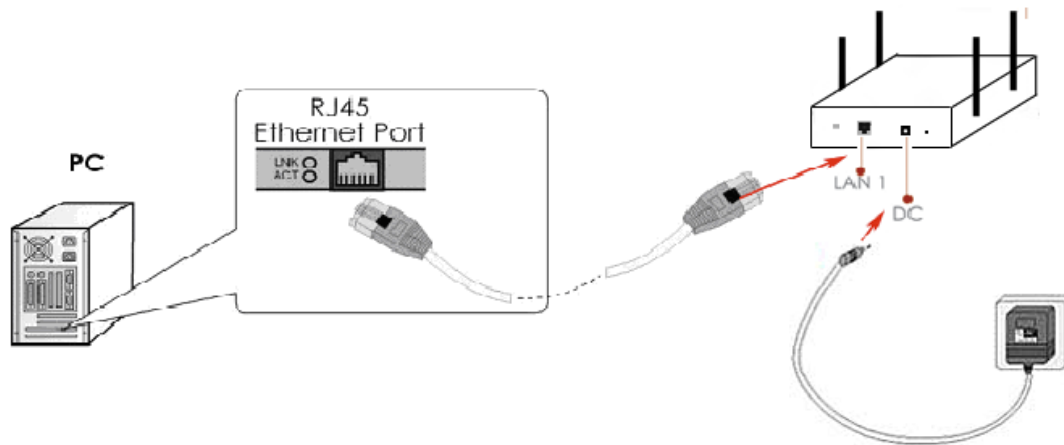
Method 2: Midspan Injector

1. Connect one of an Ethernet patch cable into the Data In port on a PoE midspan splitter, such as the AIR802 model PSA48V19W, and the other end into your computer, switch or router.

2. Connect one end of another Ethernet patch cable into the PoE or Data Out port of the midspan splitter and the other end of the patch cable to the Ethernet port in the rear of the AP25N01 access point.

3. Connect the splitter's power adapter to the power supply connector and a power outlet.
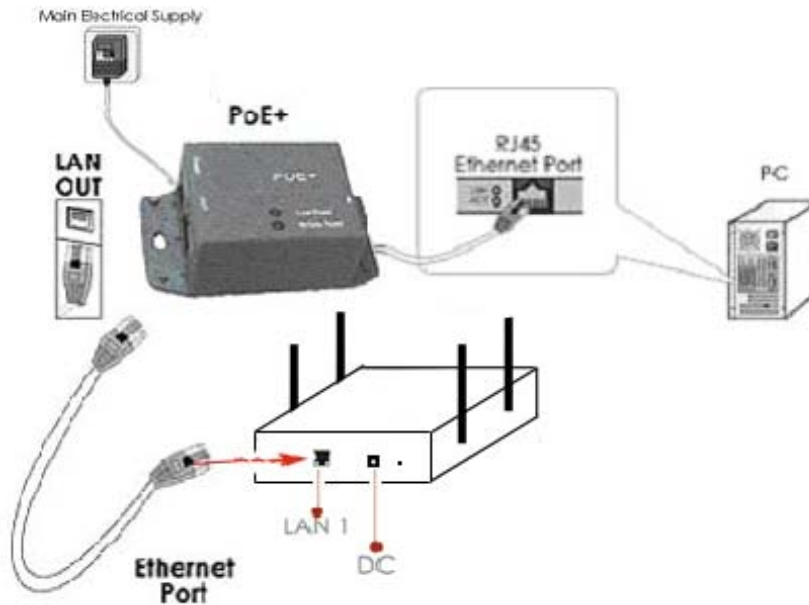
Method 3: PoE Switch

Connect an Ethernet patch cable between the Ethernet port in the rear of the AP25N01 and a port on the PoE switch.

Method 4: DC to DC converter with PoE

1. Connect an Ethernet patch cable between the Ethernet port in the rear of the AP25N01 and the Equip-PoE port of the AIR802model PDCPOE1248DR DC–DC Converter with PoE Injector.

2. Connect another Ethernet patch cable between the Network port on the PDCPOE1248DR and your computer, switch or router. Generally it is recommended to connect to your computer directly to initially configure the device. <insert photo>

CONFIGURATION PREPARATION

Assign a Static IP Address to the PC

The following example illustrates the procedure for statically assigning an IP address to your PC.

Windows 7

1. Click **Start**, **Control Panel, Network and Sharing Center.** The Network and Sharing Center opens.
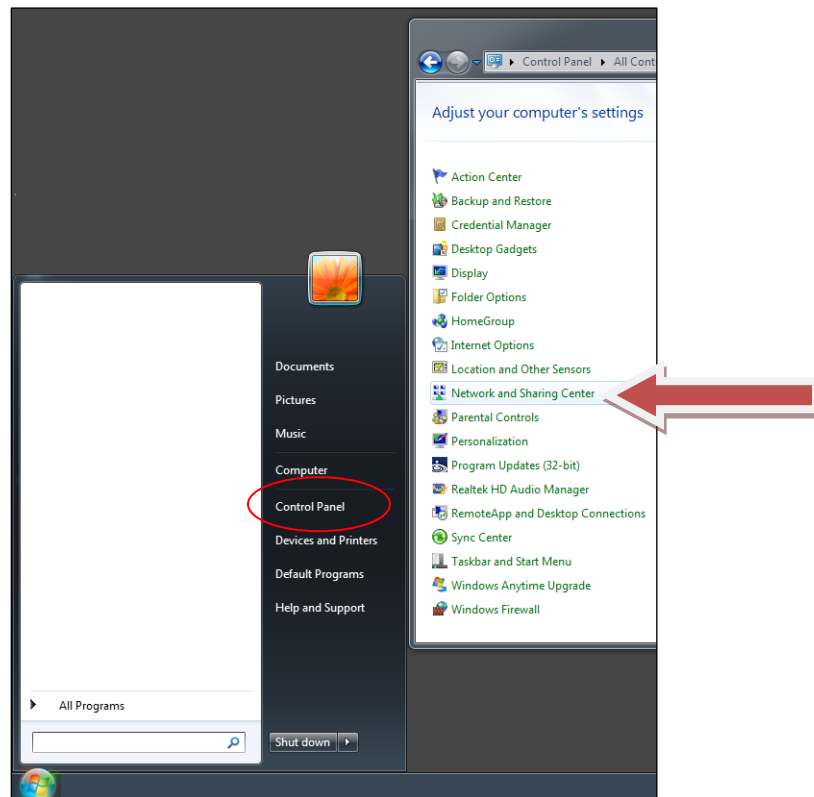
2. Click either **Local Area Connection** or **Wireless Network Connection**, depending on how you are accessing the AP25N01 (by an Ethernet network cable or via a wireless card).
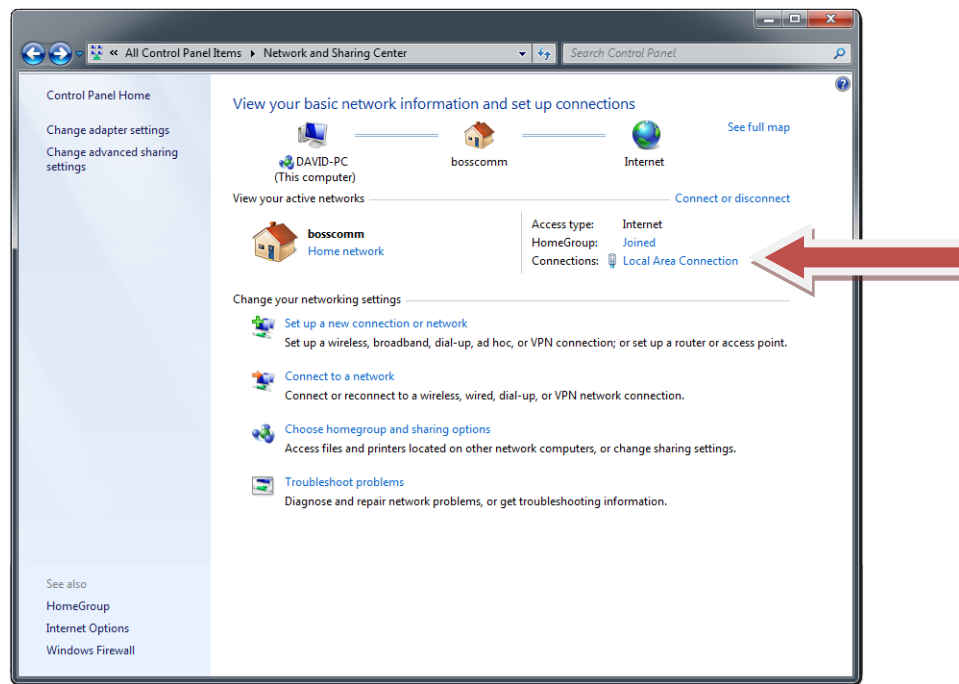
3. Click **Properties**, **Internet Protocol Version 4 (TCP/IPv4),** and click **Properties**.
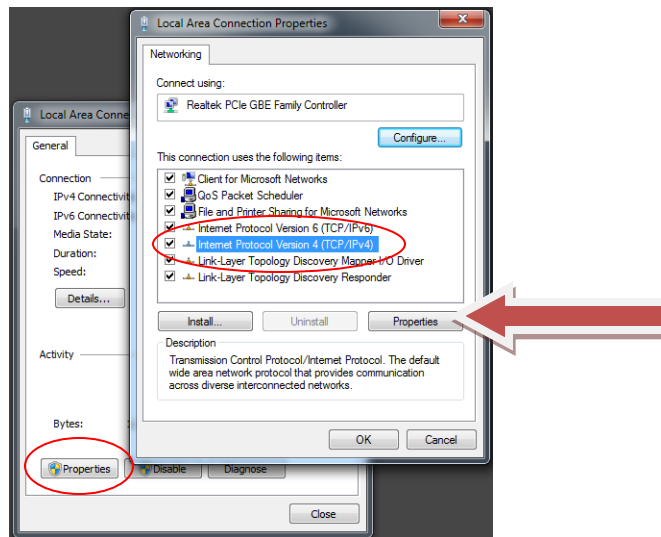
4. Click the button to select **Use the following IP address**, set the IP address to 192.168.2.X and subnet mask to 255.255.255.0 (where X can be any number from 1 to 253), and click **OK**.
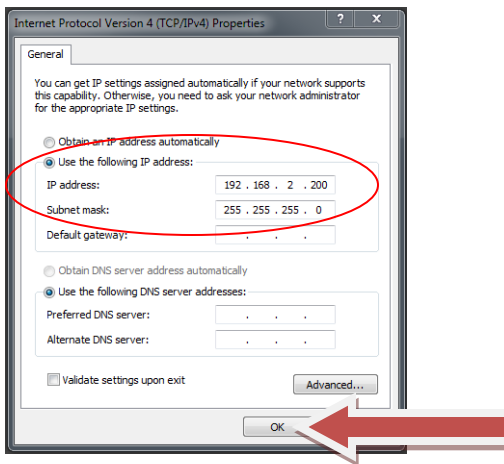
5. Click **Close**, and **Close** again in the previous Connection Properties window.

Windows VISTA

1. Click **Start**, right click **Network** and choose **Properties.** The Network and Sharing Center opens.

2. Click **Manage Network Connections** in the left sidebar.
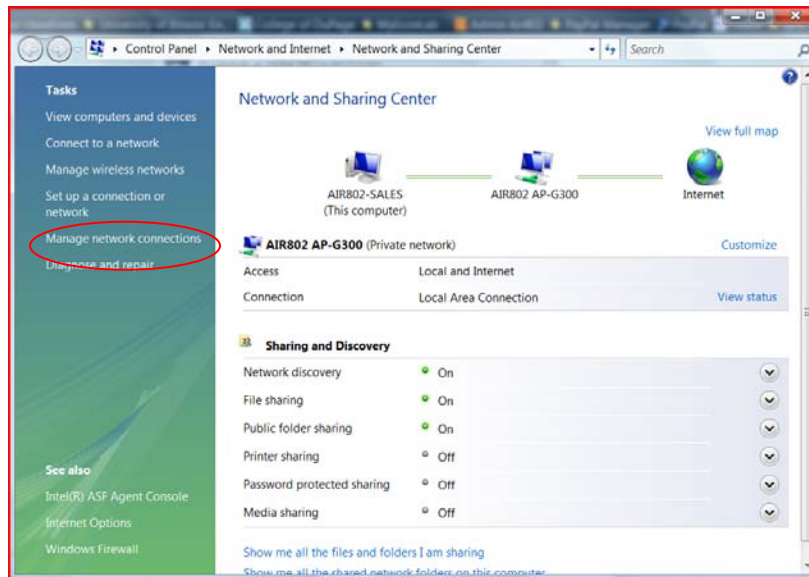
3. Right click either **Local Area Connection** or **Wireless Network Connection**, depending on how you are accessing the AP25N01 (by an Ethernet network cable or via a wireless card), and select Properties.
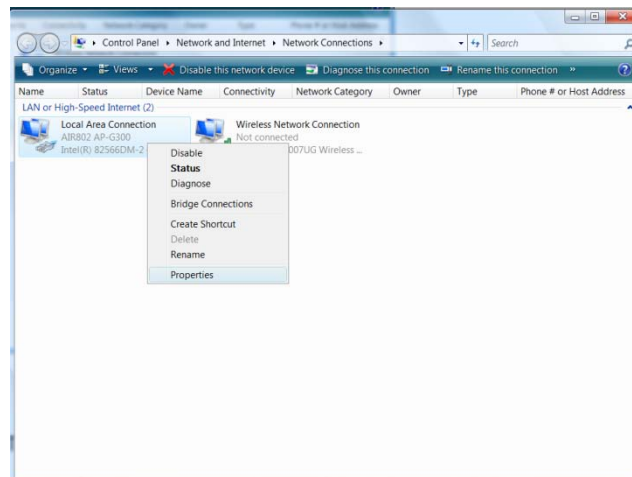
4. Click **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
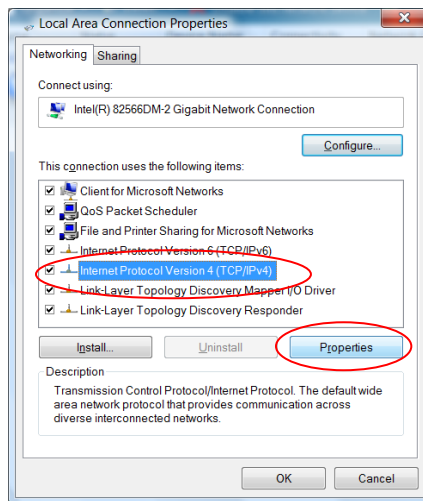
1. Click the button to select **Use the following IP address**. Set the IP address to 192.168.2.X and subnet mask to 255.255.255.0, where X can be any number from 1 to 253.
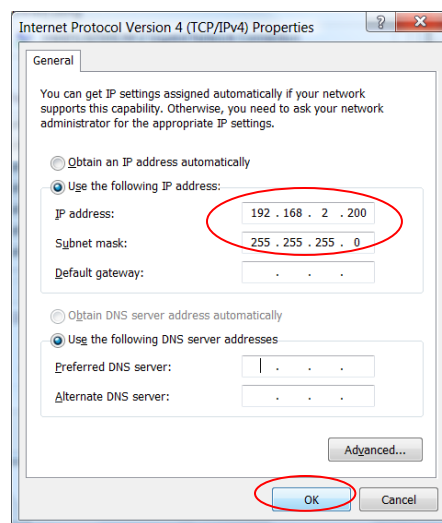
2. Click **OK**, and **OK** again in the previous Connection Properties window.

Windows XP

3. Click **Start**, right click **My Network Places** and click **Properties**.

4. Right click either **Local Area Connection** or **Wireless Network Connection**, depending on how you are accessing the device (by an Ethernet network cable or via a wireless card), and select **Properties**.
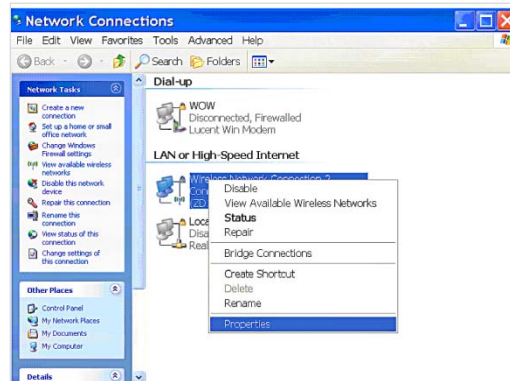
5. Select **Internet Protocol (TCP/IP)** and click **Properties**.
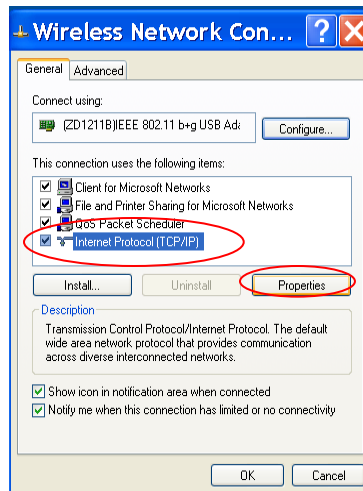
6. Click the button to select **Use the following IP address**. Set the IP address to 192.168.2.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 253.
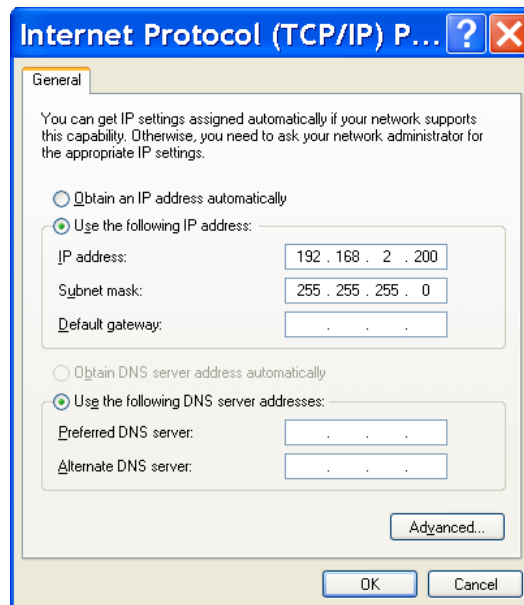
7. Click **OK**.

Web Interface

The web interface can be accessed by either directly entering the default IP address of 192.168.2.254 into the web browser or by using the uConfig utility (found on the CD).

Access with uConfig

The UConfig utility provides direct access to the web interface.

1. Click the uConfig icon to launch the utility then click **Yes**.
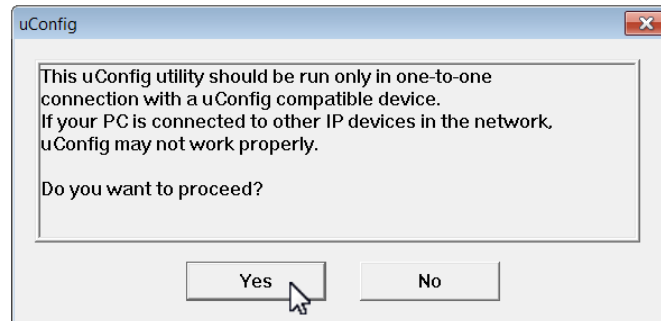
2. Select the access point from the products list and click **Open Web**. To retrieve and display the latest device(s) in the list, click **Refresh**.
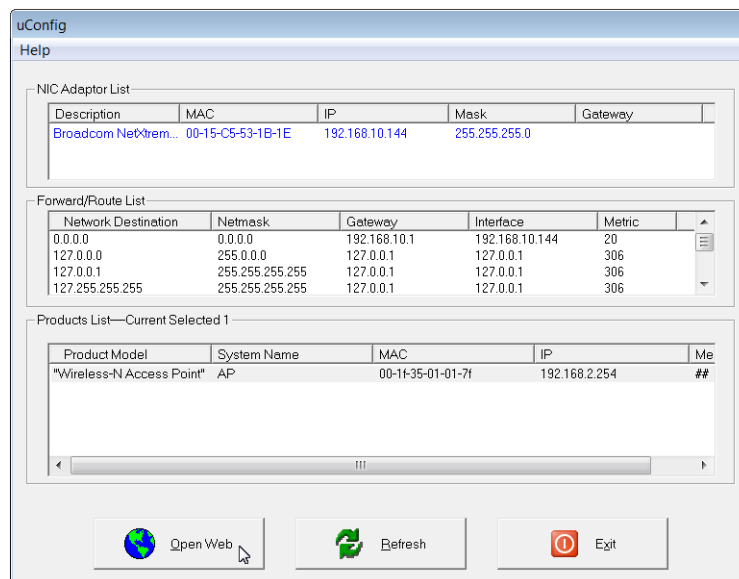
3. Click **OK**.

4. At the login prompt, enter the User Name and Password. The defaults are :

   User Name : **admin**

   Password : **password**

5. Click **OK**. The device home page (Status page) opens.

NOTE: Do not exit the uConfig program while accessing the web-based interface as this will disconnect you from the device.

Access with Web Browser

The following procedure can be performed using any standard Web browser (Internet Explorer, FireFox, Chrome, etc.). Note, however, that steps are described using Internet Explorer 9 and the menu selections may be different if you are using a different version or a different program.

1. Launch your Web browser and click **Tools**, then click **Internet options**.
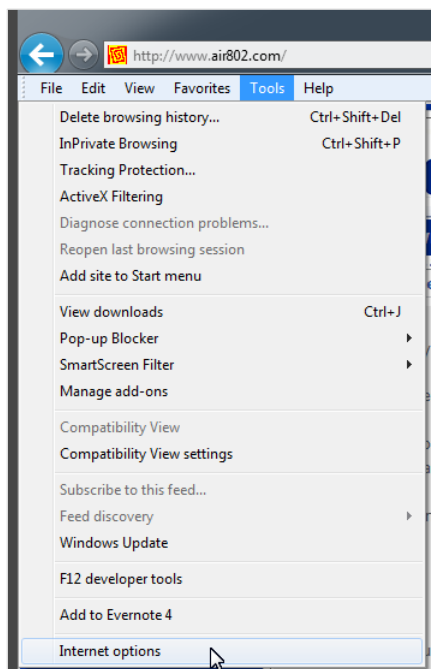
2. Click **Connections** then click **LAN settings.** Click to clear all selection boxes (remove all checkmarks).

3. Click **OK** to update the changes.
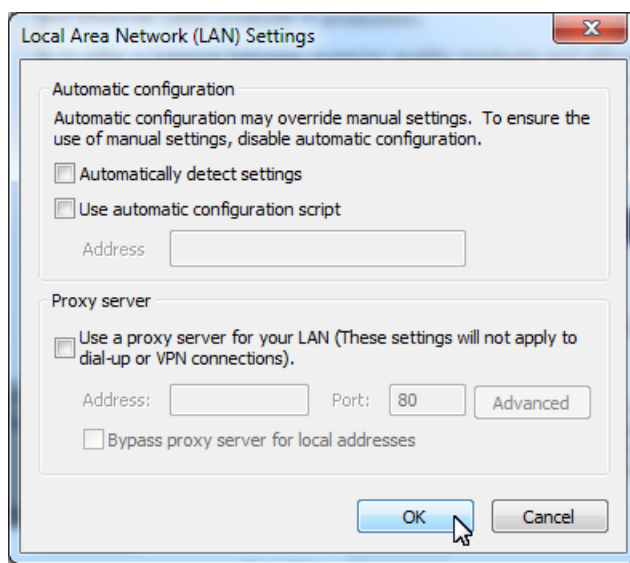
4. In the Address bar type **http://192.168.168.1** and press **Enter**.

---

5. At the login prompt, enter the User Name and Password. The defaults are :
User Name : **admin**
Password : **password**

6. Click **OK**. The device home page (Status page) opens.

Navigation

Main Menu Bar

| STATUS | BASIC WIRELESS | BASIC NETWORK | ADVANCED WIRELESS | ADVANCED NETWORK | VLAN | SERVICES | SYSTEM |

Status Displays current status of the device and statistical information.

Basic Wireless Provides the controls for wireless network configuration, basic wireless settings that define operating mode, associated details and data security options.

Basic Network Allows the configuration of network operating mode, IP settings and network services (i.e., DHCP Server).

Advanced Wireless Provides settings for advanced wireless features.

Advanced Network Provides settings for more details of network features.

VLAN lets you create virtual local network connections through the device using Ethernet or wireless connections.

Services Allows the configuration of system management services (i.e.. Ping Watchdog, Auto-Reboot, SNMP, NTP, Telnet, SSH, System Log).

System Providess controls for system maintenance routines, administrator account management, device customization and configuration backup.

Activation Keys Optional special add-on functions you can purchased separately and activate in device.

Save Changes

When you have finished making changes on any of the setup pages, click **Apply Settings** to save the changes to the device's flash memory. You are asked to confirm that you want to save the changes. Click **Save** to write the configuration changes to flash memory or **Discard** to discard the changes and return to the previous settings.

Basic Wireless

All of the basic wireless settings can be configured in this page. Operators can change the ESSID, regulatory country code, wireless profile, channel spectrum width, frequency of interest, data rates, transmit power and rate aggressiveness.

NOTE: When you click the Basic Wireless tab, the Radio Selection box opens. Currently the device supports only one 802.11n radio card. Click Radio 1 to configure.

Enable the radio

To enable the radio, click the **Enable Radio 1** selection box to place a checkmark in the box. To disable the radio, click the **Enable Radio 1** selection box to remove the checkmark in the box.

Wireless Mode

There are five modes available. Click a mode in the Wireless Mode drop-down list.

Station

This is a client mode that can be connected to the Access Point mode. It is used to bridge the wireless connection to an Access Point. It forwards all the traffic to and from network devices to the Ethernet interface. This mode translates all the packets that pass through the device to its own MAC address, resulting in a lack of transparency.

Station WDS

WDS (Wireless Distribution System) mode can be connected to the Access Point WDS mode and enables packet forwarding at layer 2 level. Unlike Station mode, it is fully transparent at layer 2 level.

Access Point

This mode can be connected to Station mode and forwards all traffic to the network devices connected to the Ethernet devices of the Station.

Access Point WDS

This mode can be connected to Station WDS mode. Using WDS protocol, it allows a client or station device to bridge wireless traffic transparently.

Repeater WDS

This mode consists of a Station WDS and an Access Point WDS mode. The Repeater WDS must first link with an Access Point WDS, and then it can link with a Station WDS. It acts as an extension to the link and you can add more Repeater WDS devices as necessary.

NOTE:

1. The WDS protocol used for Station WDS, Access Point WDS, and Repeater WDS is not defined as a standard, thus compatibility issues between equipment from different vendors might arise.

2. For Repeater WDS, ESSID must be the same for the Remote AP and the Local AP. The channels used to link one repeater to another Repeater will follow the Access Point WDS connection's selected channel.

Access Point Parameters Settings

BASIC WIRELESS SETTINGS

Wireless Mode:	Access Point ▼
Local AP-ESSID:	AIR802 ☐ Hide SSID
Country Code:	United States of America ▼ ☑ No Country Set
Wireless Profile:	NA ▼
Channel Spectrum Width:	20/40M ▼
Guard Interval:	Short ▼
Channel-Frequency:	5200M ▼ ☑ Auto [Select] [ ]
	[Interference Analyzer]
Data Rate (Mbps):	6 Mbps ▼ ☑ Auto
Transmit Power:	29 ▼ **dBm** Chainmask: 2x2 Dual - Aggregate Dual Chain Power
	☑ Maximum
	☐ Obey Regulatory Power
Rate Aggressiveness:	0 ▼

Local AP-ESSID

This is the Service Set Identifier used to identify the operator's wireless LAN. It should be specified while operating in Access Point or Access Point WDS mode.
All of the client devices within its range will receive broadcast messages from the access point advertising this SSID.

Hide SSID
Once checked, this will disable advertising the SSID of the access point in broadcast messages to wireless stations. This option is only available in Access Point, Access Point WDS and Repeater WDS mode.

Country Code

Different countries have different power level requirements and frequency selections. To ensure device operation follows regulatory compliance rules, select the correct country code for the location where the device will be used. The channel list, output power limits, IEEE 802.11 and Channel-Spectrum Width modes will be tuned according to regulations of the selected country.

No Country Set

When this option is checked, only the following frequency ranges are available:
11n 2.4GHz (2412 to 2462MHz), 11n 5GHz (5180 to 5320MHz) and 5745-5825MHz.

Wireless Profile

- NA is the 11n 5GHz band and represents a mixed of 802.11n and 802.11a mode.
- NG is the 11n 2.4GHz band and represents a mix of 802.11n, 802.11g and 802.11b mode.

Channel Spectrum Width

- 20M represents data transmission at a bandwidth of 20MHz.
- 20/40M represents data transmission at either 20MHz or 40MHz. In a very noisy environment it automatically falls back to 20MHz to be more resilient to the interference. In situations where auto fall back does not happened, manually changing channel spectrum width to 20MHz will help reduce interference on the link and improve performance.

  NOTE: 40MHz bandwidth is non-standard for 802.11n/g mode operation. If you experience unstable performance, change Channel Spectrum Width to 20M.

Guard Interval: ???

Channel – Frequency

This sets the operating frequency of the device. The frequency range available depends on the country domain selected in Country Code. For the 5GHz frequency range, some countries have regulations that control DFS characteristics. Selecting one of these

---

frequencies for operation may cause a delay of two minutes or more (possibly up to ten minutes in some situations) for the device to attempt to establish a connection.

When **Auto** is enabled, during startup the device automatically selects the channels (or frequency) with the least interference for operation.

Data Rate

Data Rates consist of both the legacy rates and the MCS (Modulation Coding Scheme – only for 802.11n) rates.

- 6 – 54Mbps are legacy rates.

- MCS0 to MCS7 are 802.11n rates that use only one stream.

- MCS8 to MCS15 are 802.11n rates that use two streams.

When **Auto** is enabled, the data rate is automatically selected using an advanced rate algorithm that takes into consideration the number of errors at each data rate and fine tunes to the best data rate possible.

Transmit Power

The maximum transmit power available is determined by the country code and the maximum transmit power of the miniPCI that is being used.

NOTE: if the channel is changed to a new frequency with higher power output permitted by regulation, the previously selected power level will remain unchanged. You need to readjust the power level to in order to take advantage of the higher output power available for the channel.

Rate Aggressiveness

Allows an increase or reduction in transmit rate while still remaining in Auto mode. There are two situations where Rate Aggressiveness is useful.

1. If the environment is noisy at times, lowering the throughput will ensure better stability. Rate Aggressiveness allows reduced transmit rate, so range or power can be higher. Choose -3, -2, or -1.

2. The environment might be free of interference, but the fully auto algorithm gives low throughput. Increased Rate Aggressiveness will increase transmit rate in this case to get higher throughput. Choose +3, +2, or +1.

Station Parameters Settings

The options below are only available in Station, Station WDS and Repeater WDS modes, unless otherwise stated.

Remote AP-ESSID

This is the Service Set Identifier used by the station to seek and connect to the access point of the same SSID identifier.

Site Survey

Site Survey will search for the available wireless networks in range on all supported channels and will allow you to select one for association. If the selected network uses encryption, you also need to set security parameters in the wireless security section. Click **Scan** to re-scan for all access points in range. Select the Access Point from the list and click **Close**. The Site Survey channel scan list can be modified using the Channel Scan List control.

Remote AP – Lock to MAC

Enter the MAC address of the remote access point the device is connected to. This option will make the device only connect to this access point. This is important when the connection is Point-to-Point operation.

Remote AP - Preferred MAC

Enter the preferred MAC addresses of the access points you want the device to connect to when it first starts up. Up to four MAC addresses can be entered. Priority is from top to bottom. In the event that all preferred MAC addresses are not available, the device will pick the matching SSID access point with the strongest signal.

Country Code

Different countries have different power level requirements and frequency selections. To ensure device operation follows regulatory compliance rules, make sure to select the correct country code for the device location. The channel list, output power limits, and IEEE 802.11 and Channel Spectrum Width modes will be tuned according to the regulations of the selected country. Station setting must match the AP country code setting.

If the **No Country Set option** is checked, only the following frequency ranges are available:

- 11n 2.4GHz (2412-2462MHz)
- 11n 5GHz (5180-5320MHz and 5745-5825MHz).

Wireless Profile

NA is the 11n 5GHz band and represents a mix of 802.11n and 802.11a mode.

NG is the 11n 2.4GHz band and represents a mix of 802.11n, 802.11g and 802.11b mode.

NOTE: Station setting must match the AP Wireless Profile setting.

Channel Spectrum Width

20M represents data transmission at a bandwidth of 20MHz.

20/40M represents data transmission at either 20MHz or 40MHz. In a very noisy environment it automatically falls back to 20MHz to be more resilient to the interference. In situations where auto fallback does not happen, manually changing channel spectrum width to 20MHz will help reduce interference on the link and improve performance.

NOTE:

1. 40MHz bandwidth is non-standard for 802.11n/g mode operation. If you experience unstable performance, change the Channel Spectrum Width to 20M.
2. Station setting must match the AP Channel Spectrum Width setting.

If the **Maximum** option is checked, maximum Tx output power will override regulated maximum for the selected country.

If the **Obey Regulatory Power** option is checked, maximum Tx output power corresponds to the regulated maximum for the selected country.

Channel Scan List

From a list of channels associated with the selected country code, you can choose which channels are scanned when scanning for an Access Point. Then the scanned channels will appear on the Site Survey.

Wireless Security Settings

All wireless security settings are chosen in this section.

The menu is the same for all Wireless modes.

WPA or WPA2 Authentication (PSK)

Security

- WPA
- WPA2

Authentication

- PSK (Pre-shared Key) method (default).

Cipher Type:

- TKIP - Temporal Key Integrity Protocol, which uses RC4 encryption algorithm.
- AES - Advanced Encryption Standard algorithm.
- AUTO (Default) – Automatically selects between the two algorithms.

Preshared Key

The pre-shared key is an alpha-numeric password between 8 and 63 characters long. This option is available for WPA or WPA2, with PSK selected.

NOTE:An 802.11n network using WPA authentication should use AES cipher type for connection. Only AES allows highest transmission speed and throughput. Using TKIP cipher type will limit maximum transmission speed to 54Mbps only.

WPA + EAP

LOCAL AP - WIRELESS SECURITY:

Security:	WPA ▼		
WPA Authentication:	EAP ▼	Cipher Type:	AES ▼
WPA Preshared Key:	11111111		
Pri. Radius Server IP:	0.0.0.0		
Sec. Radius Server IP:	0.0.0.0		
Authentication Port:	1812		
Accounting Port:	1813		
Radius Secret Key:	private		
MAC ACL:	☐ Enabled		Add
Policy:	▼		Remove

Security

- WPA

- WPA2

WPA Authentication

- EAP (Extensible Authentication Protocol). Firmware supported options are EAP-TTLS and EAP-PEAP

Cipher Type

- TKIP - Temporal Key Integrity Protocol, which uses RC4 encryption algorithm.

- AES - Advanced Encryption Standard algorithm.

- AUTO (Default) – Automatically selects between the two algorithms.

WPA Preshared Key

???

Primary Radius Server IP

Enter the Primary Radius Server IP address.

Secondary Radius Server IP

Enter the Secondary Radius Server IP address.

Authentication Port

Enter the Authentication Port number of the Radius Server. Default is 1812.

Accounting Port

Enter the Accounting Port number of the Radius Server. Default is 1813.

Radius Secret Key

Enter the Secret Key of the Radius Server. The device use this to authenticate itself with Radius Server.

MAC ACL

???

Policy

???

WPA EAP-TTLS and WPA EAP-PEAP

This applies to Station, Station WDS, and Repeater WDS modes.

Security

- WPA
- WPA2

WPA Authentication

- EAP-TTLS
- EAP-PEAP

Cipher Type

- TKIP - Temporal Key Integrity Protocol, which uses RC4 encryption algorithm.
- AES - Advanced Encryption Standard algorithm.
- AUTO (Default) – Automatically selects between the two algorithms.

WPA Preshared Key

???

Identity

Identification credential used by the WPA-supplicant for EAP authentication.

User Name

Identification credential used by the WPA-supplicant for EAP tunneled authentication in unencrypted form.

User Password

Password credential used by the WPA-supplicant for EAP authentication

IEEE802.1x Settings

NOTE: Operating with IEEE802.1x security will limit maximum wireless link speed to 54Mbps.

This applies to Access Point, Access Point WDS, and Repeater WDS modes only.

Pri. Radius Server IP

Enter the Primary Radius Server IP that the Access Point will use to query the server.

Sec. Radius Server IP

Enter the Secondary Radius Server IP that the Access Point will use to query the server.

Authentication Port

Enter the Radius Server Authentication Port number to use. The default is 1812.

Accounting Port

Enter the Radius server Accounting Port to use. The default is 1813.

Radius Secret Key

Enter the Radius server Secret Key that Access Point to use to authenticate itself with radius

server.

IEEE802.1x Key Rotation

Time before activating key rotation in authentication process for higher security. Enter time in seconds.

IEEE802.1x Key Length

This is the key length of the initial seed key. Select 64 or 128bit.

WEP

NOTE: Operating with WEP security will limit maximum wireless link speed to 54Mbps.

Authentication Type

- Open Authentication –No authentication. This is the default and is recommended.

- Shared Authentication – May not be compatible with all Access Points. Not recommended.

Key Type

HEX or ASCII option specifies the character format.

Current Key

Specify the Index of the WEP Key used. Four different WEP keys can be configured, but only one is used.

WEP Key

Specify the WEP encryption key for the wireless traffic encryption and decryption.

WEP Key Length

Select 64-bit (default) or 128-bit WEP Key length. . The 128-bit option will provide a higher level of security.

For 64-bit, specify the WEP key as five HEX pairs (0-9, A-F or a-f, e.g., 00112233AA) or five ASCII characters.

For 128-bit, specify the WEP key as 13 HEX pairs (0-9, A-F or a-f. e.g., 00112233445566778899AABBCC) or 13 ASCII characters.

MAC ACL

???

Policy

???

Virtual Access Point (VAP)

Virtual AP (VAP) implements mSSID (Multi-SSID), whereby a single wireless card can be configured with up to three virtual SSID or BSSID connections. Each VAP can be set with a different security authentication mode.

Only Available in Access Point and Access Point WDS Mode.

All VAPs are created from the same radio and share the same wireless channel, country code, channel spectrum width and transmit power.

NOTE: Security options like IEEE802.1x and WPA-EAP uses radius server for authentication and accounting. You may not use a different secret key for each VAP. Or you should configure only one SSID with radius authentication.

Basic Network Settings

Click **BASIC NETWORK** on the menu bar to open the Basic Network page.

Network Information

Network Mode
Select between Bridge (default) and Router mode.

Local Area Network

LAN Mode

- **Static**: (default) lets you enter a specific IP address for the device. Default IP address is 192.168.168.1
- **DHCP Client**: lets the device learn the IP address automatically from the network.

Netmask
Let you set the class for the IP address set. Default is class C and value 255.255.255.0

Gateway IP (optional)
Enter the gateway IP address of the network the device is connected.

DHCP Fallback IP

???

DHCP Mode

- **None**: function disabled
- **DHCP Server**: Check to enable. Device act IP address distribution server automatically issue. IP address and other network information to the DHCP Client request them.
- **DHCP Relay**: check to enable. Enter the IP address of the remote DHCP server where the DHCP Client request will be relayed.

DHCP Start IP Address

Enter the starting IP address to be issue.

DHCP End IP Address

Enter the last IP address the server will issue.

DHCP Netmask

Lets you set the IP class for the IP address range set for the start and end address.

NOTE: if device is also the router then IP class must be same as device IP class.

DHCP Gateway IP

Enter the last IP address the server will issue.

DHCP Lease Time

Enter the new lease time in seconds (default is 3600 seconds or 1hour)

DHCP Relay Server IP

Enter the IP address of the remote DHCP server where the DHCP Client request will be relayed to get the IP address.

DHCP Relay Gateway IP

Enter the IP address of the remote gateway where the DHCP Client request will be relayed to get the gateway IP address.

Enable DNS Proxy

Device router operation will act as proxy to resolve all DNS requests. Check to enable function.

DHCP Reservations

DHCP SERVER RESERVATIONS:

IP Address	Hardware MAC	Description	
			Add

Click **Add** to enter the IP address and MAC address for each device.

All DHCP active lease devices are displayed in the Status tab page from the More Status selection.

Domain Name Server Entry

DOMAIN NAME SERVER ADDRESSES

○ Obtain DNS server address automatically

◉ Use the following DNS server addresses:

Primary DNS IP:

Secondary DNS IP:

The Primary and Secondary DNS IP addresses entry is for device operation to resolve the domain name to reach certain servers like internet time servers and other services that use domain name.

NOTE: Ensure the device gateway IP is also set to allow access to the internet.

Primary DNS IP (optional)

Enter the primary DNS IP address nearest to the gateway router.

Secondary DNS IP (optional)

Enter the secondary DNS IP address nearest to the gateway router.

Bandwidth Control between Ethernet and Wireless

BANDWIDTH CONTROL:

Bandwidth Control:	☑ Enabled	Configure

Click the selection box to enable then click **Configure**.

BANDWIDTH CONTROL SETUP

Ethernet to WirelessTraffic Limit (kbit)-Download:	0
Wireless to EthernetTraffic Limit (kbit)-Upload:	0

An entry of value "0" means no bandwidth flow limit between the 2 interfaces. An entry of "2000" means traffic flow is limited to 2000Kbit or 2Mbit between the two interfaces.

The default is "0".

Advanced Wireless Settings

Click **Advanced Wireless** on the menu bar and select **RADIO 1** to open the Advanced Wireless page.

Long Range Parameters

Check to enable parameters.

Beacon Interval

Define the time interval (in millisecond) the beacon will broadcast. The default is 100 ms (recommended).

RTS Threshold

 The default is OFF.

Fragmentation Threshold

The default is OFF.

Distance

Enter the distance in meters between devices then click **Calculate**. Close approximate values for Slot Time, ACK Timeout, and CTS Timeout will be calculated. These can be fine tuned for best performance and link reliability.

Noise Immunity

When enabled, it automatically adjusts the signal/noise level for best performance. In a low noise environment it is recommended to turn off this function.

Signal Strength Indicator (RSSI)

The four LEDs turn on at various levels to indicate the RSSI signal strength. The default values are LED1-Red (10), LED2-Yellow (20), LED3-Green (30), LED4-Green (40). With these settings, when LED1 and LED2 are lit it indicates the RSSI is greater than 20, and when all 4 LEDs are lit RSSI is greater than 40.

For long distance installation when signal strength is expected to be between 20 and 30, the values can be adjusted to display over a lower range, such as

> LED1: RSSI value=7
>
> LED2: RSSI value=15
>
> LED3: RSSI value=22
>
> LED4: RSSI value=27

Chainmask Selection

Available selections are: 1x1 Left Chain, 1x1 Right Chain and 2x2 Dual Chain.

Selecting **1x1 Left Chain** will force the radio card to operate with one transmit and one receive stream on the left port of the radio card only.

Selecting **1x1 Right** Chain will force the radio the card to operate with one transmit and one receive stream on the right port of the radio card only.

Selecting **2x2 Dual Chain** (default) will enable the radio card to operate with two transmit and two receive streams and automatically transmit /receive on either of the radio card.

Station Isolation

When checked it prevents wireless clients on same AP from discovering other clients.

Minimum Station RSSI

???

Advanced Network

Click **Advanced Network** on the menu bar.

NOTE: This menu will not open when the device is in Bridge mode. To open the page, first enable Router mode in the Basic Network menu.

NAT Setup

NAT

Enable when in Router mode. Disable when in Bridge mode.

DMZ

Default is disabled. Check box to enable.

DMZ Private IP

Input the IP address of the local PC to receive the DMZ packets.

Port Forwarding

Default is disabled. Check on box to enable.

IP Forwarding

Default is disabled. Check on box to enable.

For configuration details refer to the Appendix.

Static Routing Table

???

Routing Information Protocol (RIP)

Routing Info Protocol

Default is disabled. Check on box to enable.

For configuration refer to Appendix section.

Router Info Protocol version

Select RIPv1 or RIPv2.

Firewall Setup

Firewall

Default is disabled. Click selection box to enable then click **Configure**.

Firewall

	On Comment	Policy	IP Type	Source IP/Mask	Src Port	Destination IP/Mask	Des Port
1.	☐	ACCEPT ▼	TCP ▼				
2.	☐	ACCEPT ▼	TCP ▼				
3.	☐	ACCEPT ▼	TCP ▼				
4.	☐	ACCEPT ▼	TCP ▼				
5.	☐	ACCEPT ▼	TCP ▼				
6.	☐	ACCEPT ▼	TCP ▼				
7.	☐	ACCEPT ▼	TCP ▼				
8.	☐	ACCEPT ▼	TCP ▼				
9.	☐	ACCEPT ▼	TCP ▼				
10.	☐	ACCEPT ▼	TCP ▼				
11.	☐	ACCEPT ▼	TCP ▼				
12.	☐	ACCEPT ▼	TCP ▼				
13.	☐	ACCEPT ▼	TCP ▼				
14.	☐	ACCEPT ▼	TCP ▼				
15.	☐	ACCEPT ▼	TCP ▼				
16.	☐	ACCEPT ▼	TCP ▼				
17.	☐	ACCEPT ▼	TCP ▼				
18.	☐	ACCEPT ▼	TCP ▼				
19.	☐	ACCEPT ▼	TCP ▼				
20.	☐	ACCEPT ▼	TCP ▼				

Apply | Cancel

Comment

Enter a brief name for the service.

Policy

Select Accept or Deny for the apply rule.

IP Type

Select ICMP, TCP, or UDP packet type.

Source IP/Mask

Enter the source IP address and Netmask. This is the source IP of the packet (specified within the packet header); usually it is the IP of the host system that sends the packets.

Src Port

Enter the source port number. This is the source port of the TCP/UDP packet (specified within the packet header); usually it is the port of the host system application that sends the packets.

Destination IP/Mask

Enter the destination IP and Netmask. This is the Destination IP of the packet (specified within the packet header); usually it is the IP of the system to which the packet is addressed.

Des Port

Enter the destination port. This is the destination port of the TCP/UDP packet (specified within the packet header); usually it is the port of the host system application to which the packet is addressed.

Click **Apply** to save the rule set or **Cancel** to clear the rule set.

Multicast Routing

???

Remote Management

???

UPnP

Default is disabled. Check box to enable.

When enabled, a client PC running Microsoft UPnP services can automatically open certain specific ports required by the PC application in the router.

For security reasons this service should not be enabled. It is recommended that ports be manually opened using the Port Forwarding service.

Services

Click **Services** on the menu bar.

This section provides various useful and enhanced functions to assist device operations.

Spanning Tree Setup

Spanning Tree Protocol

Click box to enable (add checkmark). Default is disabled.

Root Priority

Smaller value has higher priority. Default value is 32768.

Root Hello Time

Default time is 2 seconds.

Root Forward Delay

Default is 15 seconds

Root Maximum Age

Changing to a lower time can cause high overheads to the network. Default is 20 seconds.

Ping Watchdog

Enable Ping Watchdog

Default is disabled. Click box to enable (add checkmark).

IP Address To Ping

Target IP address for ping test.

Ping Interval

This is Ping test duration. Default is 5 seconds (minimum).

Startup Delay

One time delay after device startup. Default is 60 seconds(minimum).

Failure Count To Reboot

This is the number of ping failures before device starts the reboot process. Default is 5.

Auto-Reboot

Auto-Reboot Mode

This mode lets you preset a timer to automatically force a reboot. Timer can specify a fixed number of hours (By Hour) or at a specified time of day (By Time). Default is disabled.

- **By Hour**: Enter the number of hours device is to run before starting the reboot process.
- **By Time**: Enter the specific time of day in hh:mm (24-hour format) to start the reboot process.

SNMP Setup

Enable SNMP
Default is disabled. Click box to enable (add checkmark).

Read Only Password
Password to query device.

Engine ID
Default is 800007e5BD00002704D000007c.

Enable SNMP Trap
Default is disabled. Check on box to enable.

Trap Destination IP
Enter the IP to send the info when trap is triggered.

Community
Enter the SNMP community string.

NTP Setup

Select Your Time Zone
Select your country from the list.

Current Router Time
???

Proposed Router Time
???

Enable NTP Client
???

Known Time Server
Select a time server from the list. ???

Time Server

Enter the preferred time server domain or IP. Default is "time.nist.gov". ???

Web Server

Web Server Mode

Option is HTTP and HTTPs. Default is HTTP.

HTTP(s) Port

Enter preferred port number. Default is 80 for HTTP and 413 for HTTPs.

Telnet Server

Enable Telnet Server

Default is enabled. Remove check from box to disable.

Server Port

 Enter preferred port number. Default is 23.

SSH Server

Enable SSH Server

Default is disabled. Click box to enable (add checkmark).

Server Port

Enter preferred port number. Default is 22.

System Log

Enable System Logging

Default is disabled. Click box to enable (add checkmark).

Logging IP /Domain Name

Enter destination IP address of device to receive log.

Logging Port

Default is 514. Enter the new preferred port number.

System

Click **System** on the menu bar.

The System Page contains Administrative options that let the administrator customize, reboot the device, set it to factory defaults, upload new firmware, backup or update the configuration and configure administrator's credentials.

FIRMWARE UPGRADE

Firmware Version:	2.28 (build 120306)
	[ ] [Browse...]
	[Upload]

HOST NAME

Host Name:	AP
	[Apply]

ADMINISTRATIVE ACCOUNT

Administrator Username:	admin
Current Password:	[ ]
New Password:	[ ]
Verify New Password:	[ ]
	[Apply]

READ-ONLY ACCOUNT

Enable Read-Only Account:	☑
Read-Only Username:	guest
Password:	[ ]
	[Apply]

CONFIGURATION MANAGEMENT

Backup Configuration:	[backup...]
Backup System Log:	[backup...]
Upload Configuration:	[ ] [Browse...]
	[Restore]

DEVICE MAINTENANCE

[Reboot...]	[Reset to defaults...]

Firmware Upgrade

Use this section to determine the current software version and update the device with new firmware. The device firmware update is compatible with all configuration settings. System configurations are preserved while the device is updated with a new firmware version.

NOTE: Download the new firmware to the PC before starting this procedure.

Firmware version

Displays the version of the current firmware of the device system.

Firmware File

Click **Browse** to navigate to and select a new firmware file or specify the full path to the file location.

Upload

Click **Upload** to open the Firmware Upload window and start the upload process.

NOTE:

1. The firmware upgrade routine can take 3-7 minutes. The device will not be accessible until the firmware upgrade routine is completed.

2. Do not switch off the device, reboot or disconnect the device from the power supply during the firmware upgrade process as these actions will damage the device!

3. It is highly recommended to backup the system configuration and the Support Info file before uploading the new configuration.

Host Name

Host Name is the system wide device identifier. It is reported by SNMP Agent to authorized management stations. Host Name will be represented in popular Router Operating Systems registration screens and discovery tools.

Host Name

Specifies the system identity.

Apply

Saves the Host Name if activated.

Administrative Account

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first system setup:

Administrator Username

Specifies the name of the system user. Default is "admin".

Current Password

Administrator is required to enter a current password. It is required for Password or Administrator Username change routine. Default is "password".

New Password

Specify a new password to be used for administrator authentication.

Verify New Password

Re-enter the new password to verify its accuracy.

Click **Apply** to save the changes.

Read-Only Account

Enable Read-Only Account

Click box to enable or disable (add or remove checkmark).

Read-Only Username

Specify a username to be used for read-only access.

Password

Specify a password to be used for read-only authentication.

Configuration Management

Backup Configuration

Click **Backup** to export the current configuration to a file.

Backup System Log

Click **Backup** to export the system log to a file.

Upload Configuration

Click **Browse** to navigate to and select the new configuration file or specify the full path to the configuration file location.

Click **Restore** to transfer the new configuration file to the system then click **Apply**. The new configuration will be effective after a system reboot cycle is completed. The previous system configuration is deleted.

NOTE:

1. It is highly recommended to back up the system configuration before uploading the new configuration.

2. Use only configuration backups for the same type of device. Behavior may become unpredictable when mixing configurations from different devices.

Device Maintenance

The controls in this section are for the device maintenance routines: rebooting and resetting.

Reboot

Click **Reboot** to initiate full reboot cycle of the device. The effect of the software reboot is the same as a hardware reboot or power off - power on cycle. The system configuration is not modified after the reboot cycle completes however any non-applied changes will be lost.

Reset to Defaults

Click **Reset to Defaults** to reset all device settings to the factory default. The running system configuration will be deleted and the default system configuration will be set. After the Reset to Defaults routine and Reboot process are completed, the device will return to the default IP configuration (192.168.168.1/255.255.255.0) and will operate in Station-Bridge mode.

NOTE: It is highly recommended to back up the system configuration before uploading the new configuration.

Status

Click **Status** on the menu bar.

The Status Page displays a summary of link status information, current values of basic configuration settings (depending on operating mode), network settings and traffic statistics of all the interfaces.

Main

Uptime

Displays device up time since last boot up. The time is expressed in days, hours, minutes and seconds.

Host Name

Displays the assigned device host name (ID).

System Time

Display device current date and time. Accurate system date and time is retrieved from the internet services using NTP (Network Time Protocol) if the device is setup and connected to the internet. Otherwise, the date and time is maintained by the device`s internal clock.

Version

Firmware Version

Displays the firmware version in use.

Loader Version

Displays the loader version in use.

LAN Setting

LAN MAC

Displays the MAC address of the device LAN (Ethernet) interface.

Mode

Displays the mode used, either static or DHCP client.

IP Address

Displays the current IP address of the LAN (Ethernet) interface.

Gateway IP Address

Displays the IP address of the gateway used in LAN.

Pri. DNS IP

Displays the Primary DNS IP address of the LAN setting.

Sec. DNS IP

Displays the Secondary DNS IP address of the LAN setting.

LAN Cable

???

WAN Setting

WAN MAC

Displays the MAC address of the device WAN interface.

Mode

Displays the mode used, either DHCP, PPPoE or Static IP.

IP Address

Displays the current IP address of the WAN interface.

Gateway IP Address

Displays the IP address of the gateway used in WAN.

Pri. DNS IP

Displays the Primary DNS IP address of the WAN setting.

Sec. DNS IP

Displays the Secondary DNS IP address of the WAN setting.

Radio

Wireless Mode

Displays the current operating mode of the device.

Local AP SSID

Displays the current SSID (Service Set Identifier) of device when operating in access point mode.

Frequency

Displays current operating frequency.

MAC

Displays the MAC address or BSSID of the current active WLAN card running in device.

Local/ AP MAC

Displays the MAC address of the connected WLAN card.

Security
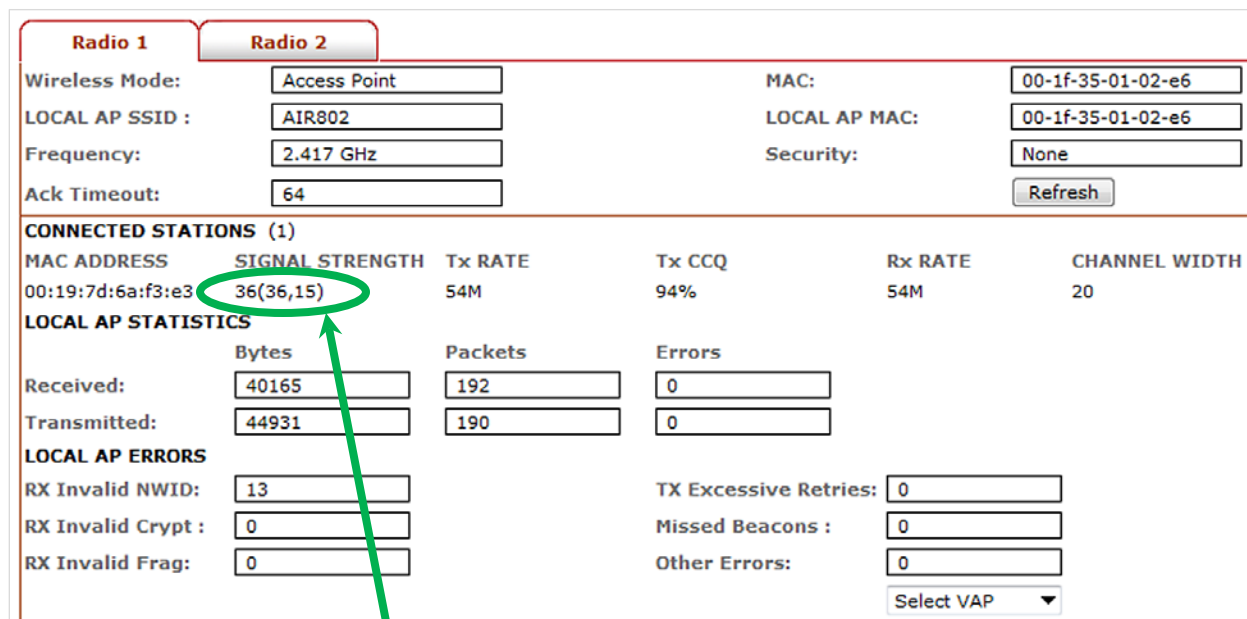
Display the currently active security mode.

Client Connection Status

All clients connected to the AP can be view from the AP Status page.

Below is an example of a client connection status info.

Click **Refresh** to refresh the client connection statistics and status page.

Radio 1	Radio 2		
Wireless Mode:	Access Point	MAC:	00-1f-35-01-02-e6
LOCAL AP SSID :	AIR802	LOCAL AP MAC:	00-1f-35-01-02-e6
Frequency:	2.417 GHz	Security:	None
Ack Timeout:	64		Refresh

CONNECTED STATIONS (1)

MAC ADDRESS	SIGNAL STRENGTH	Tx RATE	Tx CCQ	Rx RATE	CHANNEL WIDTH
00:19:7d:6a:f3:e3	36(36,15)	54M	94%	54M	20

LOCAL AP STATISTICS

	Bytes	Packets	Errors
Received:	40165	192	0
Transmitted:	44931	190	0

LOCAL AP ERRORS

RX Invalid NWID:	13	TX Excessive Retries:	0
RX Invalid Crypt :	0	Missed Beacons :	0
RX Invalid Frag:	0	Other Errors:	0

Select VAP ▼

The radio card's signal strength values can be used to adjust the antenna for balanced reception. The numbers are : Average signal (Left port signal, Right port signal).

MAC Address

Displays the MAC address of the current active WLAN card.

Signal Strength

Displays the received wireless signal level for Average (Left port, Right port) .

TX Rate and RX Rate

Displays the current 802.11 data transmission (TX) and data reception (RX) rate while operating in Station mode. Typically, the higher the signal, the higher the data rate and consequently the higher the data throughput.

Channel Width

20 indicates established connection is 20MHz channel width

40+ indicates established connection is 40MHz channel width

Local AP Statistics:

Transmitted and received values represent the total amount of data (in bytes) transmitted and received during the connection.

Local AP Errors

Displays counters for 802.11 specific errors that were registered on the wireless interface:

- **Rx invalid NWID**: value represents the number of packets received with a different NWID or ESSID, i.e., packets that were destined for another access point. It can help to detect configuration problems or identify the adjacent wireless network existence on the same frequency.

- **Rx Invalid Crypt**: value represents the number of transmitted and received packets that were encrypted with the wrong encryption key and failed the decryption routines. It can be used to detect invalid wireless security settings and encryption break attempts.

- **Rx Invalid Frag**: value represents the number of packets missed during transmission and reception. These packets were dropped due to re-assembling failure as some link layer fragments of the packet were lost.

- **Tx Excessive Retries**: value represents the number of packets that failed to be delivered to the destination. Undelivered packet are retransmitted a number of times before an error occurs.

- **Missed beacons**: value represents the number beacons (management packets sent at regular intervals by the Access Point) that were missed by the client. This can indicate that the wireless client is out of range.

- **Other errors**: value represents the total number of transmitted and received packets that were lost or discarded for other reasons.

More Status

The options in More Status provide some useful tools and additional status pages.

Ping Utility

A ping tool to test the connectivity between devices.

ARP Table

Displays a list of MAC addresses of the connected devices

Bridge Table

Displays a list of devices connect to the bridge interface

DHCP Active Lease Table

Display a list of IP addresses leased to all computers.

VLAN

Click **VLAN** on the menu bar.

These settings let you create virtual local network connections through the device via Ethernet and over wireless connections. By default VLAN mode is disabled.

VLAN Switch

To setup VLAN network check on VLAN Switch

To add a VLAN ID Tag for an Ethernet port, in ETHERNET VLAN enter the ID number, select **Tag** and click **Add.**

To add a VLAN ID Tag for the MAIN wireless SSID, in RADIO 1 VLAN click the **Main** tab, enter the ID number, select **Tag** and click **Add**.

To add a VLAN ID Tag for VAP1 wireless SSID, enter the ID number, in RADIO 1 VLAN click the **VAP1** tab, select **Tag** and click **Add**.

To add a VLAN ID Tag for VAP2 wireless SSID, in RADIO 1 VLAN click the **VAP2** tab, enter the ID number, select **Tag** and click **Add**.

To add a VLAN ID Tag for VAP3 wireless SSID, in RADIO 1 VLAN click the **VAP3** tab, enter the ID number, select **Tag** and click **Add**.

Similarly, to untag a VLAN ID enter the ID number, select **Untag** and click **Add.**

WARNING: Adding a VLAN ID Tag to a device interface port can cause loss of connection to the device web manager if the PC ethernet port or wireless connection do not have a VLAN ID Tag or do not have the same VLAN ID Tag setup. If this happens, use the device Reset button to clear the config and reconfigure. See the Reset button operations section.

Refer to Appendix V for VLAN setup examples.

VLAN Management

VLAN management lets you control and limit client connection of same VLAN ID tag group be open AP device web page.

NOTE:

1. VLAN Management works only in VLAN tag pass-through mode. i.e., VLAN Switch is disabled.

2. When the VLAN Switch is enabled or configured, the VLAN Management function stops operating.

Example:

Assuming there are two VLAN ID groups, 2001 and 2002 set up in the AP device.

One entry in VLAN Management has VLAN ID 2001 with masquerade IP address 192.168.168.20.

Another entry in VLAN Management has VLAN ID 2002 with masquerade IP address 192.168.168.10.

You can only select one of the entries to be the active VLAN ID and IP address.

If the VLAN ID 2001 group is selected, then only computers in that group can open the AP device web page using the IP address http://192.168.168.20.

To change to ID group VLAN ID 2002, click the 2002 radio button under Management IP, then click **Apply** and **Saved**.

If there is no entry in VLAN Management, there is no restriction. All computers can open the AP device web page using the default IP address defined in the Basic Network page.

AUTO-DISCOVERY TOOL

Auto-discovery can be used to find any AIR802 access points in your local area network. The tool is named **WirelessConfig.exe** and can be found on the CD included with the AP25N01.

1. Locate the file on the CD and click to open the file. The configuration tool screen opens.
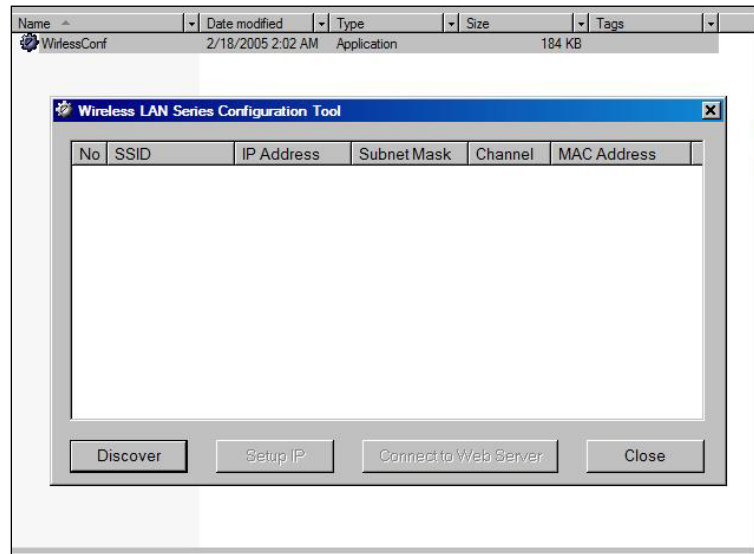
2. Click the Discover button. Any AIR802 access points on the network will appear in the list area.
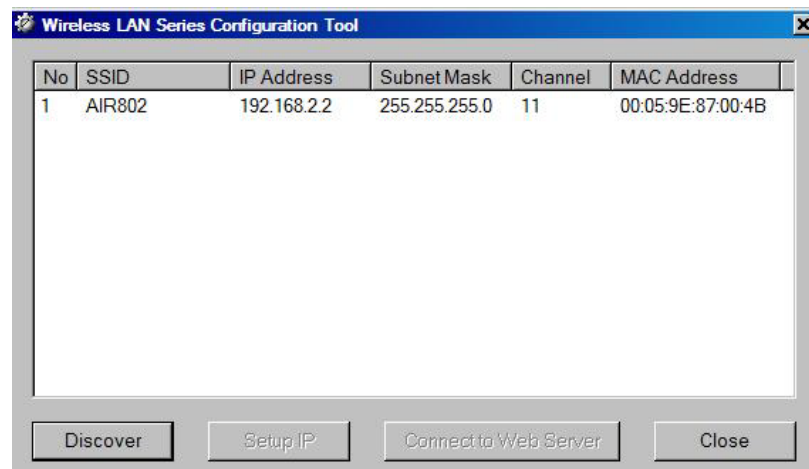
3. Click once on the desired network. The following screen will appear.
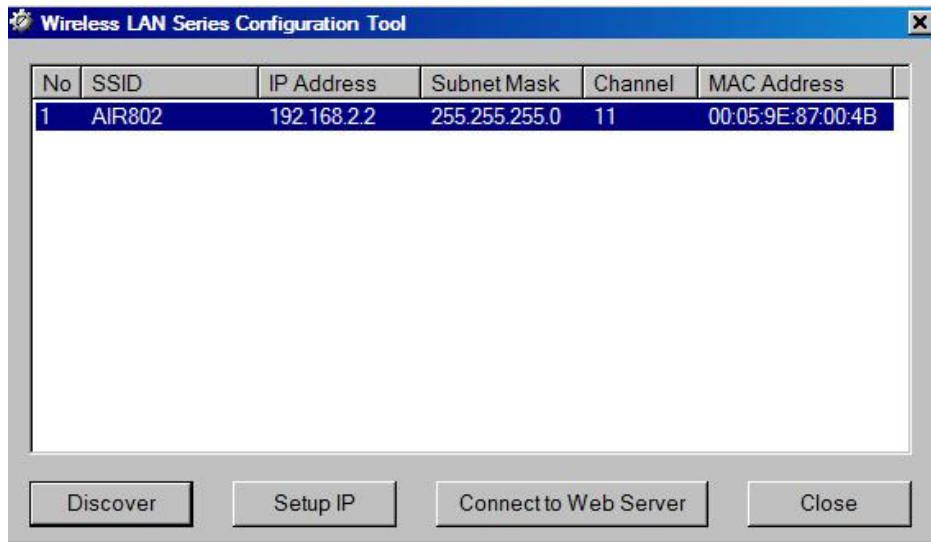
To change the IP address and/or User Name and Password of the AIR802 access point, click **Setup IP**.

If are you on the same subnet, you can connect to an access point by clicking twice on the listing in the discover area or clicking **Connect to Web Server**. Depending on the access point configuration mode, you can access it via the wireless or wired interface.

TROUBLESHOOTING

Basics

After you turn on power to the AP25N01, the following sequence of events should occur:

1. When power is first applied, the Power LED turns on.
2. if a computer/router/modem is connected via the Ethernet port, the Ethernet LED turns on after approximately one minute.

Power LED Not On

If the Power and other LEDs are off, make sure that the power supply is properly connected to the AP25N01 and to a power source. If the error persists, there is a hardware problem and you should contact technical support.

Ethernet LED Not On

If the Ethernet LED does not light when the Ethernet connection is made, the AP25N01 is not "seeing" the other device. Check the following:

- Ensure that you are using a good, proper cable.
- Make sure that the Ethernet cable connections are securely connected to the access point and at the other end of the cable.

Web Browser Configuration Screen Not Available

If you are unable to access the AP25N01's Web Configuration interface from a computer on your local network or a directly connected computer, check the following:

- Check the Ethernet connection between the computer and the router. The Ethernet LED must be on; if it is not on, a proper connection does not exist and there is likely a cabling problem.
- Make sure your computer's IP address is on the same subnet as the AP25N01. If you are using the default addressing scheme of the AP25N01, your computer's address should be in the range of 192.168.2.1 to 192.168.2.253. Refer to Configuration Preparation in this manual for instructions on how to verify the TCP/IP properties and for instructions on how to configure your computer.
- If you do not know the AP25N01's current IP address, you can use the "auto-discovery tool" on the CD that comes with the AP25N01. This will discover the IP address whether or not your computer has an IP address on the same subnet. If it is not discovered by our tool or you can't gain access by typing the IP address into the web browser URL line, make sure that you do not have a firewall blocking access.
- If you have previously successfully gained access and changed the operation mode to "Router", you will not be able to access the AP25N01 from the wired interface.

- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.

- If you are configuring more than one access point using the same PC, you may encounter an Address Resolution Protocol (ARP) issue. This is due to the access points having the same default IP address but different MAC addresses. If this is the case, try and clear the ARP table of your PC through a DOS command (click Start, click Run, enter CMD in the dialog box, enter arp –d at the prompt and press Enter). Alternatively, you can clear the issue by restarting your PC.

- Try quitting the browser and launching it again.

- If you still can't gain entry, try a hard reset by pressing the reset switch (with power on) for 10 seconds. The unit takes one to two minutes to fully reload the default configuration settings. This will reset the IP address back to 192.168.2.254 if it had been changed.

Configuration Changes Not Saved

If the AP does not save changes you have made to the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click **Apply Settings** before moving to another menu or tab, or your changes will be lost.

- Click **Refresh** or **Reload** in the Web browser. The changes may have been made but the Web browser is caching the old information.

No Internet Access ???

Wireless (Bridge - AP Mode)

If you are unable to access the Internet through the AP25N01:

- Verify that you have established a wireless connection between your computer and the AP25N01.

- Unless you are using static IP addresses in your network, verify whether you have been provided an IP address. To do this go click **Start**, click **Run**, Type "CMD" in the dialog box and press **Enter**, type "ipconfig" at the prompt and press **Enter**. Scroll up as necessary to see if a valid IP address has been provided. Note: Recent versions of Windows and MacOS will generate and assign an IP address in the range of 169.254.x.x if the computer cannot reach a DHCP server. If the listed IP address is in this range, you have not been assigned an IP address by the DHCP Server. This indicates a likely issue in the configuration or cabling to an upstream device providing DHCP function.

- If you have enabled encryption (security), access the AP25N01 via the wired Ethernet interface (unless the operating mode is Router). Disable security and re-check to see if you have connectivity. If you do have connectivity, encryption was not properly established between your computer and the AP25N01.

- If your computer has been given a proper IP address, make sure that the IP address is in the same subnet as the IP address of the AP25N01. If it is, click **Start**, click **Run**, Type "CMD" in the dialog box and press **Enter**. At the prompt, type "Ping x.x.x.x" (where the x's equal the IP address of the AP25N01). You should receive four replies, which indicates that you have a proper connection to the AP25N01. Change your computer's IP address back to the normal setting. You should then be able to "ping" the IP address of any device farther back in the network (another router, modem, etc.). If you are unable to ping a device farther into the network, then you don't have a connection between the AP25N01 and the next device.

Troubleshooting a TCP/IP Network Using a Ping Utility **???**

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. This makes troubleshooting a TCP/IP network very simple.

Testing the LAN Path to Your AP

You can ping the AP from your computer to verify that the LAN path to your AP is set up correctly.

To ping the router from a PC running Windows:

1. From the Windows toolbar, click **Start** and select **Run**.

2. In the field provided, type "ping" followed by the IP address of the router, for example:

   ping 192.168.2.254

3. Click **OK**.

   You should see a message like this one:

   Pinging <IP address> with 32 bytes of data

   If the path is working, you see this message:

   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

   If the path is not working, you see this message:

   Request timed out

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections

  – Make sure the Ethernet port LED is on. If the LED is off, follow the troubleshooting instructions "Ethernet Light (LED) Not On" earlier in this section.

– Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) connected to your workstation and router.

- Wrong network configuration

    – Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.

    – Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device. From the Windows run menu, type:

PING -n 10 <IP address>

where *<IP address>* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information will not be visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway.

- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

- Check that your cable or DSL modem is connected and functioning.

- If your ISP assigned a host name to your computer, enter that host name as the User Name in the WAN Interface menu.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized computer. To do this, click on the WAN Interface link under the TCP/IP heading of the browser interface at *192.168.2.254*, and enter the authorized computer's MAC address under "Clone MAC Address".

APPENDIX I: Network

This section provides more detailed explanation of the network operation modes.

The Network Page allows the administrator to set up bridge or routing functionality. Device can operate in bridge or router mode. The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually. Use the Network menu to configure the IP settings.

Network Mode Selections

Network Mode: Specify the operating network mode for the device. The mode depends on the network topology requirements:

- **Bridge** operating mode is selected by default as it is widely used by subscriber stations forconnecting to Access Point or using WDS. In this mode the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation and broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic. Additional Firewall settings can be configured for Layer 2 packet filtering and access control in Bridge mode.

- **Router** operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation – wireless clients will be on a different IP subnet. Router mode will block broadcasts while it is not transparent.

This device supports Multicast packet pass-through in Router mode. The router can act as a DHCP server and use Network Address Translation (Masquerading), which is widely used by Access Points. NAT will act as the firewall between LAN and WLAN networks. Additional Firewall settings can be configured for Layer 3 packet filtering and access control in Router mode.

Bridge Mode

Bridge Mode Network Settings

In bridge mode, the device forwards all network management and data packets from one network interface to the other without any intelligent routing. For simple applications this provides an efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment, which has the same IP address space. WLAN and LAN interfaces form the virtual bridge interface while acting as the bridge ports. The bridge has assigned IP settings for management purposes.

Bridge IP Address

The device can be set for static IP or can be set to obtain an IP address from the connected DHCP server. One of the IP assignment modes must be selected:

- DHCP : choose this option to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.

- STATIC : choose this option to assign the static IP settings for the bridge interface. Enter the IP address of the device. This IP will be used for device management purposes.

IP Address and Netmask settings should correspond with the address space of the network segment where device resides. If the device IP settings and administrator PC IP settings use different address space, the device will become unreachable.

Netmask

When expanded into binary, this value provides a mapping to define which portions of the IP address groups can be classified as host devices and network devices. Netmask defines the address space of the network segment where the device resides. Address 255.255.255.0 (or /24) is commonly used among many C Class IP networks.

Gateway IP

Typically, this is the IP address of the host router that provides the point of connection to the internet. It can be a DSL modem, Cable modem, or a WISP gateway router. The device will direct the packets of data to the gateway if the destination host is not within the local network. THe Gateway IP address should be from same address space (on same network segment) as the device.

Primary/Secondary DNS IP

The Domain Name System (DNS) is an internet "phone book" that translates domain names to IP addresses. These fields identify the server IP addresses of where the device looks for the translation source.

The Primary DNS server IP address should be specified for the device management purposes.

A Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server becomes unresponsive.

Spanning Tree Protocol

Multiple interconnected bridges create larger networks using the IEEE 802.1d Spanning Tree Protocol (STP), which is used for finding the shortest path within a network and to eliminate loops from the topology.

If STP is turned on, the Bridge device will communicate with other network devices by sending and receiving Bridge Protocol Data Units (BPDU). STP should be turned off (selected by default) when the device is the only bridge on the LAN or when there are

no loops in the topology as there is no reason for the bridge to participate in the Spanning Tree Protocol.

Bridge mode Firewall Configuration Settings

Firewall functionality on the bridge interface can be enabled using the "Enable Firewall" option. Bridge Firewall rules can be configured, enabled or disabled while using the Firewall configuration window, which is opened with the "Configure" button.

Firewall entries can be specified by using the following criteria:

- Interface: the interface (WLAN or LAN) where filtering of the incoming/passing-through packets is processed.

- IP Type: sets which particular L3 protocol type (ICMP, TCP, and UDP) should be filtered.

- Source IP/mask: the source IP of the packet (specified within the packet header), usually it is the IP of the host system that sends the packets.

- Source Port: the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application that sends the packets.

- Destination IP/mask: the destination IP of the packet (specified within the packet header), usually it is the IP of the system to which the packet is addressed.

- Destination Port: the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application to which the packet is addressed.

- Comments: the informal field for comments on the particular firewall entry. Typically, a few words about the particular firewall entry purpose are saved there.

- On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in system configuration file, however only the enabled firewall entries are active during the system operation.

New Firewall entries can be saved by clicking **Apply** or discarded by clicking **Cancel** in the Firewall configuration window.

All active firewall entries are stored in the FIREWALL chain of the ebtables filter table, while the device is operating in Bridge mode.

Click **Apply Setting** and **Save Changes** buttons to save the changes made in the Network page.

Appendix II – Wireless with Router Mode

This section provides more details on the wireless with router function.

The role of the LAN and WLAN interface will change accordingly to the Wireless Mode while the device is operating in Router mode: ???

- The wireless interface and all the wireless clients connected are considered as the internal LAN and the Ethernet interface is dedicated for the connection to the external network while the device is operating in AP/AP WDS wireless mode.

- The wireless interface and all the wireless clients connected are considered as the external network and the all the network devices on LAN side as well as the Ethernet interface itself is considered as the internal network while the device is operating in Station/Station WDS mode.

Wireless/wired clients are routed from the internal network to the external one by default. Network Address Translation (NAT) functionality works the same way.

AP-Router Mode Network Settings

IP Address

This IP address represents the LAN or WLAN interface that is connected to the internal network according to the wireless operation mode described above. IP will be used for routing in the internal network (it will be the Gateway IP for all the devices connected on the internal network). IP address will also be used for device management.

WLAN IP Address

This IP addresses represents the LAN or WLAN interface that is connected to the external network according to the wireless operation mode described above. This address can be used for routing and the device management purposes. The external network interface can be set for static IP or can be set to obtain an IP address from the DHCP server, which should reside in the external network. One of the IP assignment modes must be selected for the external network interface:

- **DHCP** – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external DHCP server.

- **PPPoE** – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external PPPoE server.

- **Static** – choose this option to assign static IP settings for the external interface. IP Address and Netmask settings should correspond to the address space of the network segment where the device resides. If the device IP settings and IP settings of the administrator PC (which is connected to the device either wired or wirelessly) use different address space, the device will become unreachable.

Netmask

This is used to define the device IP classification for the chosen IP address range. Address 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

Gateway IP

This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the internet. This can be a DSL modem, cable modem, or a WISP gateway router. The device will direct all the packets to the gateway if the destination host is not within the local network.

Gateway IP address should be from the same address space (on the same network segment) as the device's external network interface (wireless interface in the Station case and LAN interface in the AP case).

Primary/Secondary DNS IP

The Domain Name System (DNS) is an internet "phone book" that translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requests are forwarded by the device.

The primary DNS server IP is mandatory. It is used by the DNS Proxy and for the device management purpose.

A secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

Enable NAT

Network Address Translation (NAT) enables packets to be sent from the wired network (LAN) to the wireless interface IP address and then sub-routed to other client devices residing on its local network while the device is operating in AP/AP WDS wireless mode and in the opposite direction in "Station/Station WDS" mode.

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables NAT table while the device is operating in Router mode. Refer to available iptables information for details of NAT functionality in Router mode. Static routes should be specified in order that the packets pass through the device if NAT is disabled while operating in Router network mode.

Enable DHCP Server

Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients that will associate with the wireless interface while the device is operating in AP/AP WDS wireless mode and assigns IP addresses to clients that will connect to the LAN interface while the device is operating in Station/Station WDS mode.

Range Start/End

This range determines the IP addresses given out by the DHCP server to client devices on the internal network, which use dynamic IP configuration.

Lease Time

The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensures client operation without interruption, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it acquires new IP addresses from the DHCP server.

Port Forwarding Settings

Port Forwarding

Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for applications such as FTP servers, gaming, etc. where different host systems need to be seen using a single common IP address/port. Port forwarding rules can be set in the Port Forwarding window, which is opened by enabling the Port Forwarding option and clicking **Configure**. New entries can be saved by clicking **Save** or discarded by clicking **Cancel** in the Port Forwarding configuration window.

Port Forwarding entries can be specified using the following criteria.

Private IP

The IP of the host that is connected to the internal network and needs to be accessible from the external network.

Private Port

The TCP/UDP port of the application running on the host that is connected to the internal network. The specified port will be accessible from the external network.

Type

The L3 protocol (IP) type, which needs to be forwarded from the internal network.

Public Port

The TCP/UDP port of the based device that will accept and forward the connections from the external network to the host connected to the internal network.

Comments

The informal field for comments on the particular port forwarding entry. Usually a few words about the purpose of the particular port forwarding entry are saved there. Enabled flag enables or disables the effect of the particular port forwarding entry. All the

added firewall entries are saved in system configuration file, however only the enabled port forwarding entries are active during system operation.

DNS Proxy

The DNS Proxy forwards the Domain Name System requests from the hosts that reside in the internal network to the DNS server while device is in operating in Router mode. Valid Primary DNS Server IP needs to be specified for DNS Proxy functionality. Internal network interface IP of the device should be specified as the DNS server in the host configuration in order for the DNS Proxy to be able to get the DNS requests and translate domain names to IP addresses afterwards.

Bridge mode Firewall Configuration Settings

Firewall functionality on any router interface can be enabled using the "Enable Firewall" option. Router Firewall rules can be configured, enabled or disabled while using the Firewall configuration window, which is opened by clicking **Configure**. New entries can be saved by clicking **Apply** and **Save Changes** or discarded by clicking **Cancel** in the Firewall configuration window.

All active firewall entries are stored in the FIREWALL chain of the iptables filter table while the device is operating in Router mode.

Firewall entries can be specified by using the following criteria:

Interface

The interface (WLAN, LAN or PPP) where filtering of the incoming/passing-through packets is processed.

IP Type

Sets which particular L3 protocol type (ICMP, TCP, UDP, P2P) should be filtered.

Source IP/mask

The source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets.

Source Port

The source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application that sends the packets.

Destination IP/mask

The destination IP of the packet (specified within the packet header), usually it is the IP of the system to which the packet is addressed.

Destination Port

The destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application to which the packet is addressed.

Comments

The informal field for comments about the particular firewall entry. Usually a few words about the particular firewall entry purpose are saved there.

On flag

Enables or disables the effect of the particular firewall entry. All added firewall entries are saved in system configuration file, however only the enabled firewall entries are active during device operation.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers.

Select the IP Address option PPPoE to configure a PPPoE tunnel in order to connect to an ISP. Only the external network interface can be configured as a PPPoE client as all the traffic will be sent via this tunnel. The IP address, Default gateway IP and DNS server IP address will be obtained from the PPPoE server after PPPoE connection is established. Broadcast address is used for the PPPoE server discovery and tunnel establishment. Valid authorization credentials are required for the PPPoE connection.

PPPoE Username

Username to connect to the server (must match the configured on the PPPoE server).

Password

Password to connect to the server (must match the configured on the PPPoE server).

PPPoE MTU/MRU

The size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for the data encapsulation while transferring it through the PPP tunnel.

Enable DMZ

The Demilitarized zone (DMZ) can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers, and E-mail Servers so that these services can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with the NAT functionality as an alternative for Port Forwarding that makes all the ports of the host network device visible from the external network side.

DMZ Management Port

If the DMZ Management Port option is enabled, Web Management Port for the based device will be used for the host device (TCP/IP port 80 by default). In this case the device will respond to requests from the external network as if it is the host specified by DMZ IP. It is recommended to leave the Management Port disabled as the device will be inaccessible from the external network if enabled.

DMZ IP

Connected to the internal network host, the DMZ IP address will be accessible from the external network. With a multicast design, applications can send one copy of each packet and address it to the group of computers that are to receive it. This technique addresses packets to a group of receivers rather than to a single receiver. It depends on the network to forward the packets to the hosts that need to receive them. Common Routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however provide multicast traffic pass-through functionality.

Click **Change** to save the changes made in the Network page.

Appendix III- Advanced Settings

This section provides more detailed explanation for advanced setting for routing and wireless settings.

The Advanced options page allows you to manage advanced settings that influence device performance and behavior. The advanced wireless settings are intended for advanced users who have a sufficient knowledge about wireless LAN technology. These settings should not be changed unless you know what effect the changes will have on your device.

Advanced Wireless Setting

The 802.11a/g data rates include 6, 9, 12, 18, 24, 36, 48, 54Mbps.

The 802.11n data rates are the MCS (Modulation Coding Scheme) rates.

- MCS0 to MCS7 are 802.11n rates, which use only 1 Tx/Rx stream.

- MCS8 to MCS15 are 802.11n rates, which use 2 Tx/Rx streams.

The Rate Algorithm has a critical impact on performance in outdoor links as generally lower data rates are more immune to noise while higher rates are less immune, but are capable of higher throughput.

Rate Aggressiveness

Allows user to reduce or increase transmit rate while still remain in Fully Auto Algorithm. There are two scenarios where rate aggressiveness is useful. If the environment is noisy at times, lowering the throughput will ensure better stability. Rate aggressiveness allows the device to reduce the transmit rate, so range or power can be higher. Choose a range of value from -3,-2,-1. Also the environment might be free of interference, but the fully auto algorithm might give low throughput. Increased Rate Aggressiveness will increase transmit rate in this case to get higher throughput. Choose a range of value from +3, +2, +1.

Noise Immunity

Increases the robustness of the device to operate in the presence of noise disturbance, which is usually generated by external 802.11 traffic sources, channel hopping signals and other interference.

RTS Threshold

Determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or "off". The default value is 2347, which means that RTS is disabled.

RTS/CTS (Request to Send / Clear to Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden

terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

System uses Request to Send/Clear to Send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending an RTS frame first while data is sent only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS, which provides clear media for the requesting station to send the data. CTS collision control management has time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

Fragmentation Threshold

Specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or "off". Setting the Fragmentation Threshold too low may result in poor network performance.

The use of fragmentation can increase the reliability of frame transmissions. Because smaller frames are sent, collisions are much less likely to occur. However lower values of the Fragmentation Threshold will result lower throughput as well. Little or no modification of the Fragmentation Threshold value is recommended as the default setting of 2346 is optimum for most wireless networks.

Station Isolation

This option allows packets only to be sent from the external network to the CPE and vice versa (applicable for AP/AP WDS mode only). If Client Isolation is enabled, wireless stations connected to the same AP will not be able to interconnect on both layer 2 (MAC) and layer 3 (IP) level. This is effective for the associated stations and WDS peers also.

Acknowledgement Timeout

This device has an auto-acknowledgement timeout algorithm that dynamically optimizes the frame acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance outdoor links. The user can also enter the value manually.

Distance

Specify the distance value in miles (or kilometers) using the slider or enter the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.

ACK Timeout

Specify the ACK Timeout. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set timeout it re-sends the frame. The performance drops

---

when too many data frames are re-sent, thus if the timeout is set too short or too long, it will result poor connection and throughput performance.

Changing the ACK Timeout value will change the Distance to the appropriate distance value for the ACK Timeout.

Auto

Adjust control and enable the ACK Timeout Self-Configuration feature. If enabled, the ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm described above. It is not recommended to use the Auto Adjust option for long range links if the signal level is low or the high level of interference is present.

If two or more stations are located at considerable distance from the Access Point, the highest ACK Timeout for the farthest station should be set at the AP side. It is not recommended to use the Auto Adjust option for Point-to-Multipoint connections as it will not warrant highest network performance in all the use cases.

Signal Strength LED Settings

LED Thresholds Configuration

The signal strength LEDs on the device can be made to light when received signal levels reach the values defined in the following fields. This allows a technician to easily deploy a CPE without logging into the unit (i.e., for antenna alignment operation).

Signal LED Thresholds specify the marginal value of signal strength (dBm) that will switch on LEDs indicating signal strength:

LED 1 (Red), **LED 2** (Yellow), **LED 3** (Green) and **LED 4** (Green) will switch on when the Signal Strength reaches the value set in the associated entry field.

Configuration example: if the signal strength fluctuates around RSSI 15-30, the LED thresholds can be adjusted to the RSSI values 15, 20, 25, 30.

Appendix IV- Services

This section provides more details on the system management services.

Ping WatchDog

The ping watchdog sets the device to continuously ping a user defined IP address (the internet gateway for example). If it is unable to ping under the user defined constraints, the device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.

Enable Ping Watchdog

Control will enable Ping Watchdog Tool.

IP Address To Ping

Enter the target host IP address to monitor.

Ping Interval

Specify the time interval (in seconds) between sending the ICMP "echo requests".

Startup Delay

Specify the initial time delay (in seconds) from device startup or reboot to starting sending ICMP "echo requests". Minimum value is 60 seconds.

Failure Count To Reboot

Specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. The device contains an SNMP agent that allows it to communicate to SNMP management applications for network provisioning.

SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of

management information between network devices). SNMP Agent allows network administrators to monitor network performance, and find and solve network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

Enable SNMP Agent

Control will enable SNMP Agent.

SNMP Community

Specify the SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access for devices that supports SNMP v1.

Contact

Specify a contact in case an emergency situation should arise.

Location

Specify the physical location of the device.

NTP Client, Web, Telnet, SSH Server

NTP Client

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the device system time. If the Log option is enabled, System Time is reported with every System Log entry while registering system events.

Web Server

The following the device Web Server parameters can be set there:

- **Use Secure Connection (HTTPS):** If enabled, the Web server will use secure HTTPS mode. HTTP mode is selected by default.

- **Secure Server Port**: Web Server TCP/IP port setting while using HTTPS mode.

- **Server Port**: Web Server TCP/IP port setting while using HTTP mode.

Telnet Server

The following Telnet Server parameters can be set:

- **Enable Telnet Server**: Enables Telnet access to the device.

- **Server Port**: Telnet service TCP/IP port setting.

SSH Server

The following SSH Server parameters can be set:

- **Enable SSH Server**: Enables SSH access to the device.
- **Server Port**: SSH service TCP/IP port setting.

System Log

Enable Log

Option enables the registration routine of the system log messages. Enable Remote Log enables the syslog remote sending function while System log messages are sent to a remote server specified by the Remote Log IP Address and Remote Log Port.

Remote Log IP Address

The host IP address where syslog messages should be sent. The remote host should be configured properly to receive syslog protocol messages.

Remote Log Port

The TCP/IP port of the host syslog messages should be sent. Port "514" is the default port for commonly used system message logging utilities.

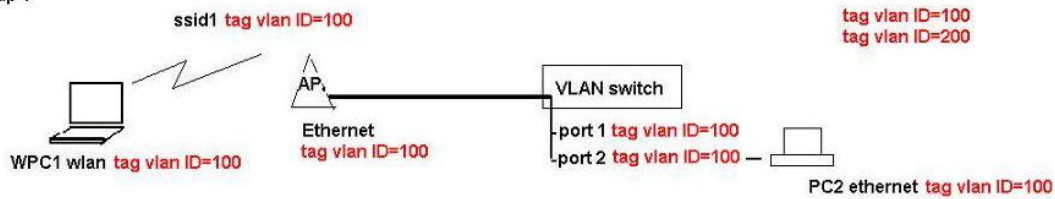Every logged message contains at least a System Time and a Host Name. Usually a particular service name that generates the system event is also specified within the message. Messages from different services have different context and different level of details. Usually error, warning or informational system services messages are reported. The more detailed the reported system messages, the greater volume of log messages generated.
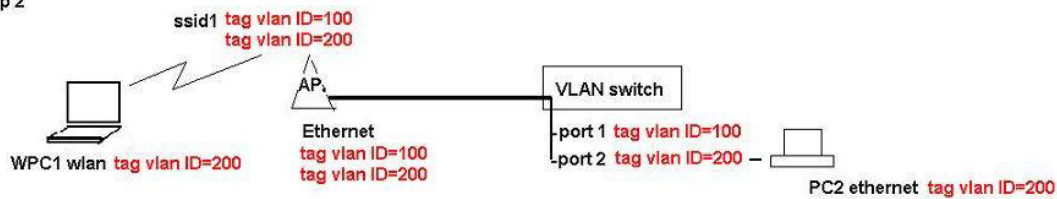
Appendix V- VLAN Setup examples

Tagged Wireless VLAN to Tagged Ethernet VLAN Setup
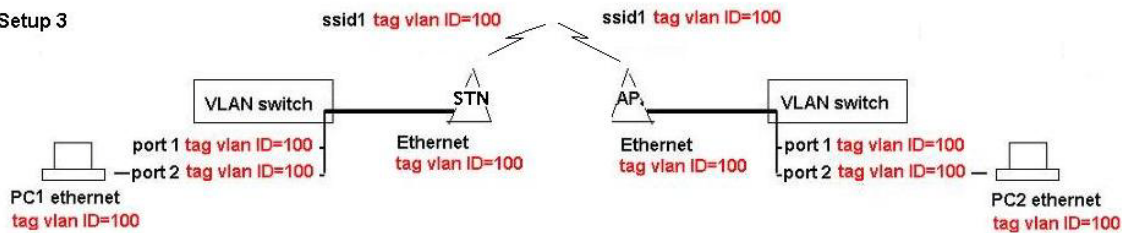

Tag vlan connection Setup

Setup 1

ssid1 tag vlan ID=100

tag vlan ID=100
tag vlan ID=200

AP

VLAN switch

Ethernet
tag vlan ID=100

WPC1 wlan tag vlan ID=100

port 1 tag vlan ID=100
port 2 tag vlan ID=100

PC2 ethernet tag vlan ID=100

Setup 2

ssid1 tag vlan ID=100
tag vlan ID=200

AP

VLAN switch

Ethernet
tag vlan ID=100
tag vlan ID=200

WPC1 wlan tag vlan ID=200

port 1 tag vlan ID=100
port 2 tag vlan ID=200

PC2 ethernet tag vlan ID=200

Hints:-

For each vlan id group to send between AP and wireless clients,
AP wlan and ethernet interface must add that vlan group.
AP ethernet port connecting to the switch must set to the default vlan id same as switch port its connecting.

Setup 3

ssid1 tag vlan ID=100   ssid1 tag vlan ID=100

VLAN switch   STN   AP   VLAN switch

port 1 tag vlan ID=100
port 2 tag vlan ID=100

Ethernet
tag vlan ID=100

Ethernet
tag vlan ID=100

port 1 tag vlan ID=100
port 2 tag vlan ID=100

PC1 ethernet
tag vlan ID=100

PC2 ethernet
tag vlan ID=100

Untagged Wireless VLAN to Tagged Ethernet VLAN setup

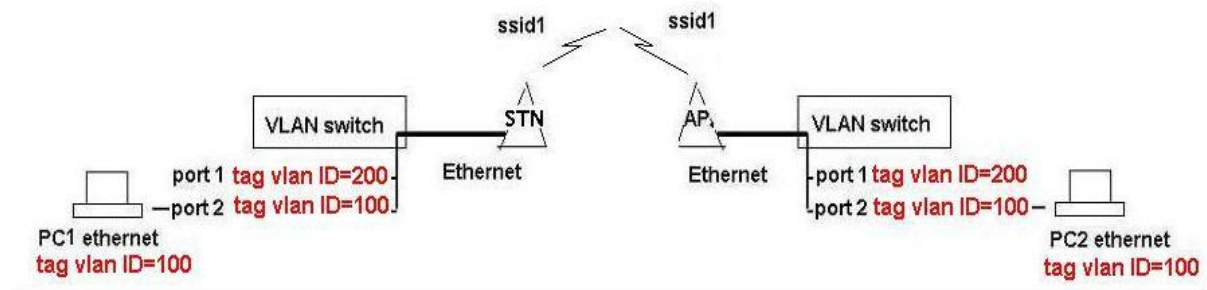Multi-SSID with untag vlan connections to secured wired tag vlan network connections
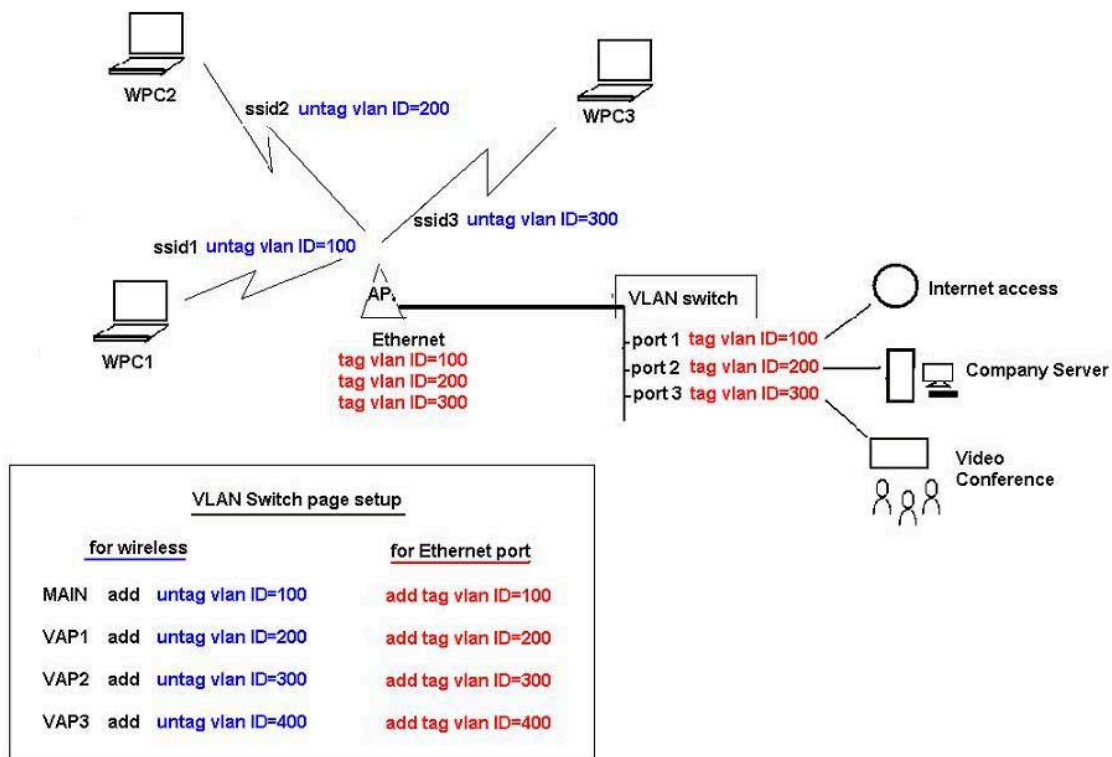
Tagged VLAN Pass-Through

Tagged VLAN pass-through. AP and Station link no VLAN Setup Required

＊ - AP and Station devices no VLAN setting required

Compliance Information

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

FCC Compliance Statement:
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. This device must accept any interference received, including interference that may cause undesired operation. Product that is a radio transmitter is labeled with FCC ID.
FCC Caution*:*
(1) Exposure to Radio Frequency Radiation. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.
(2) Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.
(3) This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
(4) Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.
(5) Outdoor Operations in the 5.15~5.25GHz band is prohibited.

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.
WARNING: This AP does not support ad-hoc mode Function

FCC ID: V6U-AP25N01

Corporate Office USA	Regional Office South America
Air802 LLC	Air802 Ltda.
Suite 105	2102 Av. Fermin Vivaceta
424 Fort Hill Drive	Independencia
Naperville, IL 60565 USA	Santiago, Chile
Tel: (630) 428-3108	Tel: 562.455.0975
Fax: (630) 637-8662	Fax: 562.455.0976
Email: sales@air802.com	Email: ventas@air802.com