APX-5200

Industrial IP67 Outdoor Gigabit IEEE802.11b/g/n Wireless

AP/Client/Bridge/Repeater

User Manual

Version 1.0

www.antaira.com

Trademark Information

Antaira is a registered trademark of Antaira Technologies, LLC, Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. NetWare is the registered trademark of Novell Inc. WMM and WPA are the registered trademarks of Wi-Fi Alliance. All other brand and product names are trademarks or registered trademarks of their respective owners.

Disclaimer

Antaira Technologies, LLC provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Antaira Technologies, LLC may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Antaira Technologies, LLC will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

FCC NOTICE

This device 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 device 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 device does cause harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

RF Exposure Warning

The equipment complies with FCC RF exposure limits set forth for an uncontrolled environment.
The equipment must not be co-located or operating in conjunction with any other antenna or transmitter.

ICES 003 Statement
This Class B digital apparatus complies with Canadian ICES-003.

Declaration of Conformity

Antaira declares the following:

Product Type: Wireless Access Point
Model No.: APX-5200 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 conformity to the following European Norms (in brackets are the equivalent international standards.)

Electromagnetic Interference (Conduction and Radiation): EN 55022 (CISPR 22)
Electromagnetic Immunity: EN 55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11)
Low Voltage Directive: EN 60 950: 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.

Antaira 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 301 489-17)**

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.

Industrial Wireless

Gigabit AP/Client/Bridge/Repeater

User Manual
Version 1.0 July 2014

This manual supports the following model:

- APX-5200

This document is the current official release manual. Please check our website (www.antaira.com) for any updated manual or contact us by e-mail (support@antaira.com).

Table of Contents

1. Overview

Antaira Technologies' APX-5200 series is a waterproof IP67 rated industrial gigabit wireless network Access Point (AP). This managed wireless device has two gigabit Ethernet ports and two MIMO antennas for enhanced throughput. The APX-5200 series utilizes an Atheros chipset and boasts network robustness, stability and wider network coverage. This series of wireless products is capable of operating as an access point, client, bridge or repeater and also includes some routing capabilities making it suitable for a wide array of wireless applications.

The outdoor unit can be protected by utilizing the grounding plane that is conveniently located within the mounting bracket. The APX-5200 series receives power though the Ethernet port and is a PoE Powered Device (PD) that conforms to the IEEE802.3af standard. This series of outdoor wireless products has an operating temperature of -20 to 70°C.

To protect your security and privacy, the access point is armed with the latest wireless security features such as IEEE 802.11i standards, MAC address filtering, IEEE 802.1x authentication and WEP/WPA/WPA2 encryption to ensure privacy for the heterogeneous mix of users within the same wireless network. The unit also incorporates a unique set of advanced features such as virtual AP to deliver multiple services and long-range parameter fine-tuning which provides the access point with the ability to auto-calculate parameters like slot time, ACK time-out and CTS time-out to achieve a longer range.

1.1 Features and Benefits

Point-to-Point & Point-to-Multipoint Support

Point-to-point and point-to-multipoint communication between different buildings enable users to bridge wireless clients that are kilometers apart while unifying the networks.

Virtual AP (Multiple SSID)

Virtual AP implements multi-SSID (mSSID) allowing a single wireless system to be set up with multiple virtual AP connections with different SSIDs or Basic Service Set Identifiers (BSSID) and different security settings.

Highly Secured Wireless Network

The access point supports the highest available wireless security standard which is IEEE802.11i compliant. The access point also supports IEEE 802.1x for a secure and centralized user-based authentication. Wireless clients are thus required to authenticate through highly secure methods like EAP-TTLS and EAP-PEAP, in order to obtain access to the network.

uConfig Utility

The uConfig utility allows users to access the user-friendly web configuration interface of the access point without having to change the TCP/IP setup of the workstation.

HTTPS

The access point supports HTTPS (SSL) in addition to the standard HTTP.
HTTPS (SSL) features additional authentication and encryption for secure communication.

Telnet

Telnet allows a computer to remotely connect to the access point Command Line Interface (CLI) for control and monitoring.

SSH

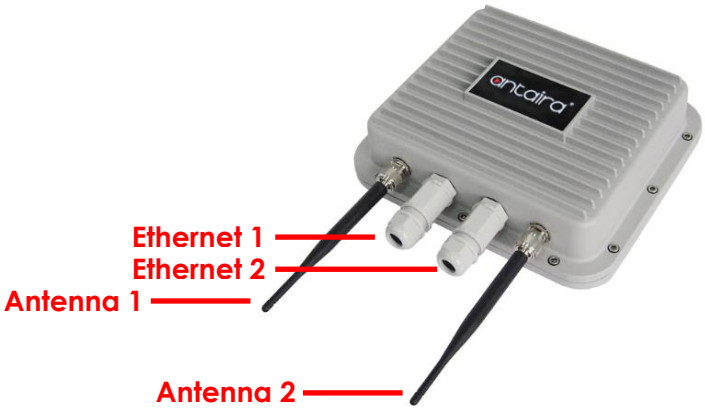
Secure Shell Host (SSH) establishes a secure host connection to the access point's CLI for control and monitoring.

2. Hardware Description

2.1 Hardware Connections

The following table describes the connectors on the APX-5200.

Port	Description
10/100/1000 RJ-45 Gigabit Ethernet Ports	2*10/100/1000 Base-T(X) RJ-45 Gigabit Ethernet port supports IEEE 802.3af PoE (powered device) Default Speed: Auto
ANT (1/2)	N-type connector for external antenna

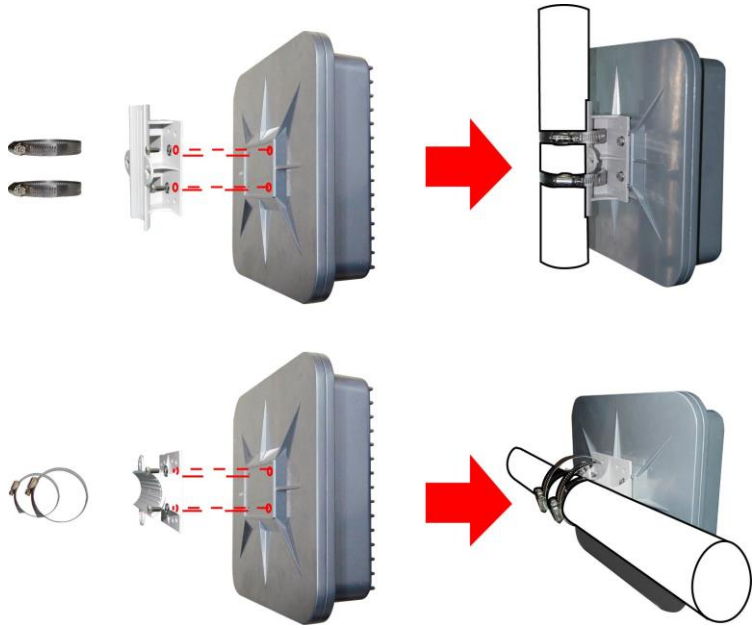


Front Panel of the APX-5200

2.2 Mounting Installation

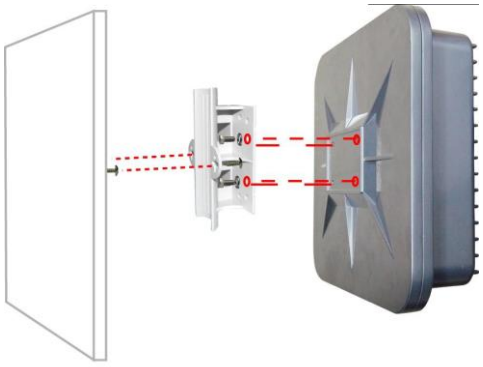
2.2.1 Pole Mounting

Each AP has a pole mounting kit on the rear panel. The pole mounting kit helps to fix the AP in the appropriate location.



2.2.2 Wall Mount Installation

Each AP has another installation method to fix the AP. A wall mount panel can be found in the package. The following step shows how to mount the AP on a wall.



2.3 Cables and Antennas

2.3.1 Ethernet Cables

The APX-5200 WLAN AP has a PoE Ethernet port. According to the link type, the AP use CAT 3, 4, 5,5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm	UTP 100 m (328 ft)	RJ-45
1000Base-TX	Cat. 5, 5e, 6 100-ohm	UTP 100 m (328 ft)	RJ-45

10BaseT/100/1000BaseTX Pin Assignments

The APX-5200 supports auto MDI/MDI-X operation. You can use a straight-through cable to connect PC and AP. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

MDI/MDI-X Pin Assignments

Note: *"+" and "-" signs represent the polarity of the wires that make up each wire pair.*

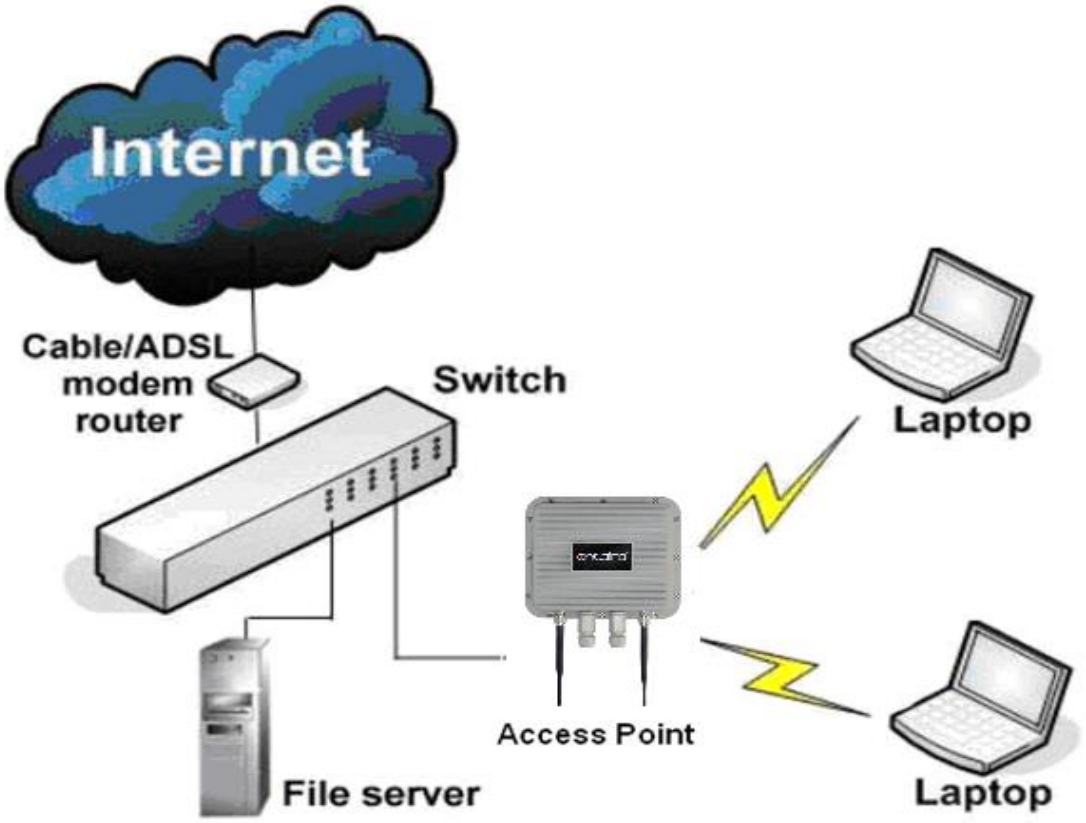
2.3.2 Wireless Antenna

2.4GHz Multiple-Input and Multiple-Output (MIMO) antennas are used for the APX-5200 and are connected using N-type connectors. External antennas can also be used with this type of connector.

3. Operation Modes and Connection Examples

3.1 Access Point and Access Point WDS Mode

The access point mode is the default mode for the device. It enables the bridging of wireless clients to wired network infrastructures and enables transparent access and communication with each other. The illustration below shows a typical application when resources are sharing the same AP. The wireless users are able to access the file server connected to the switch, through the access point in AP mode.

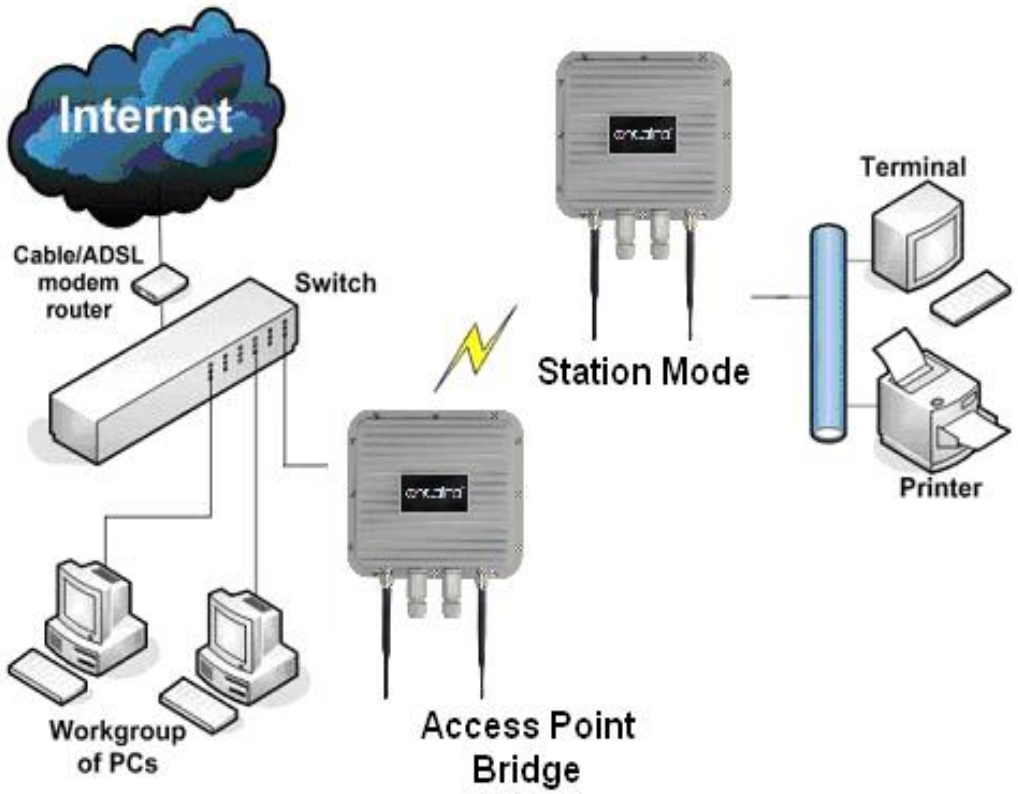


This mode is generally used for point-to-point or point-to-multi-point connections, and is mainly used with station WDS to build the point and multi-point connections.

3.2 Station Mode

In station mode, the device acts as a wireless client. When connected to an access point, it creates a network link between the Ethernet network connected at the client device and the wireless Ethernet network connected at the access point.

In the example below, the workgroup of PCs on the Ethernet network are connected to the station device, which can access the printer across the wireless connection to the access point where the printer is connected.

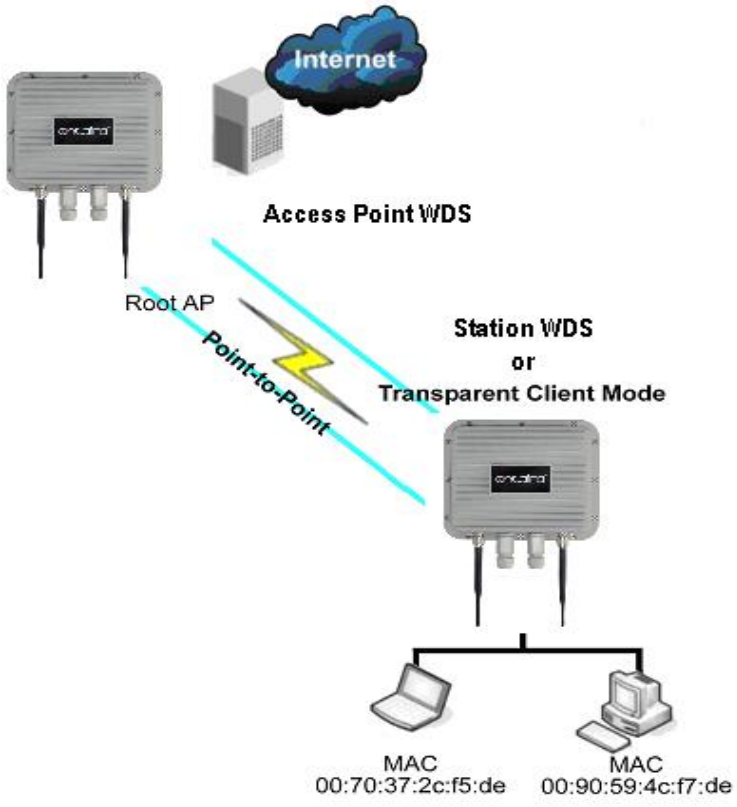


3.3 Station WDS Mode

Station WDS mode is similar to Station mode. The difference is that Station WDS mode must be connected to an AP that is configured in Access Point WDS (or RootAP) mode.
Station WDS is mainly used for a point-to–point connection between two buildings or locations that are further away.

Point-to-Point	Point-to-Multi-Point
An access point setup as Access Point WDS (or RootAP) and the other as Station WDS (Transparent Client).	An access point setup as Access Point WDS (or RootAP) and several other devices as Station WDS (or Transparent Client).

This mode is generally used for outdoor connections over long distances, or for indoor connections between local networks.



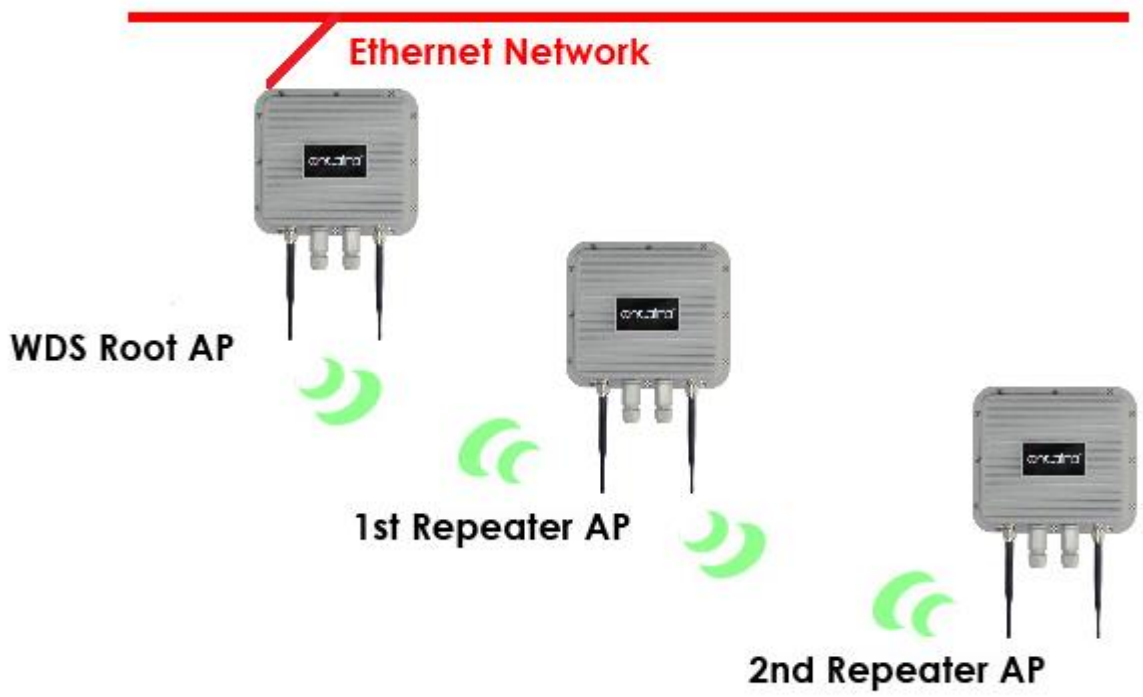
3.4 Repeater WDS Mode

Repeater WDS Mode is mainly used to extend the wireless range and coverage of the wireless network allowing access and communication to go over places which are generally difficult for wireless clients to connect to a network.

In repeater mode, the AP acts as a relay for network signals on the network by regenerating the signals it receives, and retransmitting them to the main network infrastructure.

*Detailed information on the repeater mode is available in the 'Repeater Setup' section.

**** Note:** ***Repeater WDS requires the AP to be setup in RootAP or Access Point WDS mode in order to work.***



4. Configure the IP Address

After setting up the hardware, the user needs to assign an IP address to the PC so that it is in the same subnet as the access point.

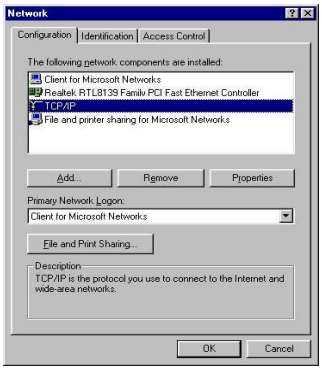
4.1 For Windows 95/98/98SE/ME/NT

Step 1:

From your desktop, right-click the **Network Neighborhood** icon and select **Properties**.

Step 2:

Select the network adapter that you are using, then right-click and select **Properties**.

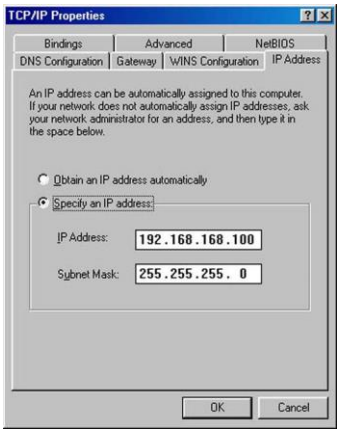


Step 3:

Highlight **TCP/IP** and click on the **Properties** button.

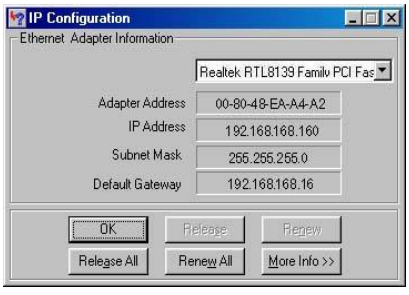
Step 4:

Select the **Specify an IP address** radio button.
Set the IP address to 192.168.168.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 254.



Step 5:

To verify that the IP address has been correctly assigned to your PC, go to the **Start** menu, select **Run**, and enter the command: *winipcfg*.



Select the Ethernet adapter from the drop-down list and click **OK**.

The PC is now setup with a proper IP address to communicate with the access point.

4.2 For Windows XP/2000

Step 1:

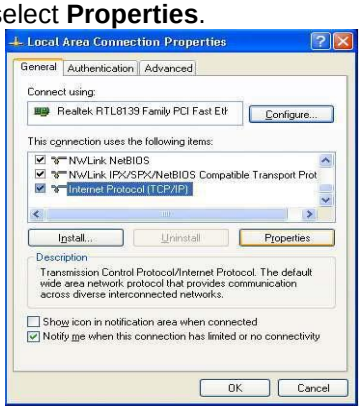
Go to your desktop, right-click on the **My Network Places** icon and select **Properties**.

Step 2:

Right-click the network adapter icon and select **Properties.**

Step 3:

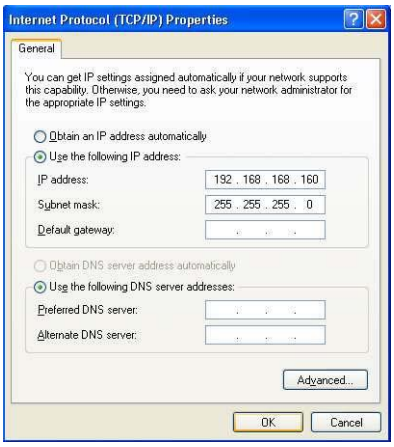
Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.



Step 4:

Select the **Use the following IP address** radio button.

Set the IP address to 192.168.168.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 254.

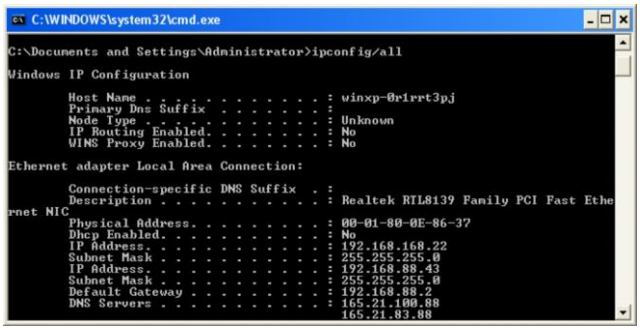


Step 5:

Click on the **OK** button to close all windows.

Step 6:

To verify that the IP address has been correctly assigned to your PC, go to the **Start** menu, **Accessories**, select **Command Prompt**, and type the command: *ipconfig/all*



PC is now setup with a proper IP address to communicate with the access point.

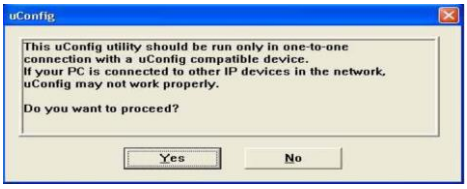
5. Access the Web Interface

5.1 Access with uConfig

The uConfig utility provides direct access to the web interface.

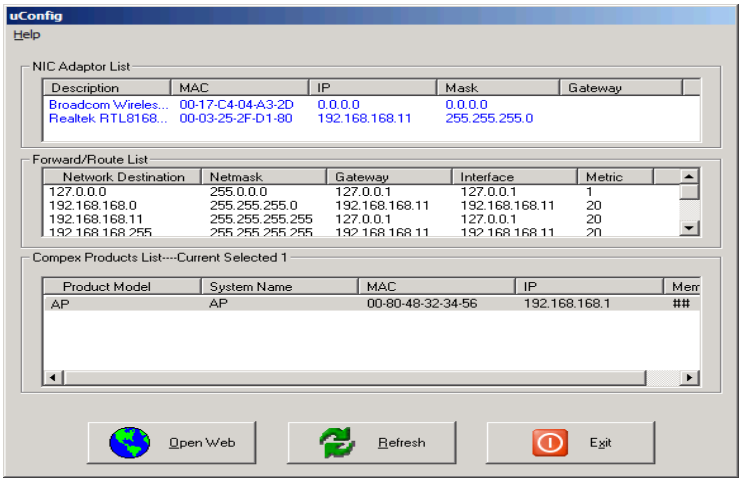
Step 1:

Click **uConfig** icon to launch the utility then click **Yes** button.



Step 2:

Select the access point from the products list and click on the **Open Web** button. To retrieve and display the latest device(s) in the list, click on the **Refresh** button.



Step 3:

Do not exit the uConfig program while accessing the web-based interface as this will disconnect you from the device. Click on the **OK** button.

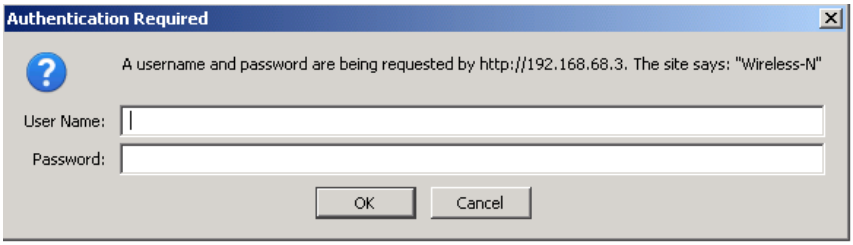
Step 4:

At the login prompt, enter the User Name and Password.

The default are :

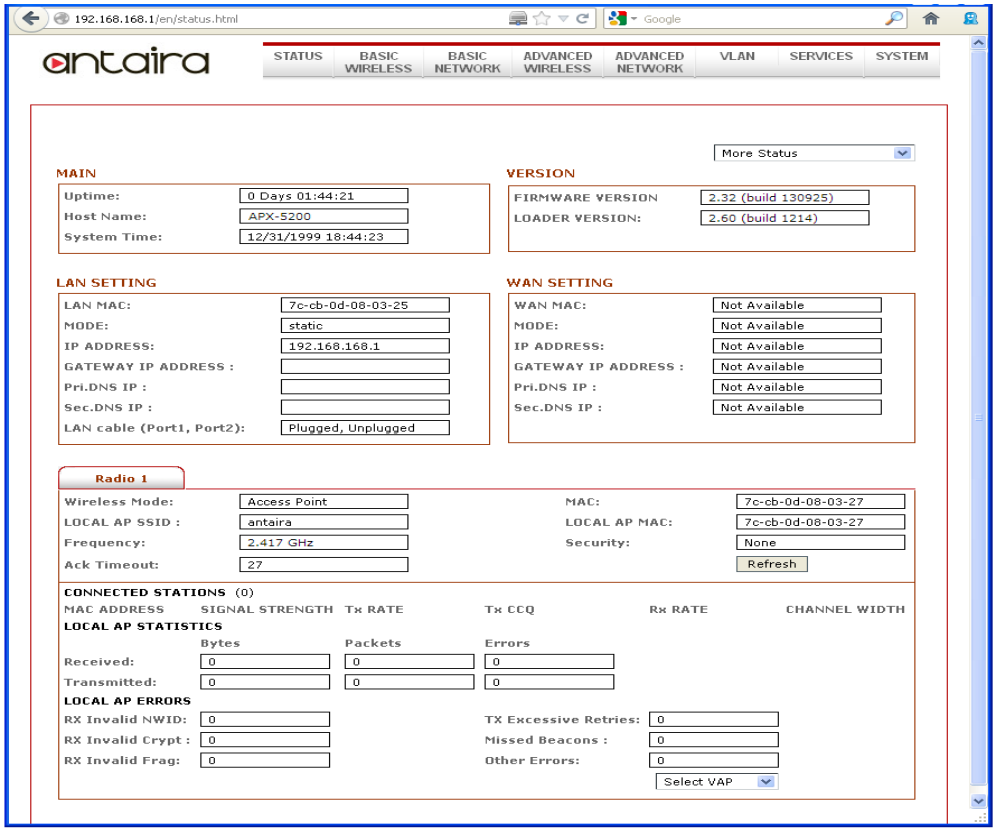
User Name : **admin**

Password : **password**



Step 5:

It then opens the device's home page - the 'Status' page.



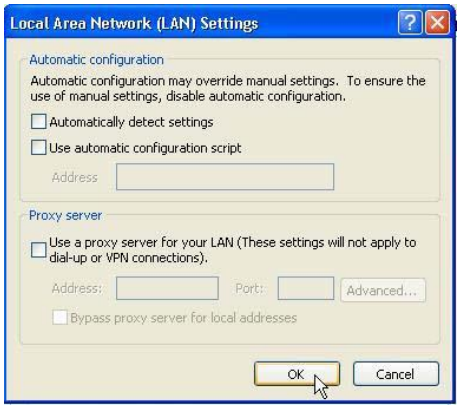
6. Access with Web Browser

Step 1:

Launch your web browser, e.g. Internet Explorer, FireFox, Netscape, etc.
If using MS IE, under the **Tools** tab, select **Internet Options.**

Step 2:

Open the **Connections** tab and in the **LAN Settings** section disable all the option boxes. Click on the **OK** button to update the changes.



Step 3:

At the **Address** bar type in http://192.168.168.1 and press **Enter** on your keyboard.

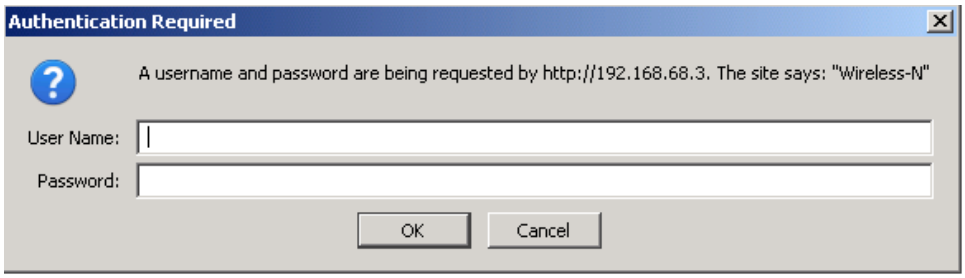
Step 4:

At the login prompt, enter the User Name and Password.

The default are :

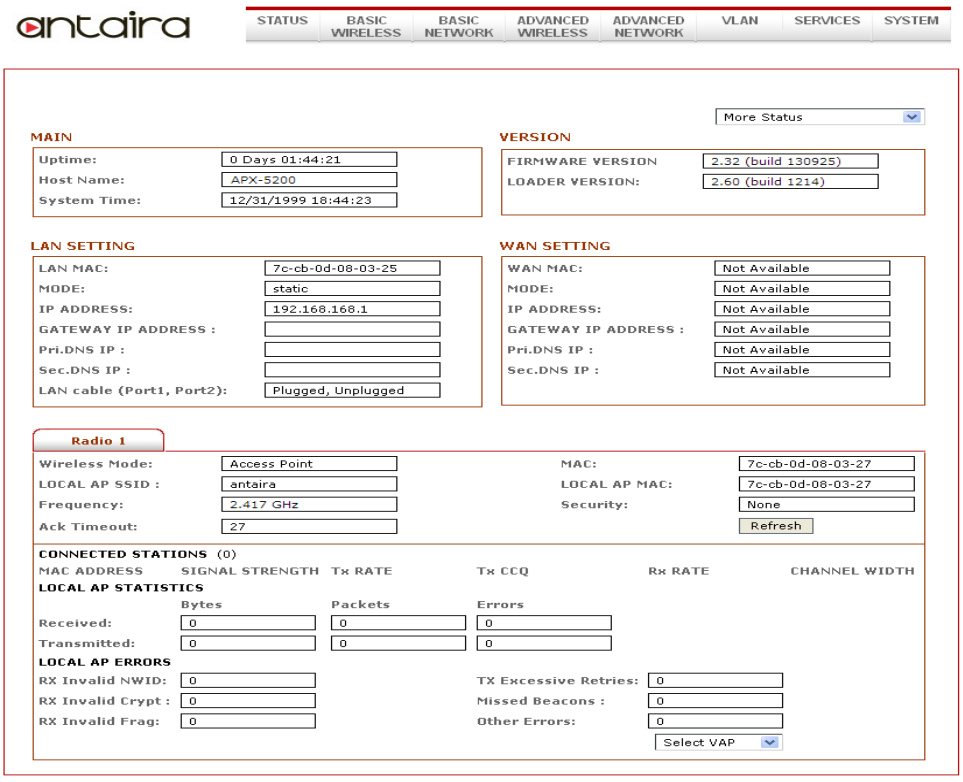
User Name : admin

Password : password



Step 5:

It then opens the device's home page - the 'Status' page.



7. Navigation

Main Menu Bar

Status: Page displays current status of the device and the statistical information.

Basic Wireless: Page contains the controls for a wireless network configuration, while covering basic wireless settings which define operating mode, associating details and data security options.

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

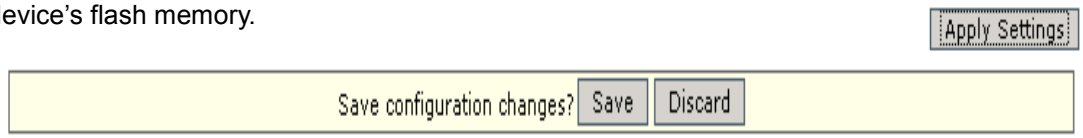
Advanced Wireless: Page settings are intended for advanced wireless features. See 'Advanced Network' page settings for more details.

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

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

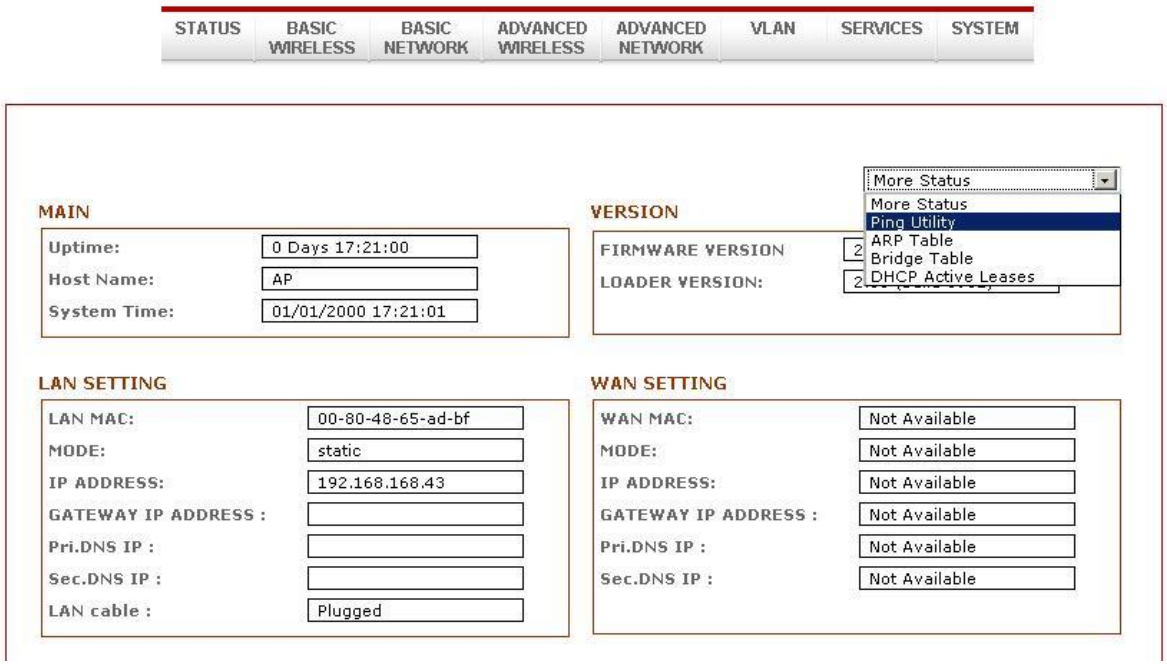
How to Save Changes

After changes have been made from each respective setup page, click this button, and the prompt below will appear. The user will then be asked to confirm if changes want to be permanently saved to the device's flash memory.



- Clicking **Save** will write all configuration changes to the device's flash memory.
- Clicking **Discard** will discard all changes made.
- If unsure about any changes made earlier, it is recommend to discard and reconfigure again.

7.1 Status Page



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

7.1.1 Status Reporting

Main

- **Uptime:** Displays the device's up time since boot up. The time is expressed in days, hours, minutes and seconds.
- **Host Name:** Displays the assigned device's host name (ID).
- **System Time:** Displays the device's current date and time. An accurate system date and time is retrieved from the internet services using Network Time Protocol (NTP) only if the device is setup and connected to the internet, otherwise, the date and time update will be from the device's inaccurate autonomous clock.
- **Version Firmware Version:** Displays current firmware version in operation.
- **Loader Version:** Displays current loader version of the device.

LAN Setting

- **LAN MAC:** Displays the MAC address of the device's LAN (Ethernet) interface.
- **LAN Mode:** Displays the mode used, either static or DHCP client.
- **LAN IP Address:** Displays the current IP address of the LAN (Ethernet) interface.
- **LAN Gateway IP Address:** Displays the IP address of the gateway used in LAN.
- **LAN Pri. DNS IP:** Displays the primary DNS IP address of the LAN setting.
- **LAN Sec. DNS IP:** Displays the secondary DNS IP address of the LAN setting.

WAN Setting

- **WAN MAC:** Displays the MAC address of the device's WAN interface.
- **WAN Mode:** Displays the mode used, either DHCP, PPPoE or Static IP.
- **WAN IP Address:** Displays the current IP address of the WAN interface.
- **WAN Gateway IP Address:** Displays the IP address of the gateway used in WAN.
- **WAN Pri. DNS IP:** Displays the primary DNS IP address of the WAN setting.
- **WAN Sec. DNS IP:** Displays the secondary DNS IP address of the WAN setting.

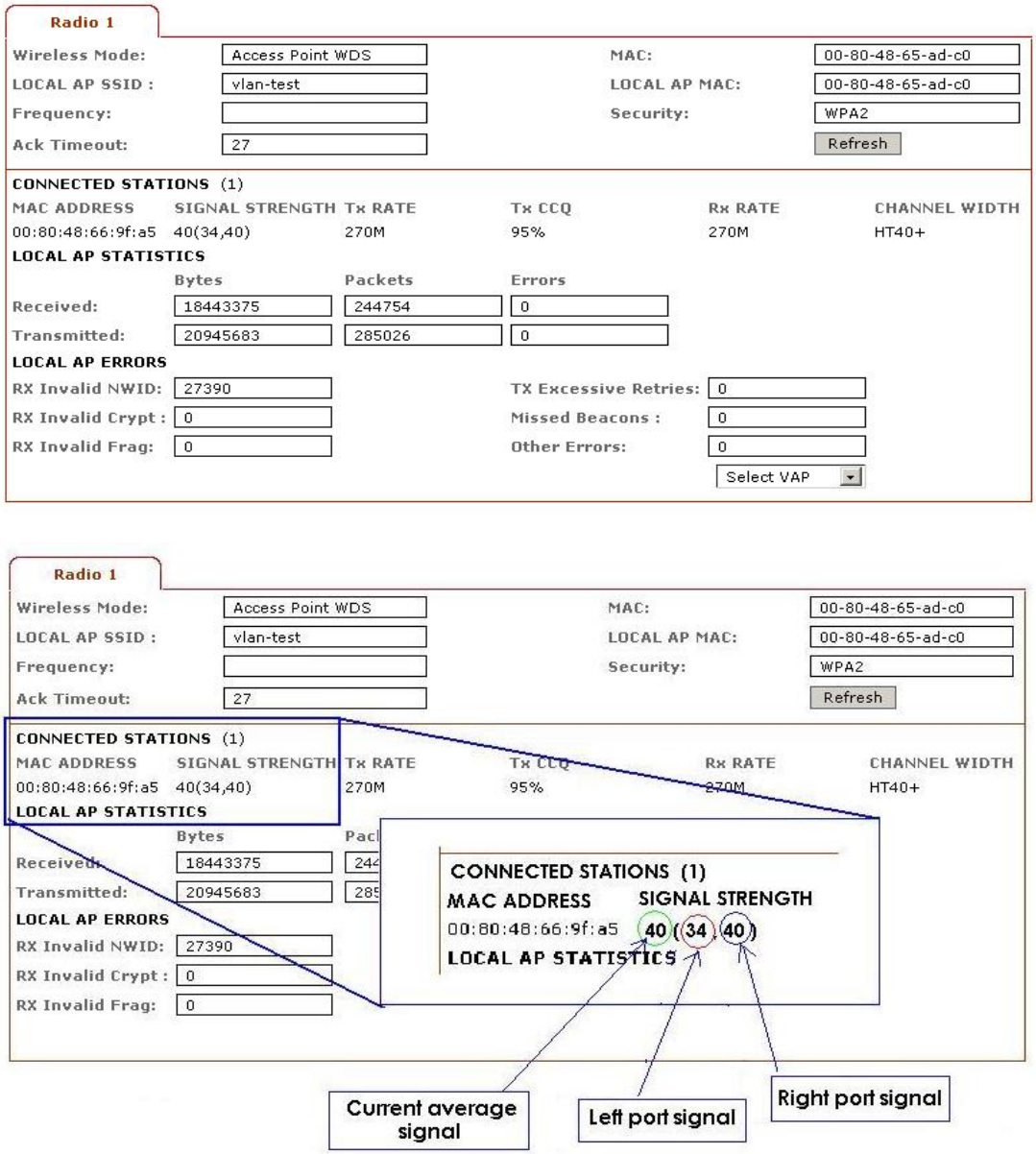
Radio

- **Wireless Mode:** Displays the current operating mode of the device.
- **Local AP SSID:** Displays the current Service Set Identifier (SSID) of the device when it operates in access point mode.
- **Frequency:** Displays current operating frequency running in the device.
- **WLAN MAC:** Displays the MAC address or BSSID of the current active WLAN card running in the device.
- **WLAN Local/Remote AP MAC:** Displays the MAC address of the WLAN card connected to it.
- **WLAN Security:** Displays the current active security mode.

7.1.2 Clients Connection Status in AP Status Info

All clients connected to the AP can be viewed from the AP Status page.
The following images are an example of a client's connection status info.

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

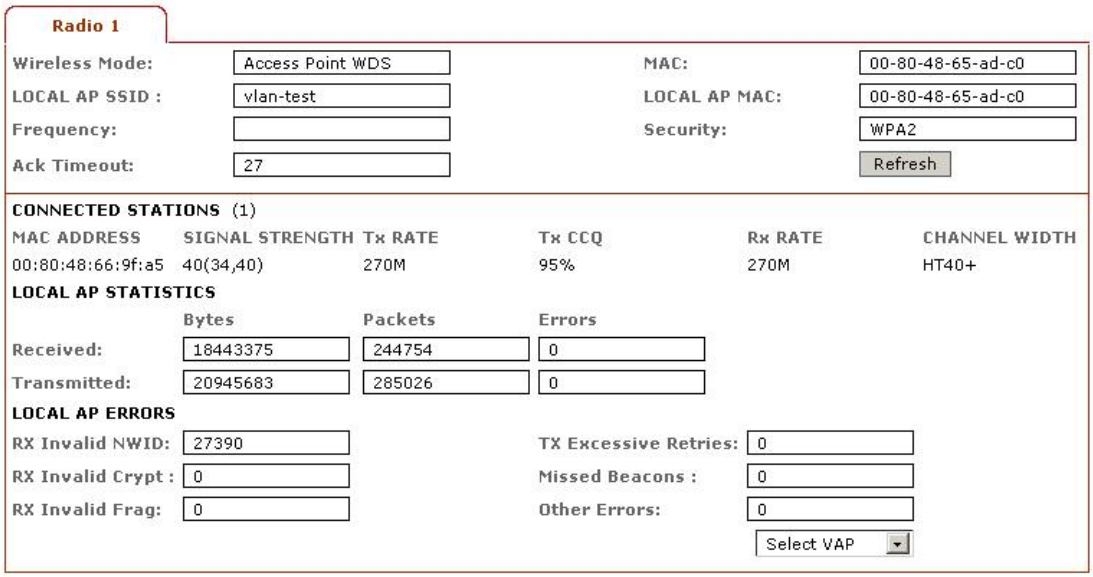


The signal strength at the left and right port of the radio card can be viewed more accurately when the antenna is adjusted which will help to acquire a more balanced reception.

7.1.3 Station Connection Info

Status Info

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



WLAN Connected Status:

- **MAC Address:** Displays the MAC address of the current and active WLAN card.
- **Signal Strength:** Displays the received wireless signal level of the opposite connected device.
- **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 will be.
- **Channel Width:** HT20 indicates established connection is 20MHz channel width.
    - **HT40+ indicates established connection is 40MHz channel width**

WLAN Local AP Statistics: Bytes transmitted/received value represents the total amount of data (in bytes) transmitted and received during connection.

WLAN Local AP Errors: This section displays the counters of 802.11 specific errors which were registered on the wireless interface.

- **Rx invalid NWID** value represents the number of packets received with a different NWID or ESSID - packets which 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 which

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.

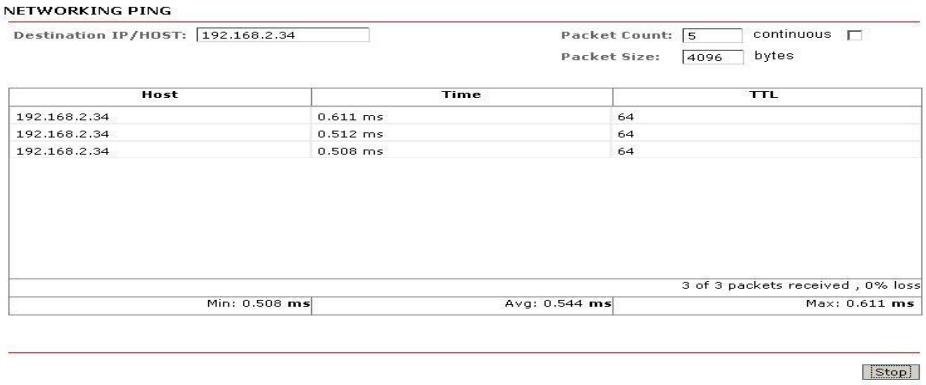
- **Rx Invalid Frag** value represents the number of packets missed during transmission and reception. These packets were dropped due to re-assembling failure as some link layer fragments of the packet were lost.
- **Tx Excessive Retries** value represents the number of packets which failed to be delivered to the destination. Undelivered packet are retransmitted a number of times before an error occurs.
- **Missed Beacons** value represents the number of beacons (management packets sent at regular intervals by the access point) which were missed by the client. This can indicate that the wireless client is out of range.

Other error values represent the total number of transmitted and received packets that were lost or discarded for other reasons.

7.1.4 More Status

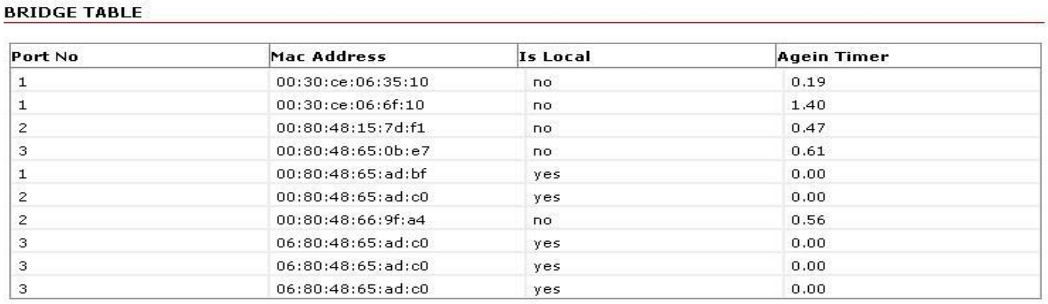
The ‘More Status’ option contains useful tools specifically for the status pages.

Ping Utility – Use the ping tool to test the connectivity between devices.



ARP Table displays a list of MAC addresses of the connected devices.

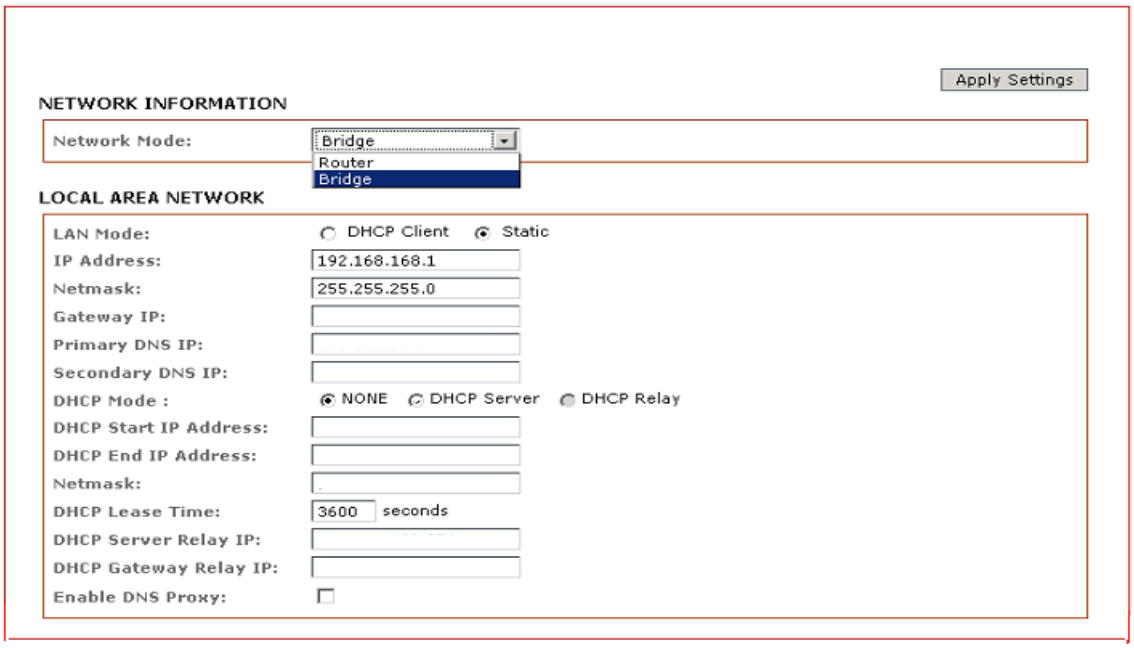
Bridge Table displays a list of devices connected to a bridge interface.



DHCP Active Lease Table displays a list of IP addresses leased to all computers.

7.2 Basic Network Tab

Click **BASIC NETWORK** from the menu bar to open the page shown below.



Network Mode: Bridging and Routing

Network Mode:

Select between bridge (default) and router mode.

7.2.1 LAN Setup

LAN Mode:

- **Static:** (Default) This allows the user to enter a specific IP address for the device.
  - Default IP address is 192.168.168.1
- **DHCP Client:** When setup, this allows the device to learn the IP address automatically from the network.
- **Netmask:** Allows the user to set the class for the IP address set.
  - Default class C and value is 255.255.255.0
- **Gateway:** (Optional) Enter the gateway IP address of the network for the connected device.
- **Primary DNS IP**: (Optional) Enter the primary DNS IP address nearest the gateway router.
- **Secondary DNS IP:** (Optional) Enter the secondary DNS IP address nearest the gateway router.

DHCP Mode:

- **None:** Function disabled.
- **DHCP Server:** Check the box to enable the option. The device will then act as the IP address distribution server and will automatically issue an IP address and other network information to the DHCP client that has requested it.
- **DHCP Relay:** Check the box to enable the option. Then, 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, which will be issued.

DHCP End IP Address: Enter the last IP address the server will issue.

Netmask: Allows the user to set the IP class for the IP address range set for the start and end address.

**** Note:** If the device is also the router then the IP class must be the same as the device IP class.*

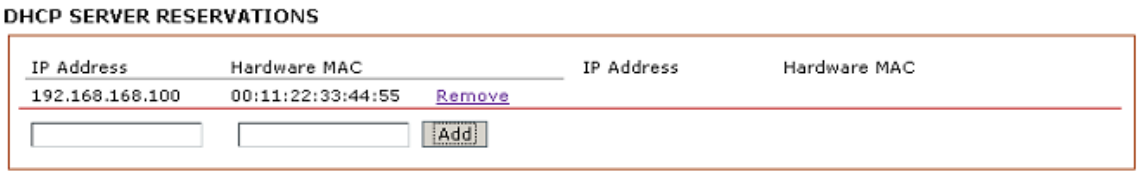
DHCP Lease Time: Enter the new lease time in seconds (default is **3600** seconds or 1 hour).

DHCP Server Relay IP: Enter the IP address of the remote DHCP server where the DHCP client request will be relayed to get the IP address.

DHCP Gateway Relay 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: Check the box to enable this function. Then, the device router operation will act as a proxy to resolve all DNS requests.

DHCP Reservations



Click **Add** to enter each device's IP address and MAC address that will be used. All DHCP active lease devices are displayed in the **Status** tab page from the **More Status** selection.

Domain Name Server Entry

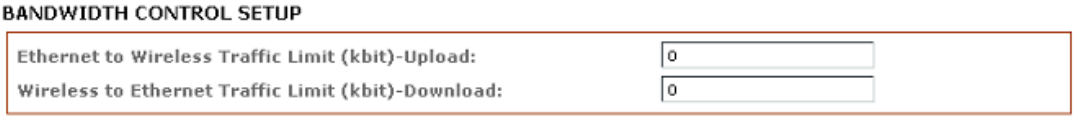
The primary and secondary DNS IP address entry is for the device's operation to resolve the domain name. It is used to reach certain servers like the internet time server among other services that use the domain name.

* ***Note:*** *Ensure the device's gateway IP is also set to allow devices to access the internet.*

Primary DNS IP: (Optional) Enter the primary DNS IP address nearest the gateway router.

Secondary DNS IP: (Optional) Enter the secondary DNS IP address nearest the gateway router.

Bandwidth Control Between Ethernet and Wireless



- An entry value of "0" means there is no bandwidth flow, which limits communication between the two interfaces.
- An entry value of "2000" means there is 2000Kbit or 2Mbit, limiting traffic flow between the two interfaces.
- Default is "0".

7.3 Basic Wireless Tab

Select **RADIO 1** to configure.
The 'Basic Wireless Tab' contains all the wireless setup, which is necessary for the operator to setup the wireless part of the link.

Enable the Radio

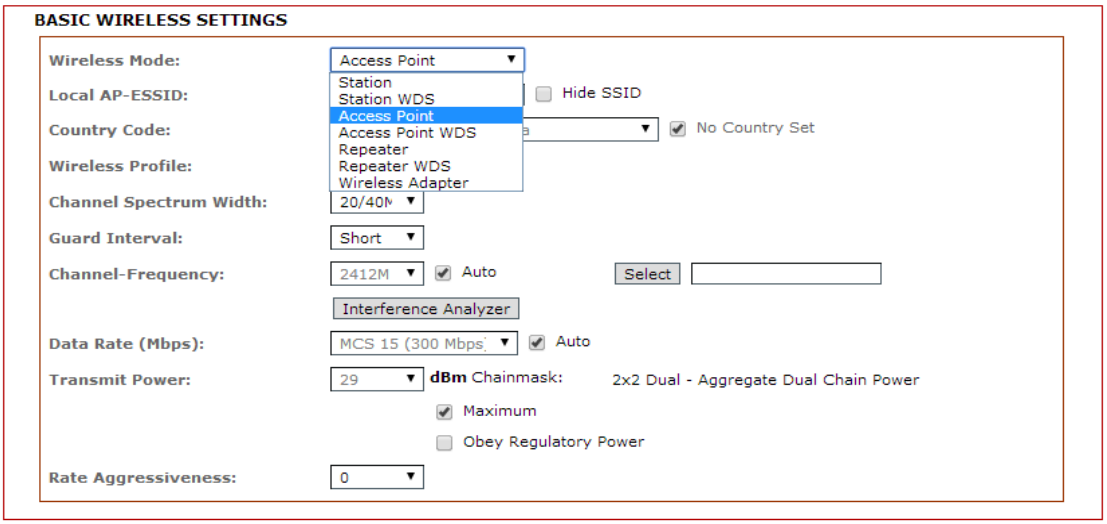
(Click or un-click the box to enable or disable the radio)

Basic Wireless Settings

All the basic wireless settings can be configured using the information on 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.

7.3.1 Wireless Mode

There are **5 modes** available.



1. **Access Point:** This mode can be connected to the **station** mode, which then forwards all the traffic to the network devices connected to the Ethernet devices of the station.

2. **Access Point WDS:** WDS is the acronym for Wireless Distribution System. This mode can be connected to **station WDS** mode. Using WDS protocol, it allows a client or station device to bridge wireless traffic transparently.

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

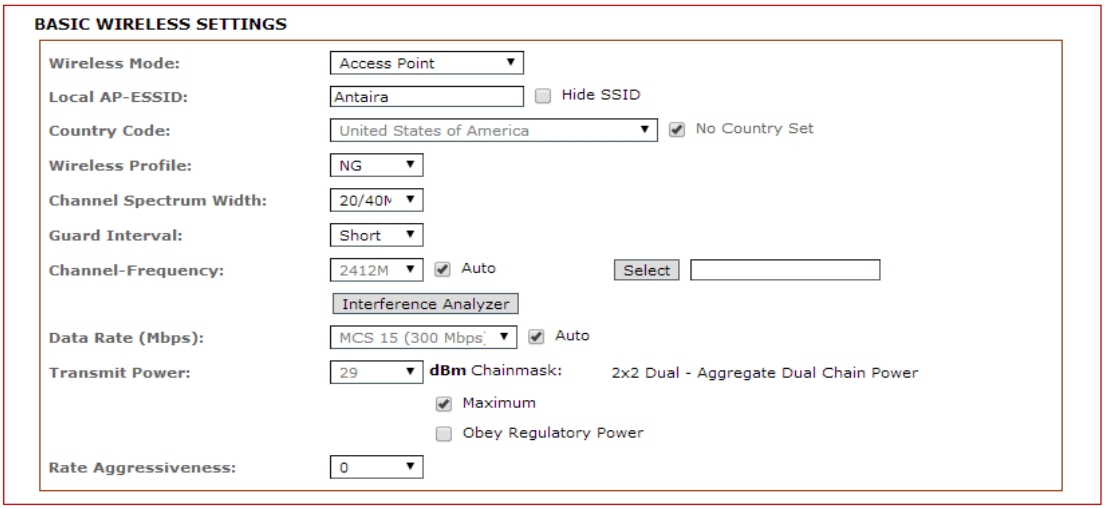
4. **Station WDS:** It can be connected to the **Access Point WDS** mode. It enables packet forwarding at the layer 2 level. Unlike station mode, it is fully transparent at layer 2 level.

Note: For Station WDS, Access Point WDS, Repeater WDS:
WDS protocol used is not defined as the standard, thus compatibility issues between equipment from different vendors might arise.

5. **Repeater WDS:** This mode consists of a station WDS and an access point WDS mode. The repeater WDS must first link up with an access point WDS, and then it can link up with a station WDS. It acts as an extension to the link and can add more repeater WDS modes as necessary.

Note: For Repeater WDS:
The Extended Service Set Identification (ESSID) must be the same for the remote AP and the local AP. The channels that used the repeater to link to another repeater will follow the access point WDS connection that the channel selected.

7.3.2 Access Point Parameter Settings



Basic Wireless Settings (Access Point/ Access Point WDS)

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 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 levels and frequency selections. To ensure the device's operation follows regulatory compliance rules, the operator must select the correct country code where the device will be used. The channel list, output power limits, IEEE 802.11 and channel-spectrum width modes will be tuned accordingly to the regulations of the selected country.

- **No Country Set*:*** Option when checked; only the frequency range is available.
  11n 2.4GHz is 2412-2462MHz.

Wireless Profile: The **NG** is 11n 2.4GHz band and represents a mix of 802.11**n**, 802.11**g** and 802.11b mode.

Channel Spectrum Width

The 20M represents the data transmitted at a bandwidth of 20MHz. 20/40MHz and represents the data transmitted at either 20MHz or 40MHz. In a noisy environment, it automatically falls back to 20MHz, in order to be more resilient to the interference. If auto fall back does not happen, manually change the channel spectrum width to 20MHz, and this will help reduce interference on the link and improve performance.

**** Note: The 40MHz bandwidth is non-standard for 802.11n/g in operation mode. If you experience unstable performance, change the channel spectrum width to 20M.***

Channel – Frequency

This is the frequency selection the user can set the device to operate on. The frequency range available depends on the country domain the user selected in 'Country Code'. Selecting one of these frequencies for operation may have an effect on the device and can delay for two or more minutes(possibly up to 10 minutes in some situations) when attempting to establish a connection.

- **Auto*:*** When checked, during startup, the device automatically selects the least interfering channels (or frequency) for the operation.

Data Rate

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

- Legacy rates are 6 – 54Mbps
- MCS0 to MCS7 are 802.11n rates, which use only one stream.

- MCS8 to MCS15 are 802.11n rates, which use two streams.
- **Auto*:*** The data rate selected will follow an advanced rate algorithm that takes the amount of errors at the data rate and fine tunes it to the best data rate it can use.

Transmit Power

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

Note on Changing Channels:

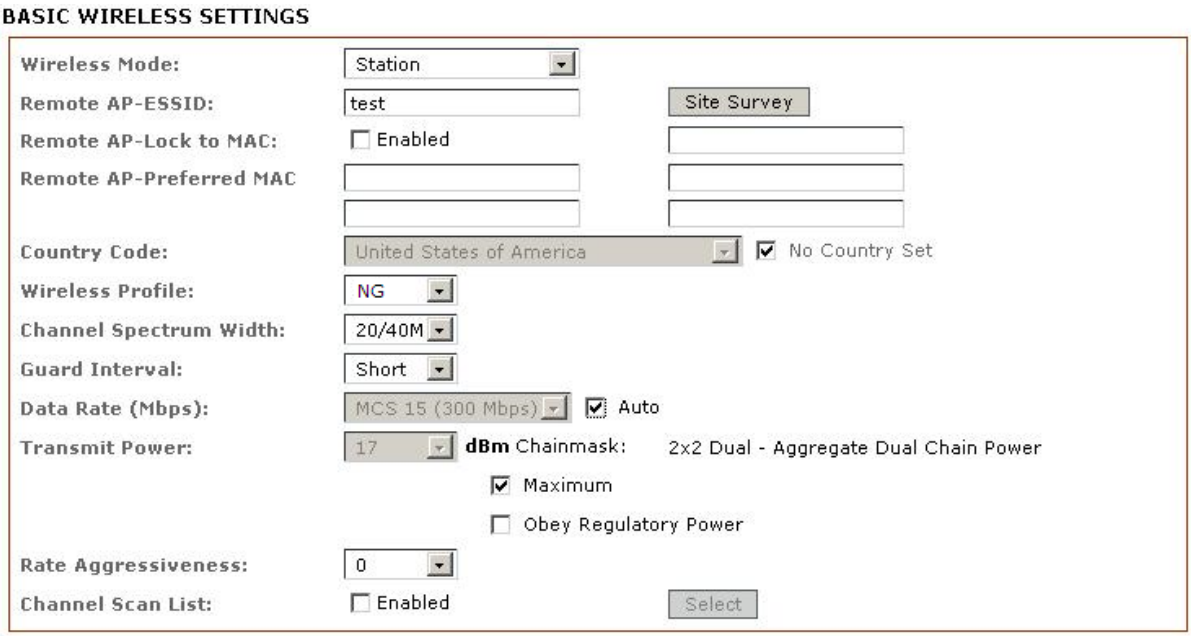
When the operator changes the channels, and the new frequency has a higher output power permitted by regulation, then the previously selected power level (low) will remain unchanged. The user then needs to readjust the power level in order to take advantage of the higher power output available for the channel.

Rate Aggressiveness

This allows users to reduce or increase the transmit rate while still remaining in full auto algorithm. There are two scenarios when rate aggressiveness is useful. First, the environment might be noisy at times, so one would lower the throughput to ensure better stability, and the rate aggressiveness allows the device to reduce the transmit rate, so the range or power can be higher.

Secondly, if one chooses a range of value from -3, -2, -1, then the environment might be free of interference, but the fully auto algorithm might give low throughput. Therefore, on must increase the rate aggressiveness to increase the transmit rate in this case to receive a higher throughput. For this, one would want to choose a range of value from +3, +2, +1.

7.3.3 Station Parameter Settings



Basic Wireless Settings (Station/Station WDS)

These options below are only available in **Station, Station WDS** and **Repeater WDS** mode unless otherwise stated. The **wireless mode** is referred to as Station mode.

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
This will search for the available wireless networks in range on all the supported channels and will allow the user to select one for association. In case the selected network uses encryption, the user will need to set security parameters in the wireless security section. Click 'Scan' to re-scan the access points in range. Select the access point from the list and click 'Close This Window'. The site survey channel scan list can be modified using the channel scan control list.

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

Remote AP - Preferred MAC
Enter the preferred MAC address of the access point the user of the devices wants to connect when it initially is started up. A maximum of four MAC addresses can be entered. Priority is from top to bottom. In the event all preferred MAC addresses are not available, the device will then pick the matching SSID access point with the strongest signal.

Country Code
Different countries have different power levels and frequency selections. To ensure the device's operation follows regulatory compliance rules, the operator should select the country code where the device will be used. The channel list, output power limits, IEEE 802.11 and channel spectrum width modes will be tuned accordingly to the regulations of the selected country. **The station setting must match the AP's country code setting.**

- **No Set Country*:*** Option when enabled, only the frequency range is available. 11n 2.4GHz is 2412-2462MHz.

Wireless Profile: The **NG** is 11n 2.4GHz band and represents a mixed of 802.11**n**, 802.11**g** and 802.11b mode.

** **Station setting must match the AP Wireless Profile setting.**

Channel Spectrum Width
The 20M represents the data transmitted at a bandwidth of 20MHz and the 20/40MHz represents the data transmitted at either 20MHz or 40MHz. In a noisy environment, it automatically reverts back to 20MHz in order to be more resilient to the interference. In a situation when auto fall back does not

happen, manually change the channel spectrum width to 20MHz in order to help reduce interference on the link and improve performance.

**** Note: The 40MHz bandwidth is not the standard for the 802.11n/g mode of operation. If you experience unstable performance, change the channel spectrum width to 20M.***

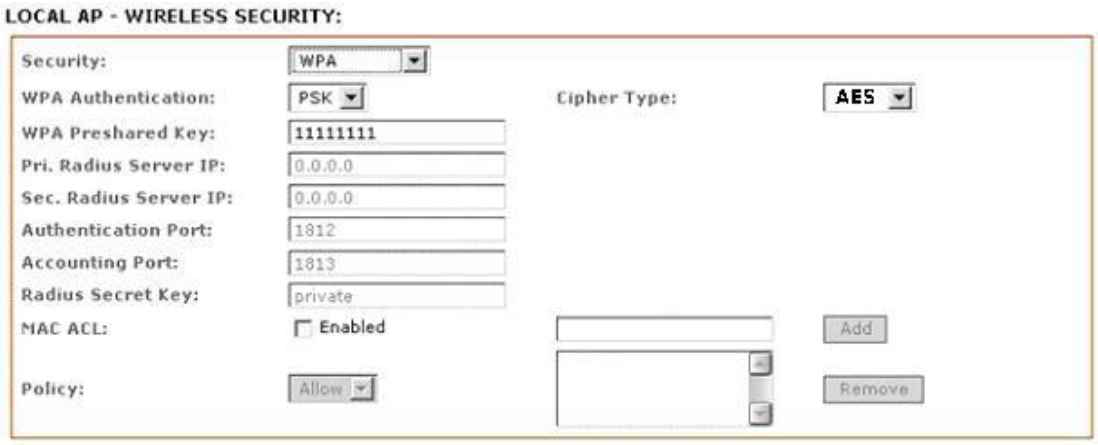
*** **Station setting must match AP channel spectrum width setting.***

- **Maximum:** Checking this box will result in a maximum Tx power output overriding the regulation.
- **Obey Regulatory Power:** Checking this box will obey with the Tx power output by country.

7.3.4 Wireless Security

All the wireless security settings are featured in this section. The operations of the keys are the same for ALL the wireless modes.

WPA or WPA2 Authentication



WPA (Access Point/Access Point WDS/Repeater WDS)

WPA PSK: PSK (Default) – WPA or WPA2 with a pre-shared key method.

Cipher Type

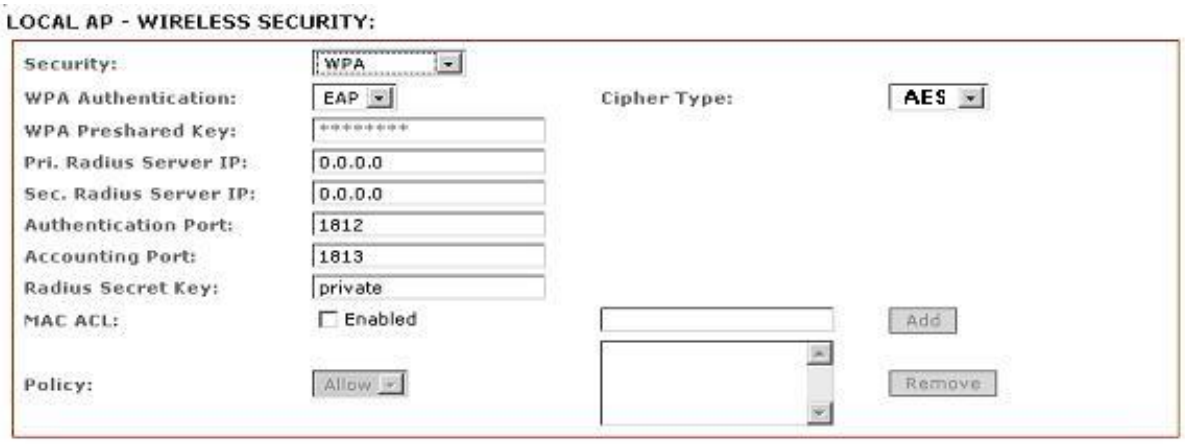
- **TKIP** - Temporal Key Integrity Protocol (TKIP) which uses an RC4 encryption algorithm.
- **AES** - Advanced Encryption Standard (AES) algorithm.
- **AUTO (Default)** – Automatically selects between both algorithms.

Pre-Shared Key: This option is available when **WPA** or **WPA2** is selected in addition to the selection of **PSK**. The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

***** Important:**

- **An 802.11n network using WPA authentication should use the AES cipher type for connection. Only AES allows for the highest transmission speed and throughput during operation.**
- **Using the TKIP cipher type device will limit the maximum transmission speed of up to only 54Mbps.**

WPA + EAP



WPA + EAP

EAP – WPA or WPA2 with Extensible Authentication Protocol (EAP).
Supported firmware options for clients are: EAP-TTLS and EAP-PEAP.

Cipher Type

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

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. The default is 1812.

Accounting Port: Enter the accounting port number of the radius server. The default is 1813.

Radius Secret Key: Enter the secret key of the radius server. The device uses this to authenticate itself with the radius server.

WPA EAP-TTLS and WPA EAP-PEAP

WPA (Station /Station WDS/Repeater WDS)

This only applies to the modes when **WPA** or **WPA2** is selected with **EAP**.

Station, Station WDS, Repeater WDS Mode

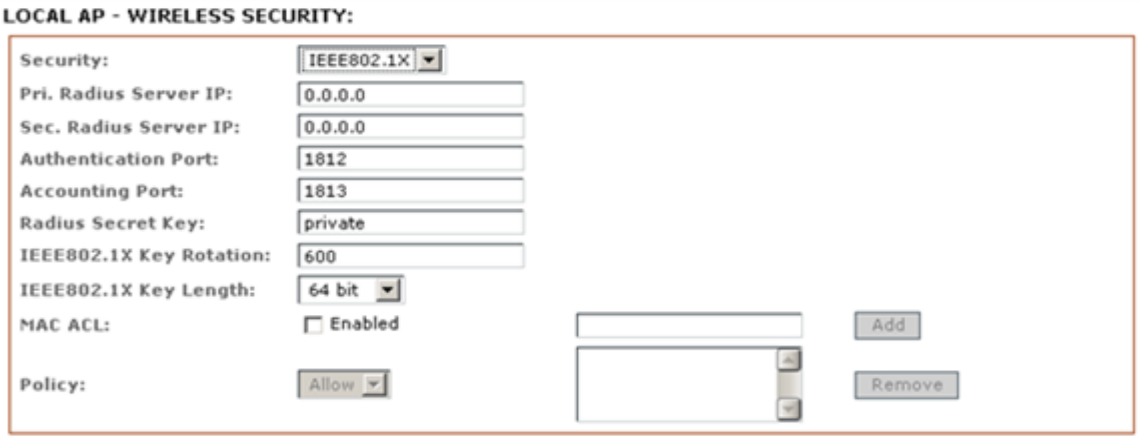
Identity: Identification credential used by the WPA-supplicant for EAP authentication.

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

User Password: The password credential used by the WPA-supplicant for the EAP authentication.

IEEE802.1x Settings: The operations of the keys are the same for ALL the modes.

***** Note: Operating with IEEE802.1x security will limit the AP to a maximum wireless link speed of only 54Mbps.***



IEEE802.1X (Access Point/Access Point WDS/ Repeater WDS

This option only applies when either WPA EAP or IEEE802.1x is selected.

Access Point, Access Point WDS, Repeater WDS Modes

Primary Radius Server IP: Enter the primary radius server IP that the access point will use to query the server.

Secondary Radius Server IP: Enter the secondary radius server IP that the access point will use to query the server.

Authentication Port: Enter the port number to be used in the radius server authentication. The default is 1812.

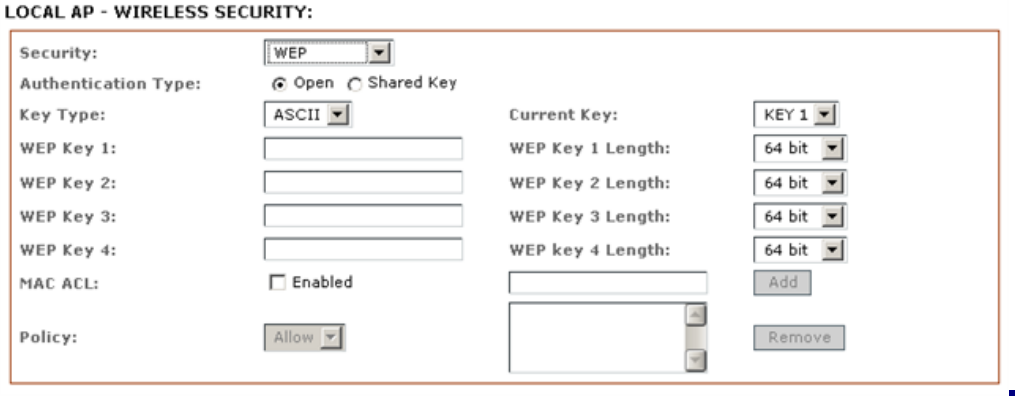
Accounting Port: Enter the radius server accounting port that will be used. The default is 1813.

Radius Secret Key: Enter the radius server secret key that the access point will use to authenticate itself with the radius server.

IEEE802.1x Key Rotation: For higher security, enter the time in seconds it takes before the key rotation is activated in the authentication process.

IEEE802.1x Key Length: This is the key length of the initial seed key. Select 64 or 128bit.

WEP



WEP

The operations of the keys are the same for ALL the modes.

***** Note: Operating with WEP security will limit the AP to the maximum wireless link speed of only 54Mbps.***

Authentication Type:

- **Open Authentication** – (Default) No authentication. It is recommend to use this standard option over the shared authentication.
- **Shared Authentication** – May not be compatible with all the access points, and it is not recommended.

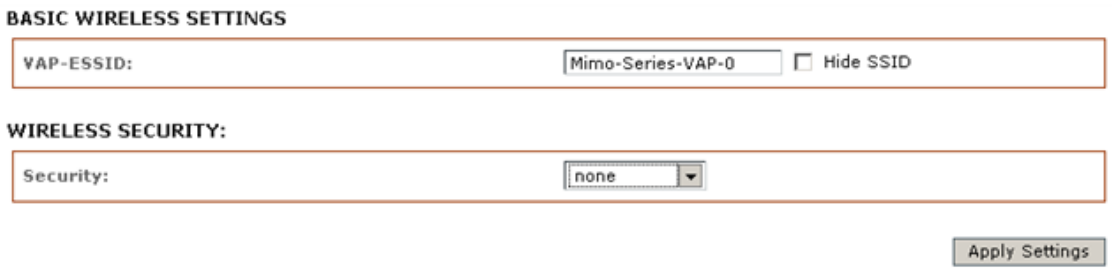
Key Type:

HEX or **ASCII** option specifies the character format for the WEP key if WEP security method is used.

- **Current Key:** Specify the index of the WEP key used. Four different WEP keys can be configured at the same time, but only one is used.
- **WEP Key:** The WEP encryption key for the wireless traffic encryption and decryption should be specified if the WEP security method is used.
- **WEP Key Length:**
  - 64-bit (selected by default) or 128-bit WEP key length should be selected if the WEP security method is used. The 128-bit option will provide a higher level of security.
  - For **64-bi**t – specify the WEP key as 5 HEX (0-9, A-F or a-f) pairs (e.g. 00112233AA) or 5 ASCII characters.
  - For **128-bit** – specify the WEP key as 13 HEX (0-9, A-F or a-f) pairs (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

7.3.5 Virtual Access Point (VAP)

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



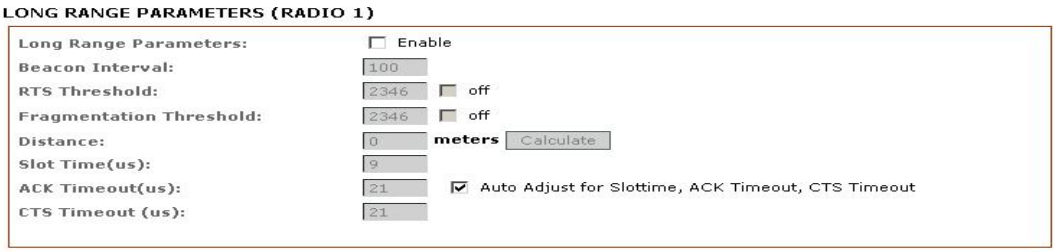
Virtual AP (Only Available in Access Point/ Access Point WDS Mode)

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

***** Note: Security options like IEEE802.1x and WPA-EAP use the radius server for authentication and accounting modes. The user may not use a different secret key for each VAP, otherwise the user should configure only for one SSID with radius authentication.***

7.4 Advance Wireless Tab

Click the **Advanced Wireless** tab from the menu and select **RADIO 1** to open the page below.



Long Range Parameters Setup

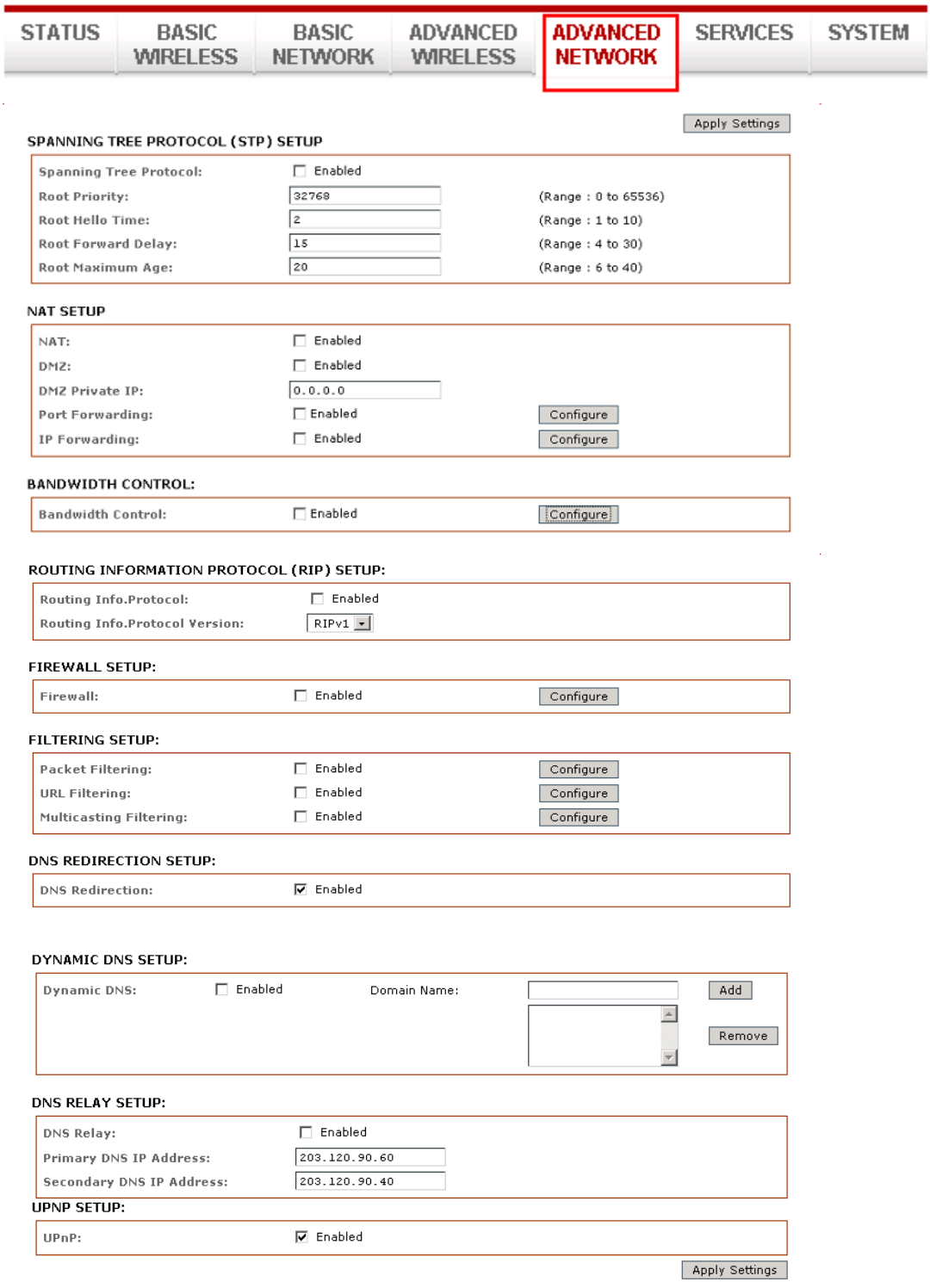
The advanced wireless page will allow the user to setup outdoor long distance connection parameters.

- **Long Range Parameters:** Check to enable parameters.
- **Beacon Interval:** (Default is 100 ms) Define the timing interval (milliseconds) of the beacon to broadcast. It is recommended using the default setting.
- **RTS Threshold:** (Default is **OFF**)
- **Fragmentation Threshold:** (Default is **OFF**)
- **Distance:** Enter the distance (meters) for the device that is connecting to the opposite device, and then click **Calculate.** The close approximate values for slot time, ACK timeout, and CTS timeout will automatically be calculated. When fine tuning it should be taken into consideration for environmental conditions which can help to achieve the best performance and better link reliability.
- **Noise Immunity:** Check the box to enable this setting. When enabled, it automatically adjusts the signal/noise level for the best performance. In low noise environments, it is recommended to turn off this function.
- **Station Isolation:** When enabled, this can help prevent wireless clients on the same AP from discovering other clients.
- **Chainmask Selection:** Available selections are: a) **1x1 Left Chain**, b) **1x1 right Chain** and c) **2x2 Dual Chain.**
    - Selecting **1x1 Left Chain** will force the radio card to operate with 1 transmit and 1 receive stream and both transmit /receive on only the left port of the radio card.
    - Selecting **1x1 Right Chain** will force the radio card to operate with 1 transmit and 1 receive stream and both transmit /receive on only the right port of the radio card.
    - Selecting **2x2 Dual Chain** (default) will enable the radio card to operate with 2 transmit and 2 receive streams and will automatically transmit /receive on any of the 2 radio card ports.

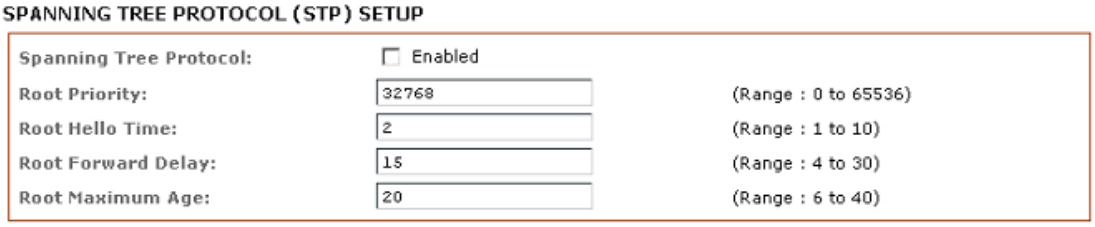
7.5 Advanced Network Tab

Click the **Advanced Network** tab from the menu to open the page below.

***Note:** This tab will not open when the device is in bridge mode.*
To open the page, first enable the router mode in the basic network.



7.5.1 Spanning Tree Setup

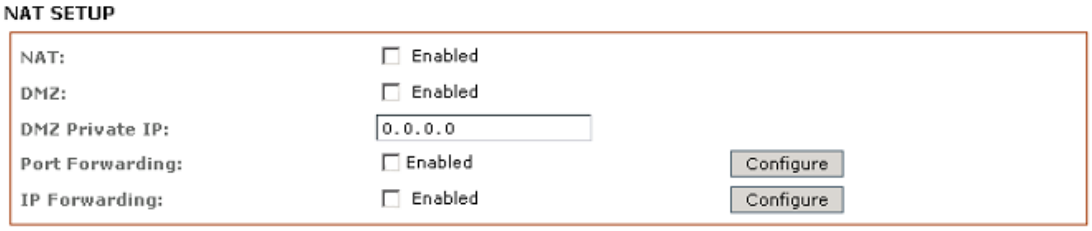


Spanning Tree Protocol: Default is **disabled**. Check the box to enable.

- **Root Priority:** Default value is 32768. A smaller value has a higher priority.
- **Root Hello Time:** Default time is 2 seconds.
- **Root Forward Delay:** Default is 15 seconds.
- **Root Maximum Age:** Default is 20 seconds.

Changing to a lower time can cause high overheads to the network.

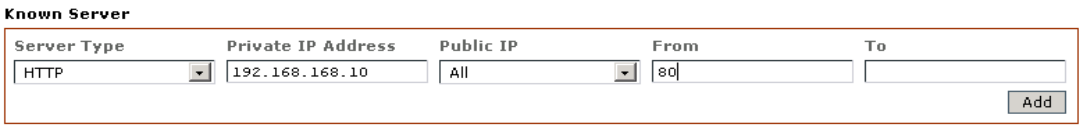
7.5.2 NAT Setup



NAT: Enabled when in router mode and disabled when in bridge mode.

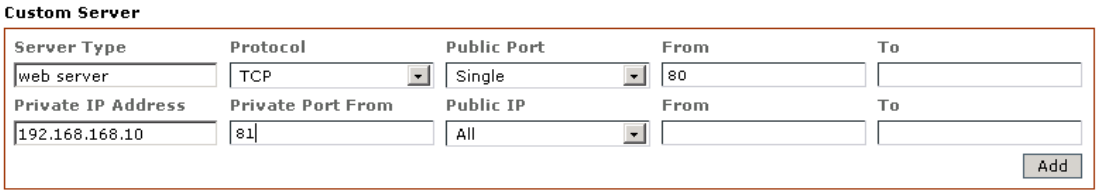
- **DMZ:** Default is disabled. Check on the box to enable.
- **DMZ IP Address:** Input the IP address of the local PC to receive the DMZ packets.
- **Port Forwarding**: Default is disabled. Check on the box to enable.

(For configuration refer to the Appendix section)



Adding an Entry from Known Server: To add an entry use the box pictured above and then select an application from the list.

- **Server Type:** Click to select the wanted application.
- **Private IP Address:** Enter the local IP of the PC running the application.
- **Public IP Address:** If the application is to allow anyone access on the internet, then select the default, **All**. If only a specific IP, select **Single** and enter the IP address. If only a specific range of IP, select **Range** and enter the IP address range.



Adding an Entry from Custom Server: An entry in the custom server box allows the user to enter the other port number services used in applications. The custom server also allows the user to enter a different public and private port service. (See image above)

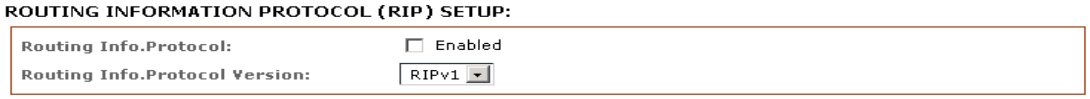
- **Server Type:** Enter a brief name for the application. This info helps the user track the application for the port numbers already set.
- **Protocol:** Select TCP or UDP for the application use.
- **Public Port:** Select single or range of ports for application use.
- **From:** If single port, enter this box only. If port range, enter starting port number here.
- **To:** If single port, leave blank. If port range, enter last port number here.
- **Private IP Address:** Enter the local IP of the PC running the application.
- **Private Port From:** If single port, enter same public port number or new port number. If port range, enter only the starting port number.
- **Public IP Address:** If the application is to allow anyone access on the internet, then select the default, **All**. If only a specific IP is allowed internet access, select **Single** and enter the IP address. If there is a specific range of IPs to receive access to the internet, select **Range** and enter IP address range.

IP Forwarding: Default is disabled. Check on box to enable.
(For configuration refer to the Appendix section)

- **Private IP:** Enter the local IP address that will receive the forward packet by the public IP.
- **Public IP:** Enter the public IP address that will be given access to forward all packets to the local IP.

Click ‘Add’ to add to list.

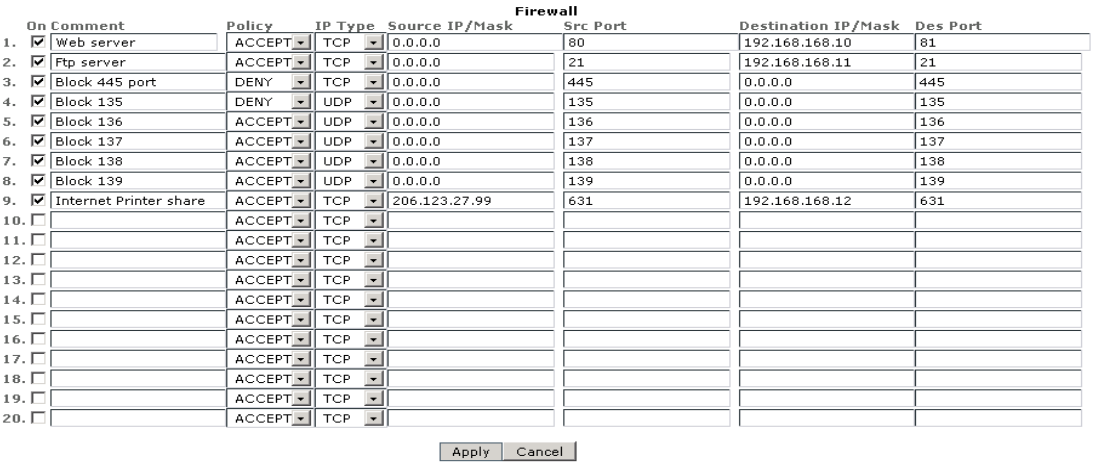
7.5.3 Routing Information Protocol (RIP) Setup



The default setting for the routing control is disabled. Check on the box to enable.
(For configuration refer to the Appendix section)

Router Info Protocol Version: Select RIPv1 or RIPv2

7.5.4 Firewall Setup



Firewall Setup: Default is disabled. Check on the box to enable.
(For configuration refer to the Appendix section)

- **Comment:** Enter a brief name for the service.
- **Policy:** Select ‘Accept’ or ‘Deny’ for the apply rule.
- **IP Type:** Select ICMP, TCP, and UDP packet type.
- **Source IP/Mask:** Enter the source IP address and Netmask. The source IP of the packet (specified within the packet header) is usually the IP of the host system which sends the packets.
- **Src Port:** Enter the source port number in the rule check. The source port of the TCP/UDP packet (specified within the packet header) is usually the port of the host system application which sends the packets.
- **Destination IP/Mask:** Enter the destination IP and Netmask. The destination IP of the packet (specified within the packet header) is usually the IP of the system in which the packet is addressed to.
- **Des Port:** Enter the destination port in the rule check. The destination port of the TCP/UDP packet (specified within the packet header) is usually the port of the host system application in which the packet is addressed to.

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

Outbound Filtering Setup

Filtering Setup: Default is disabled. Check on box to enable.
(For configuration refer to the Appendix section)

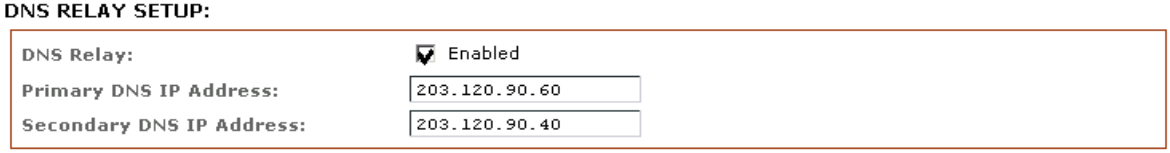
7.5.5 DNS Redirection

Default is enabled. Check on the box to disable. When DNS is enabled, the router device will act as the DNS proxy. The PC connected to this router device will need to set their TCP IP DNS IP to the router's IP address. The PC can still setup a valid DNS IP to skip the DNS proxy handling.

7.5.6 Dynamic DNS Setup

Default is disabled. Check on box to enable. The dynamic DNS allows the router's WAN dynamic IP address to be linked and automatically updated to the domain server which hosts the service every time the IP address is changed. This ensures that the users on the internet can always have access to the hosting service behind the router. *(For configuration refer to the Appendix section)*

7.5.7 DNS Relay Setup



Default is disabled. Check on box to enable. These are the primary and secondary DNS IPs for the device's proxy service that will be used to resolve the domain name on behalf of the client PCs.

- **Primary DNS IP Address:** Enter the primary DNS IP address.
- **Secondary DNS IP Address:** Enter the secondary DNS IP address.

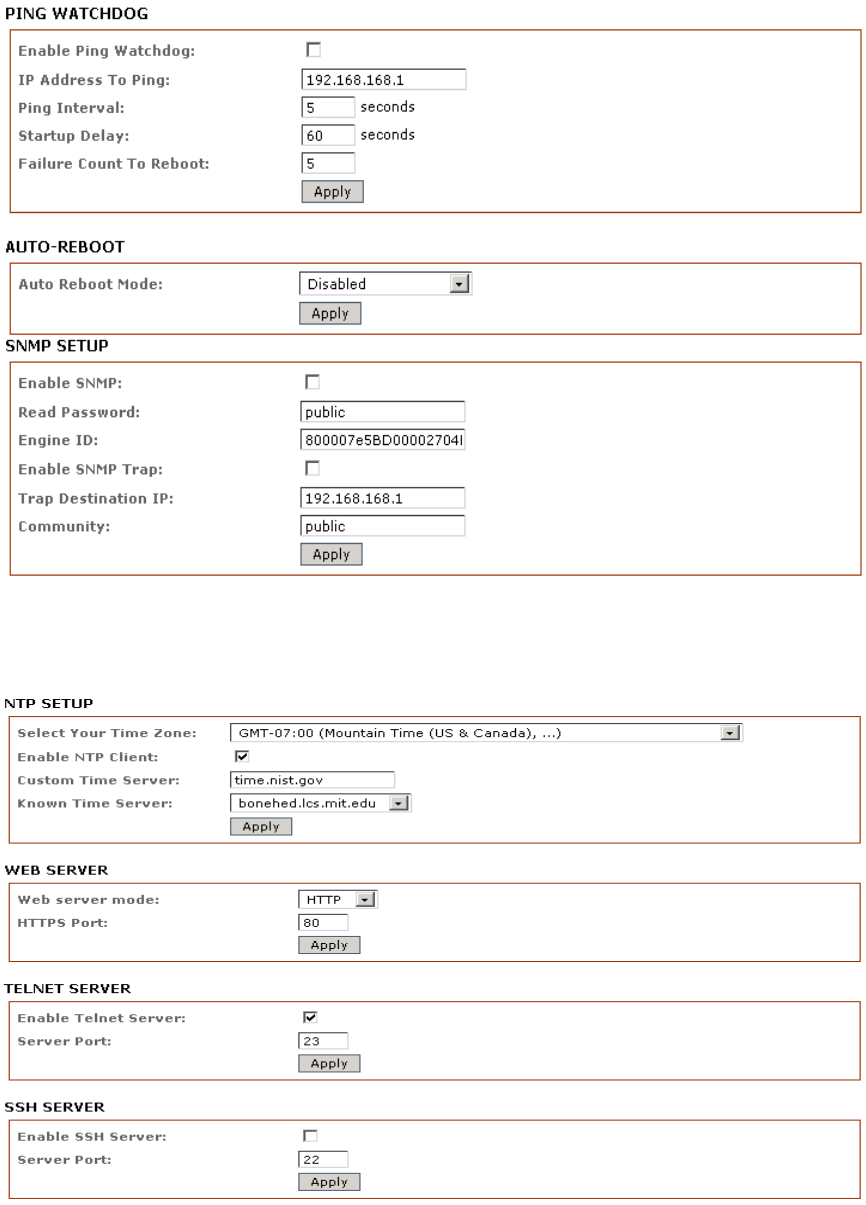
7.5.8 UPNP Setup

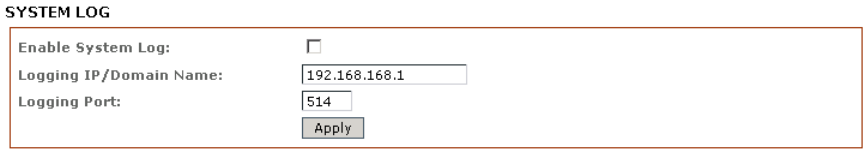
Default is disabled. Check on box to enable. When enabled, the client PC running Microsoft UPnP services can automatically open a specific port required by the PC application in the router. For security reasons, this service should not be open. It is recommended to manually setup all open port services through Port Forwarding.

7.6 Services Tab

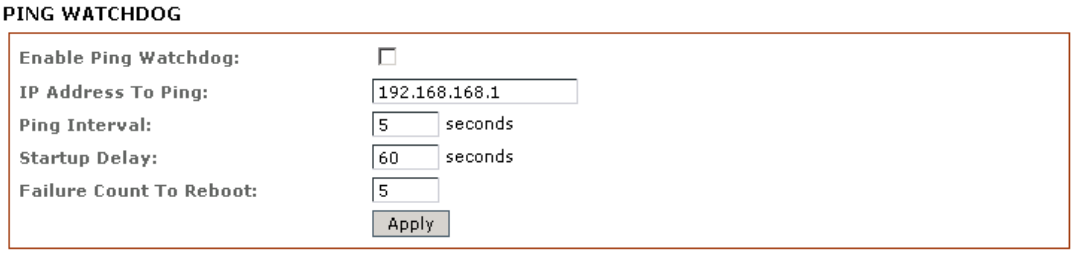
Click the **Services** tab from the menu to open the page below.

The services section provides a variety of useful and enhanced functions to help assist device operations.





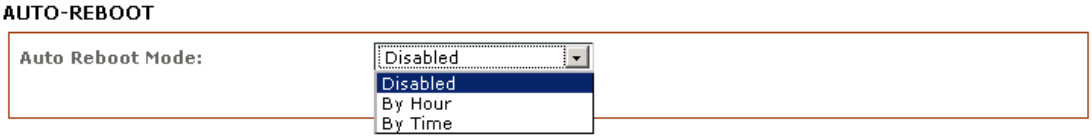
7.6.1 Ping Watchdog



Enable Ping Watchdog: Default is disabled. Check on the box to enable.

- **IP Address to Ping:** Target IP address that will be used for the ping test monitor.
- **Ping Interval:** Default is 5 seconds (minimum) and is the ping test duration.
- **Startup Delay:** Default is 60 seconds (minimum) and has a one-time delay after the device's startup.
- **Failed Count to Reboot:** The device has a default fail count of 5. This is the number of ping failures before the device kicks into the reboot process.

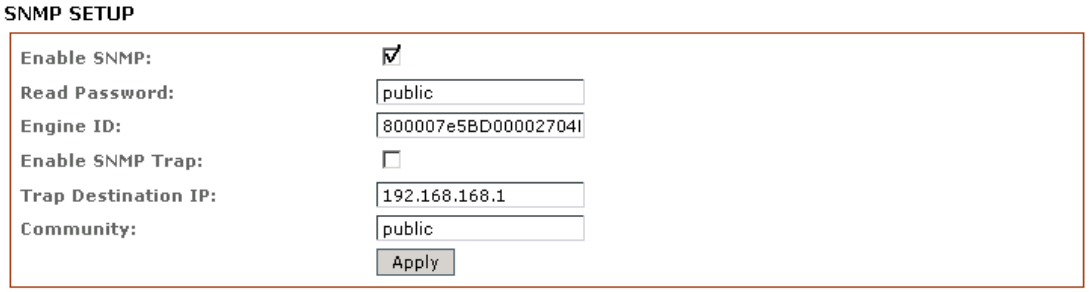
7.6.2 Auto-Reboot



Auto-Reboot Mode: Default is disabled. Select 'By Hour' or 'By Time'. Auto reboot mode allows the user to preset a timer to automatically force a reboot. The timer can be a fixed number of hours or a specified time of day.

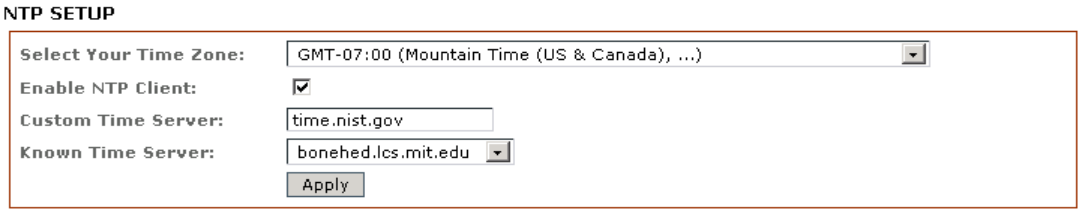
- **By Hour:** Enter the number of hours the device needs to run before the kick start reboot process.
- **By Time:** Enter the specific time of day in hh:mm (24-hour format) to kick start the reboot process.

7.6.3 SNMP Setup



Enable SNMP: Default is disabled. Check on the box to enable SNMP.
Read Only Password: Password used for the device.
Engine ID: Default is 800007e5BD00002704D000007c.
Enable SNMP Trap: Default is disabled. Check on the box to enable.
Trap Destination IP: Enter the IP to send the info when trap is triggered.
Community: Enter the SNMP community string.

7.6.4 NTP Setup



Enable NTP Client: Default is disabled. Check on the box to enable.
Select Your Time Zone: Select the country from the list where the user resides.
Custom Time Server: Default is “time.nist.gov.” Enter the preferred time server domain/IP.
Known Time Server: The user can select one option from the list as the new time server.

7.6.5 Web HTTP Server

Web Server Mode: Default is HTTP. The only options available are HTTP and HTTPs.
HTTP(s) Port: Default is 80 for HTTP and 413 for HTTPs. Enter a new preferred port number if necessary.

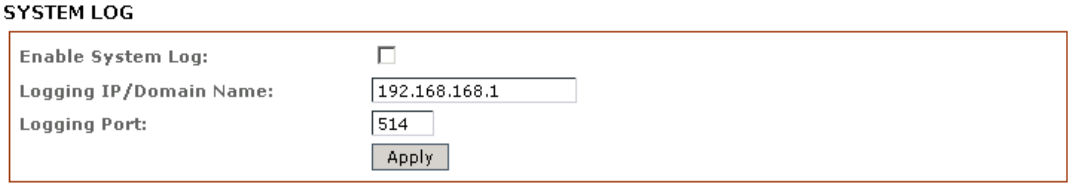
7.6.6 Telnet Access Setup

Enable Telnet Server: Default is enabled. To disable, remove the check by clicking the box.
Server Port: Default is 23. If necessary, enter a new and preferred port number.

7.6.7 SSH Access Setup

Enable SSH Server: Default is disabled. Check on the box to enable.
Server Port: Default is 22. If necessary, enter a new and preferred port number.

7.6.8 System Log Setup

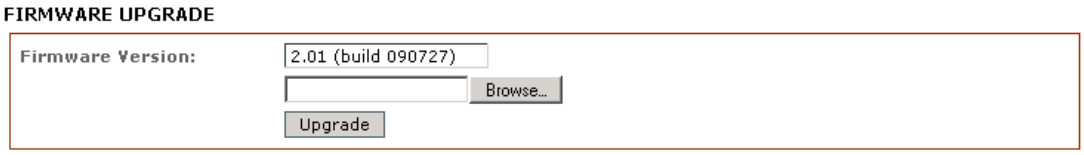


Enable System Logging: Default is disabled. Check on the box to enable.
Logging IP /Domain Name: Enter the destination IP address of the device that is supposed to receive the log.
Logging Port: Default is 514. If necessary, enter a new and preferred port number.

7.7 System Tab

The system page contains administrative options. This page enables the administrator to customize, reboot the device, set it to factory defaults, upload a new firmware, backup or update the configuration and configure administrator's credentials.

7.7.1 Firmware Upgrade



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

- **Firmware Version:** Displays current firmware version of the device system.
- **Upgrade:** Button opens the firmware upload window, if activated.
- **Current Firmware:** Displays device's version of firmware that is currently operating.
- **Firmware File:** Activates the 'Browse' button that navigates to the new firmware file. The full path to the new firmware file location can be seen there. The new firmware file is then transferred to the system after the upload button is activated.

The upgrade button should be activated in order to proceed with the firmware upgrade routine (new firmware image should be uploaded into the system first). Please be patient as the firmware upgrade routine can take 3-7 minutes. The based device will be un-accessible until the firmware upgrade routine is completed.

****Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as these actions will damage the device!****

It is highly recommended to back up the system configuration and the support info file before uploading the new configuration.

7.7.2 Host Name

The host name is the device identifier. It is reported by the SNMP agent to the authorized management stations. The host name will be represented in the popular router operating system's registration screen and discovery tools.

- **Host Name:** Specifies the system identity.
  - **Change button** saves the host name, if activated.

7.7.3 Administrative and Read-Only Account

In this section you can modify the administrator password to protect the device from an 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.
- **Current Password:** Administrator is required to enter a current password. It is required that the password or administrator username is routinely changed to ensure your security.

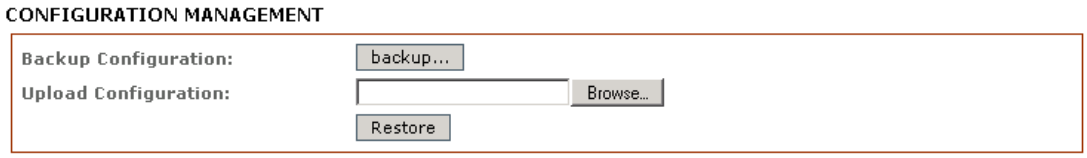
Default Administrator Login Credentials:

- User Name: **admin**
- Password: **password**
  - **New Password:** This is used to authenticate the administrator.
  - **Verify Password:** The new password must be re-entered to verify its accuracy.
- **Click the 'Change'** button to save the changes.

7.7.4 Enable Read-Only Account

Username: This is read-only and cannot be edited.
Password: A new password will be used for the read-only administrator authentication.

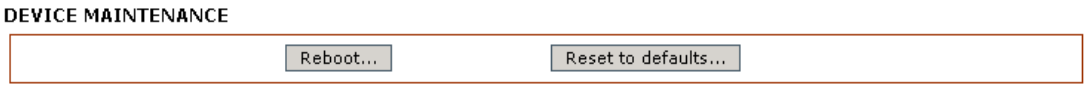
7.7.5 Configuration Management



Backup Configuration: Click the 'Download' button to export the current configuration to a file.

Upload Configuration: Click the 'Browse' button to navigate to and select the new configuration file or specify the full path to the configuration file location. Activating the 'Upload' button will transfer the new configuration file to the system. A new configuration will be effective after the 'Apply' button is activated and the system reboot cycle is completed. The previous system configuration is deleted after the 'Apply' button is activated. It is highly recommended to back up the system configuration before uploading the new configuration.
Only use the configuration backups of the same type of device - configurations backed up from PowerStation2 suits only PowerStation2, but not LiteStation2 or LiteStation5!
**Behavior may be unpredictable when mixing configurations from different types of devices.

7.7.6 Device Maintenance



The controls in this section are dedicated for the device maintenance routines: rebooting, resetting, and generating the supportive informational report.

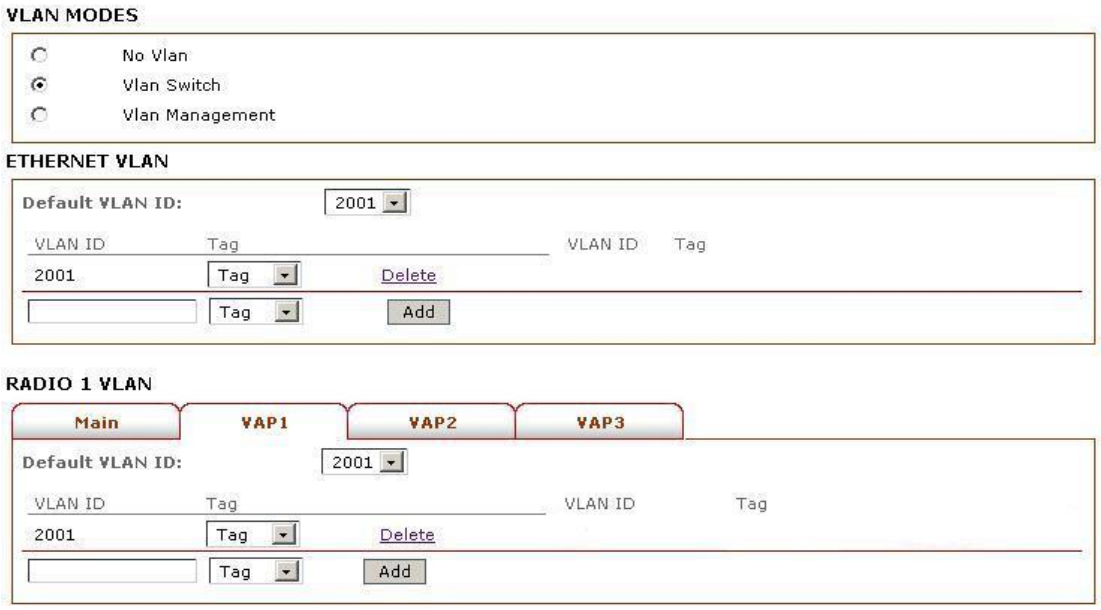
Reboot: Activate the 'Reboot' control in order to initiate a full reboot cycle of the device. The reboot effect is the same as the hardware reboot which is similar to the power off - power on cycle. The system configuration is not modified after the reboot cycle completes. Any non-applied changes will be lost.

Reset to Defaults: Activate the 'Reset to Defaults' control in order to initiate the reset of the device to the factory default routine. The reset routine initiates the system reboot process (similar to the power off - power on cycle). The running system configuration will be deleted and the default system configuration (all the system settings with no exception) will be set.

After the **Reset to Defaults** routine is completed, the device will return to the default IP configuration (192.168.168.1/255.255.255.0) and will start operating in station-bridge mode. It is highly recommended to back up the system configuration before the 'Reset to Defaults' is initiated.

7.8 VLAN Tab

This setup allows the user to create a virtual local network connection through the device's Ethernet and wireless connection. By default, the **VLAN** mode is disabled and checked on **No VLAN.**



7.8.1 VLAN Modes

VLAN Switch

To setup a VLAN network, click the circle next to the **VLAN Switch.**

- To add a Tag VLAN ID for an Ethernet port, type in the ID number, select **Tag** and click **Add**
- To add a Tag VLAN ID for MAIN wireless SSID, type in the ID number, select **Tag** and click **Add**
- To add a Tag VLAN ID for VAP1 wireless SSID, type in the ID number, select **Tag** and click **Add**
- To add a Tag VLAN ID for VAP2 wireless SSID, type in the ID number, select **Tag** and click **Add**
- To add a Tag VLAN ID for VAP3 wireless SSID, type in the ID number, select **Tag** and click **Add**

***** ***Warning:*** *Adding a Tag VLAN ID to the device's interface port can cause a loss of connection to the device's web manager, if the PC Ethernet port or wireless connection do not have a Tag VLAN ID or do not have the same Tag VLAN ID setup in the device.*

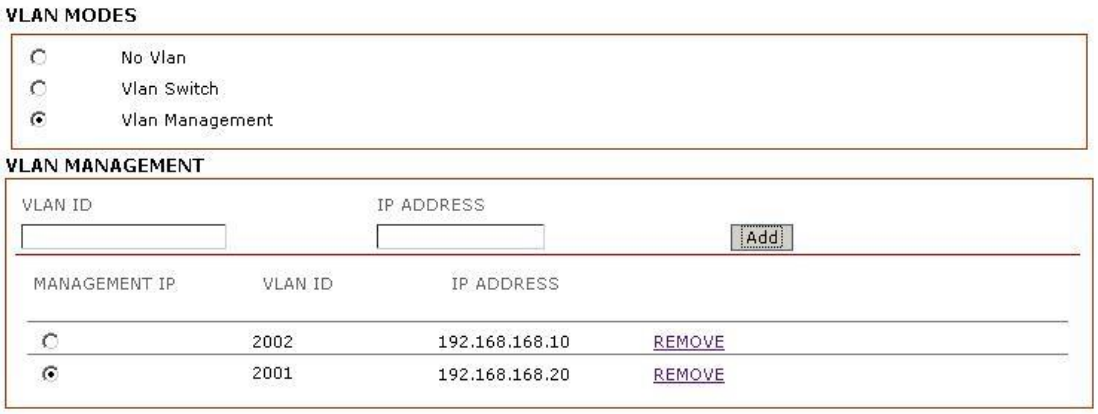
- Similarly, to add an untag VLAN ID, enter the ID number and select **Untag** and click **Add**

*(Refer to **Appendix V** for VLAN setup examples)*

VLAN Management

VLAN management allows the user to control and limit clients' connections to the same tag VLAN ID group.

**** Note: VLAN management only works in the tag VLAN pass-through mode. i.e. VLAN Switch is disabled. When VLAN Switch is enabled or configured, the VLAN management function stops operating.***



Example:
Assuming there are two VLAN ID groups, 2001 and 2002 setup in an AP device. One entry is in the VLAN Management and has a VLAN ID of 2001 with a masquerade IP address of 192.168.168.20. Another entry is in the VLAN management and has a VLAN ID of 2002 with a masquerade IP address of 192.168.168.10.

The user can only select one of the two entries in order to be the active VLAN ID and IP address. If the VLAN ID 2001 group is selected, only computers in that VLAN ID group can open the AP device web page using the IP address, http://192.168.168.20.

To change to another ID group, VLAN ID 2002, mark the radio button under the management IP, then click 'Apply' and 'Saved'. If there is no entry in the VLAN management, there is no restriction. All computers can open the AP device web page by the default IP address setup in the 'Basic Network' page.

Appendix I - Network

This section provides a more general and detailed explanation on the network operation modes.

The 'Network Page' explains how the administrator can setup the device in either bridge or router mode. The IP configuration 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: Specifies 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 the subscriber stations, while connecting to an 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 while the 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 to operate in Layer 3 to perform routing and to enable network segmentation – wireless clients will be on different IP subnets. Router mode will block broadcasts as it is not transparent.

The device supports multicast packets to pass-through in router mode. The router can act as a DHCP server and use a network address translation (masquerading) feature which is widely used by the 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 the 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 it can be set to obtain an IP address from the DHCP server it is connected to. One of the IP assignment modes must be selected.
    - **DHCP:** Choose this option to assign the dynamic IP address, gateway and DNS address to the local DHCP server.
    - **STATIC:** Choose this option to assign the static IP settings for the bridge interface.
    - **IP Address:** Enter the IP address of the device while the static bridge IP address mode is selected. This IP will be used for the device management purposes. The IP address and Netmask settings should be consistent with the address space of the network segment where the device resides. If the device's IP settings and administrator IP settings happen to be connected to the device in either a wired or wireless way, the device will use a different address space and the device will become unreachable.

- **Netmask:** A value when expanded into binary that 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. The IP address of 255.255.255.0 is a typical Netmask value for Class C networks.

- **Gateway IP:** Typically, this is the IP address of the host router that provides the point of connection to the internet. This 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 the same address space (on same network segment) as the device.

- **Primary/Secondary DNS IP:** The Domain Name System (DNS) is an internet "phone book" which translates domain names into 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 device management purposes.
    - The secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become 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 the network and it helps to eliminate loops from the topology. If the 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, and in this case there would be no reason for the bridge to participate in the Spanning Tree Protocol.

Bridge Mode Firewall Configuration Settings

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

Firewall entries can be specified by following the criteria below:

- Access the interface (WLAN or LAN) where filtering of the incoming or passing-through packets are processed.
- Filter the IP type sets for the particular Layer 3 protocol type (ICMP, TCP, and UDP).
    - Source IP/mask is the source IP of the packet (specified within the packet header), which is usually the IP of the host system which sends the packets.
    - Source port of the TCP/UDP packet (specified within the packet header), which is usually the port of the host system application which sends the packets.

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

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

Comments are the informal field of a particular firewall entry. Only a few words about the purpose for a particular firewall entry are generally saved.

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

New firewall entries can be saved by activating the ‘Apply’ button or can be discarded by activating the ‘Cancel’ button in the firewall configuration window. All the active firewall entries are stored in the FIREWALL chain of the editable filtering table while the device is operating in bridge mode. Click the ‘Apply Setting and Save Changes’ button to save the changes made in the ‘Network’ page.

Appendix II – Wireless Router Mode

This section provides more details on wireless router mode functions.

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 the *internal* LAN, and the Ethernet interface is dedicated for the connection to the *external* network while the device is operating in the **AP/AP WDS wireless mode**.
- The wireless interface and all the wireless clients connected are considered the *external* network, and all the network devices on the LAN side as well as the Ethernet interface are considered the *internal* network, while the device is operating in **station or station WDS mode**.

Wireless/wired clients are routed from the internal network to the external network by default. The 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 which is connected to the internal network according to the wireless operation mode as described above. The 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). The IP address will also be used for management purposes of the device.

WLAN IP Address: This IP address represents the LAN or WLAN interface that is connected to the external network (according to the wireless operation mode described above). It is the IP address that can be used for routing and 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 the static IP settings for the external interface. The IP address and Netmask settings should be consistent with the address space of the network segment where the device resides. If the device's IP settings and administrator PC settings are connected to the device through a wired or wireless IP setting, the device will use a different address space and will become unreachable.

Netmask: This is used to define the device's IP classification for the chosen IP address range. The IP address of 255.255.255.0 is a typical Netmask value for Class C networks, which supports the 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.
The 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 the LAN interface in the AP case).

Primary/Secondary DNS IP: The Domain Name System (DNS) is an internet "phone book" which translates domain names into 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 is used for management purposes of the device.
- The secondary DNS server IP address is *optional*. It is used as the fail-over in case the primary DNS server becomes 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 contrariwise direction in "Station or Station WDS" mode.

- **NAT** is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the IP tables and NAT tables while the device is operating in router mode. Please refer to the IP tables tutorial for a detailed description of the NAT functionality in router mode. Static routes should be specified in order for the packets to pass-through the based device, if the NAT is disabled while operating in router mode.

Enable DHCP Server: The Dynamic Host Configuration Protocol (DHCP) server assigns IP addresses to clients who will associate with the wireless interface while the device is operating in AP/AP WDS wireless mode. It also assigns IP addresses to clients that will connect to the LAN interface while the device is operating in station or station WDS mode.

Range Start/End: This range determines the IP addresses given out by the DHCP server to the client devices on the internal network that 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 lease time helps to ensure client operation without interruption but could cause potential conflicts. Lowering the lease time will help to avoid potential address conflicts, but it could also cause interruptions to the client while it acquires new IP addresses from the DHCP server.

Port Forwarding Settings

Port Forwarding: This allows specific ports from the host residing in the internal network to be forwarded to the external network. It is useful for a number of applications, such as, FTP servers and gaming 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 can be opened by enabling the 'Port Forwarding' option and activating the 'Configure' button.

Port forwarding entries can be specified by using the following criteria:

- **Private IP** is the IP of the host that is connected to the internal network and needs to be accessible from the external network.
- **Private Port** is 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** is the Layer 3 protocol (IP) type that needs to be forwarded from the internal network. The public port is 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** are an informal field for a particular port forwarding entry. Usually, only a few words about the particular port forwarding entry purpose are saved. An enabled flag can either enable or disable a particular port forwarding entry. All the added firewall entries are saved in a system configuration file, however only the enabled port forwarding entries will be active during the system's operation.

New entries in port forwarding can be saved by activating the 'Save' button or can be discarded by activating the 'Cancel' button in the port forwarding configuration window.

DNS Proxy: The DNS Proxy forwards the domain name system requests from the host that resides in the internal network to the DNS server while the device is operating in router mode. A valid primary DNS server IP address needs to be specified for the DNS Proxy functionality. The internal network IP interface 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 the domain names to the IP addresses.

Bridge Mode Firewall Configuration Settings

Firewall functionality on any router interface can be enabled using the "Enable Firewall" option. The router firewall rules can be configured, enabled or disabled when accessing the firewall configuration window that can be opened with the "Configure" button.

Firewall entries can be specified by using the following criteria:

- **Interface:** The interface (WLAN, LAN or PPP) is where the filtering of the incoming or passing-through packets are processed.
- **IP Type** sets which particular Layer 3 protocol type (ICMP, TCP, UDP, P2P) should be filtered.
- **Source IP/mask:** The source IP of the packet (specified within the packet header) is usually 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) is usually the port of the host system application that sends packets.
- **Destination IP/mask:** The destination IP of the packet (specified within the packet header) is usually the IP of the system in which the packet is addressed to.
- **Destination Port:** The destination port of the TCP/UDP packet (specified within the packet header) is usually the port of the host system application in which the packet is addressed to.
- **Comments:** The informal field for a comment of a particular firewall entry. Usually, only a few words about the particular firewall entry purpose are saved.
- **On flag** enables or disables the particular firewall entry. All the added firewall entries are saved in a system configuration file, however only the enabled firewall entries will be active during the device's operation. New entries in the firewall can be saved by activating the 'Apply Setting and Save Changes' button or can be discarded by activating the 'Cancel' button in the firewall configuration window. All the active firewall entries are stored in the FIREWALL chain of the IP tables and filtering tables while the device is operating in router mode.

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transportation. 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, and 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 the PPPoE connection is established. The broadcast address is used for the PPPoE server discovery and tunnel establishment. A valid authorization with credentials is required for the PPPoE connection.

- **PPPoE Username** – The username to connect to the server must match the configured username on the PPPoE server.
- **Password** – The password to connect to the server must match the configured password 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 through a PPP tunnel.

Enable DMZ: The Demilitarized Zone (DMZ) can be enabled and used as a place where services can be located, such as, web servers, proxy servers, and e-mail servers. These services can still serve the local network and at the same time are isolated for additional security. The DMZ is commonly used with the NAT functionality as an alternative for port forwarding. This allows all the ports of the host network device to be visible from the external network.

DMZ Management Port: The web management port for the based device (TCP/IP port 80 by default) will be used as the host device if the DMZ management port is enabled. In this case, the device will respond to the requests from the external network as if it was the host specified with the DMZ IP. It is recommended to leave the management port disabled while the based device will become inaccessible from the external network if it is enabled.

DMZ IP: This is connected to the internal network host, specified with the DMZ IP address which will be accessible from the external network. With a multicast design, applications can send one copy of each packet and address it to a group of computers that want 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 tend to isolate all the broadcast (thus multicast) traffic between the internal and external networks, however this provides the multicast traffic pass-through functionality. Click the ‘Change’ button to save the changes made in the network page.

Appendix III- Advanced Settings

This section provides a more detail explanation on advanced settings for routing and wireless settings. The advanced options page allows users to manage advanced settings for the device's performance and behavior. The advanced wireless settings are tailored for a more technically advanced user who has a sufficient knowledge about wireless LAN technology. These settings should not be changed unless the user is well aware of what device changes will occur.

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 uses only 1 Tx/Rx stream.
- MCS8 to MCS15 are 802.11n rates, which uses 2 Tx/Rx streams.

The rate algorithm has a critical impact on performance in outdoor links, because it generally lowers data rates and is more immune to noise while higher rates are less immune but are capable of higher throughput.

Rate Aggressiveness: Allows users to reduce or increase the transmit rate while remaining in a full auto algorithm. There are two scenarios when rate aggressiveness is useful. First, when the environment might be noisy, lower the throughput to ensure better stability, and the rate aggressiveness allows the device to reduce the transmit rate, so range or power can be higher. Second, choose a range of value from -3,-2,-1 when an environment is free of interference, the full auto algorithm might give low throughput, so increase the rate aggressiveness and it will increase the transmit rate, and in this case, will have a higher throughput. Choose a range of value from +3, +2, +1.

- **Noise Immunity** options 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 interferes.

RTS Threshold: This determines the packet size of a transmission and through the use of an access point helps to control traffic flow. The range is 0-2347bytes, or you can select the word "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. The RTS/CTS packet size threshold is 0-2347 bytes. If the mode wants to transmit a packet size larger than the threshold, the RTS/CTS handshake is triggered. If the packet size is equal to or less than the threshold, then the data frame is immediately sent. The system uses the request to send or clear to send frames for the handshake which provides a collision reduction in regards to the access point with hidden stations. The stations are initially sending an RTS frame while the data is only sent after a handshake with an AP is completed. Stations respond with the CTS frame to the RTS which provides clear media in order to send the data to the requesting station. The CTS collision and control management has defined the time interval for which all the other stations hold off the transmission and wait until the requesting station has finished the transmission.

Fragmentation Threshold: This specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or you can select the word “off”. Setting the fragmentation threshold too low may result in poor network performance. The use of fragmentation can increase the reliability of frame transmissions. When sending smaller frames, collisions are much less likely to occur, however lower values of the fragmentation threshold will result in a lower throughput. Minor or no modifications to the fragmentation threshold value is recommended while the default setting of 2346 is optimum in most of the wireless network cases.

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 the client isolation is enabled, wireless stations connected to the same AP will not be able to interconnect on both the layer 2 (MAC) and layer 3 (IP) level. This is effective for the associated stations and WDS peers.

Acknowledgement Timeout

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

- **Distance:** This specifies the distance value in miles (or kilometers) by using a slider or you can manually enter the value. The signal strength and throughput falls off with range. Changing the distance value will change the ACK timeout to the new and appropriate distance value.

- **ACK Timeout:** Every time the station receives a data frame, it sends an ACK frame to the AP (if transmission errors are absent). If the does not receive an ACK frame from the AP within the set timeout, it re-sends the frame. The performance drops because too many data frames are needed to be re-sent, thus if the timeout is set too short or too long, it will result in a poor connection and throughput performance. By changing the ACK timeout value, it will change the distance to the appropriate distance value for the ACK timeout.

- **Auto:** Adjust the control and enable the ‘ACK Timeout Self-Configuration’ feature. If enabled, the ACK timeout value will be dynamically derived using an algorithm similar to the conservative rate algorithm. It is not recommended to use the auto adjust option for long range links because if the signal level is low, there could be a high level of interference.

  If two or more stations are located at considerably different distances from the access point, the highest ACK timeout for the farthest station should be set at the access point side. It is not recommended to use the auto adjust option for point-to-multipoint connections as it will not warrant the highest network performance.

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's defined IP address (it can be the internet gateway for example). If it is unable to ping under the user's defined constraints, the device will automatically reboot. This option creates a "fail-proof" mechanism.
Ping watchdog is dedicated for continuous monitoring of a particular connection to a 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:** Using the 'Control' key will enable the ping watchdog tool.
- **IP Address to Ping:** Enter the target host IP address you wish to monitor.
- **Ping Interval:** Specify the time interval (in seconds) it takes between sending the ICMP "echo requests".
- **Startup Delay:** Specify the initial time delay (in seconds) it takes the device from startup or reboot to start sending the first 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 continuously received, 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.
The 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). An SNMP agent allows network administrators to monitor network performance to find and solve network problems. For equipment identification purposes, it is always a good idea to configure SNMP agents with contact and location information.

- **Enable SNMP Agent:** Using the 'Control' key will enable the SNMP agent.
- **SNMP Community:** Specify the SNMP community string. It is required to confirm access to MIB objects and functions as the embedded password. The device supports a read-only community string that gives read access to authorized management stations and to all the objects in the MIB except the community strings, but does not allow writing access for devices that supports SNMP v1.
- **Contact:** Specify a contact (identity) in case an emergency situation arises.
- **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 the computer systems over packet-switched and variable-latency data networks. If the option log is enabled, it can be used to set the device's system time which is reported next to every system log entry while registering system events.

Web Server: The following device web server parameters can be set.

- **Use Secure Connection (HTTPS):** If checked, 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 device 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 device 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: This option enables the registration routine of the system log messages.
Enabling the remote log enables the syslog to remotely send the function while the system log messages are sent to a remote server specified by the remote log IP address and remote log port.

Remote Log IP Address is the host IP address where the syslog messages should be sent. A remote host should be configured properly to receive syslog protocol messages.

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

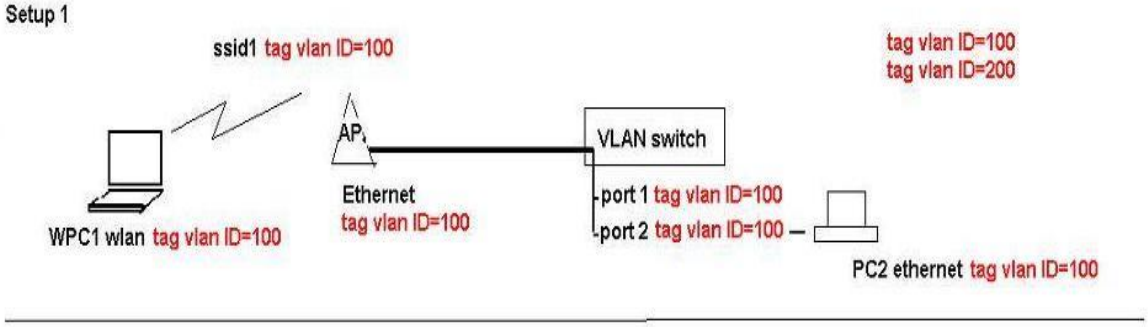
***Note: Every logged message contains at least a system time and a host name. Usually, a particular service name that generates the system event is specified within the message. Messages from different services have different context and different levels of details. Usually, an error warning or informational system service message is reported. The more detailed the system message being reported, generates a greater volume of logged messages.*

Appendix V- VLAN Setup Examples

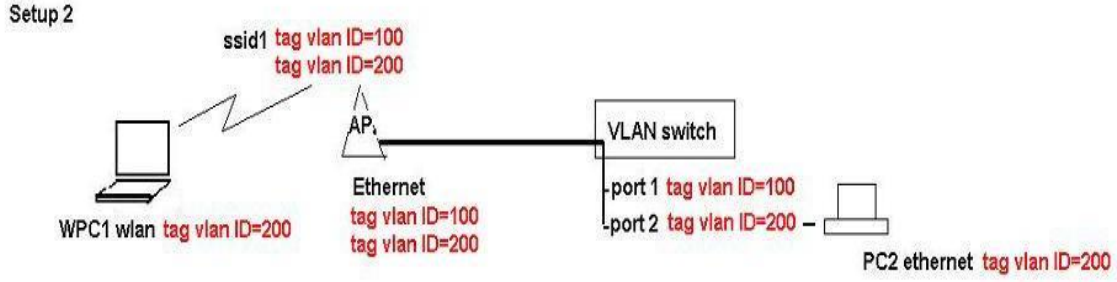
A) Tagged Wireless VLAN to Tagged Ethernet VLAN Setup

Tag vlan connection Setup

Setup 1



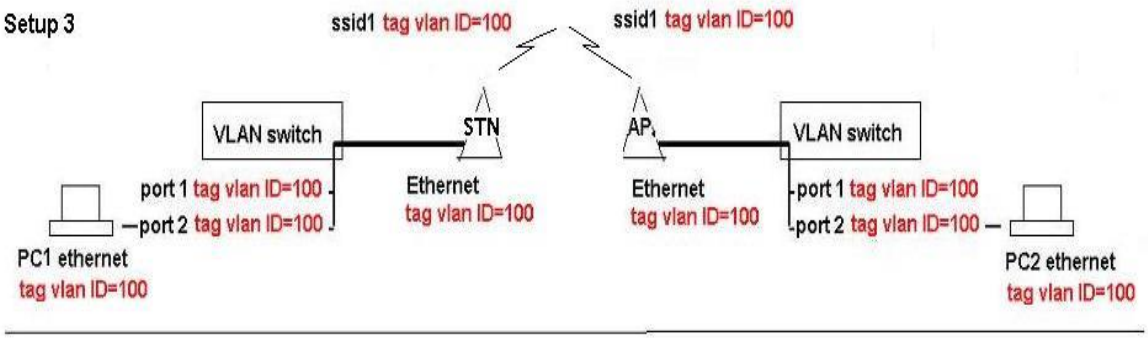
Setup 2



Hints:-

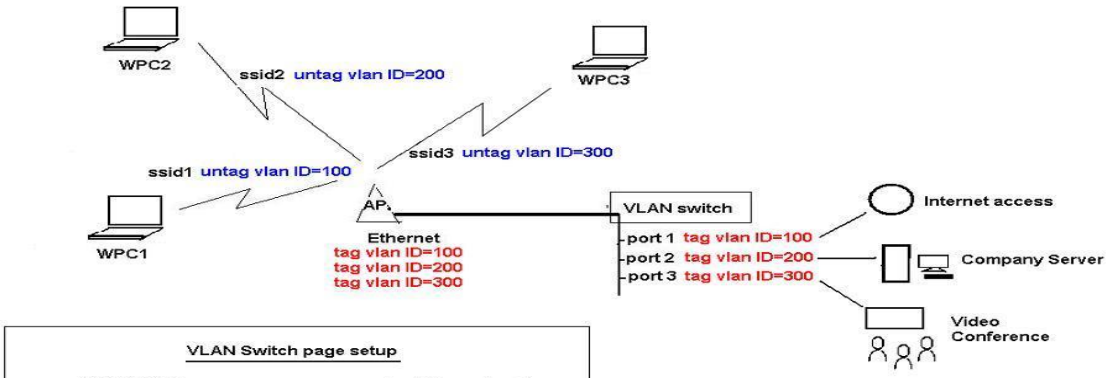
For each vlan id group to send between AP and wireless clients,
AP wlan and ethernet interface must add that vlan group.
AP ethernet port connecting to the switch must set to the default vlan id same as switch port its connecting.

Setup 3



B) Untagged Wireless VLAN to Tagged Ethernet VLAN Setup

Multi-SSID with untag vlan connections to secured wired tag vlan network connections



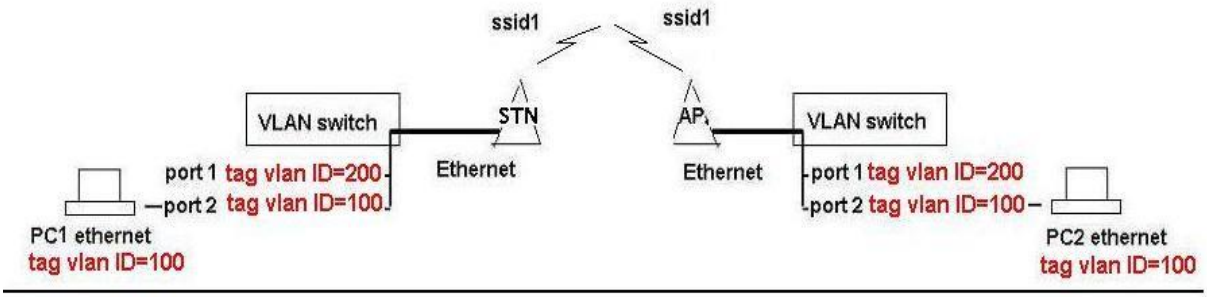
VLAN Switch page setup

for wireless			for Ethernet port
MAIN	add	untag vlan ID=100	add tag vlan ID=100
VAP1	add	untag vlan ID=200	add tag vlan ID=200
VAP2	add	untag vlan ID=300	add tag vlan ID=300
VAP3	add	untag vlan ID=400	add tag vlan ID=400

C) Tagged VLAN Pass-Through

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

* - AP and Station devices no VLAN setting required



Antaira Customer Service and Support

(Antaira US Headquarter) + 844-268-2472

(Antaira Europe Office) + 48-22-862-88-81

(Antaira Asia Office) + 886-2-2218-9733

Please report any problems to Antaira:

www.antaira.com / support@antaira.com

www.antaira.eu / info@antaira.eu

www.antaira.com.tw / info@antaira.com.tw

Any changes to this material will be announced on the Antaira website.