Industrial Wireless-N Access Point

APN-210N

User Manual

Version 1.2

www.antaira.com

© *Copyright 2013 Antaira Technologies, LLC*

All Rights Reserved

This document contains information, which is protected by copyright. Reproduction, adaptation or translation without prior permission is prohibited, except as allowed under the copyright laws.

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.

Notice: Copyrights © 2013 by Antaira Technologies, LLC. All rights reserved. Reproduction, adaptation, or translation without prior permission of Antaira Technologies, LLC is prohibited, except as allowed under the copyright laws.

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.

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

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.: APN-210N 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.

Manual Version:1.12 (January 2013)

This manual is written based on Firmware version 1.26

Table of Contents

Overview **7**
Introduction **7**
Features and Benefits 8
Hardware Installation **9**
DIN-Rail Installation **9**
Wall Mount Installation 10
Hardware Overview **11**
Front Panel 11
Front Panel LEDs 12
Top Panel 12
Rear Panel 13
Cables and Antennas **14**
Ethernet Cables 14
10BaseT/100BaseTX Pin Assignments 14
Wireless Antenna 15
Operation Modes & Connection Examples **16**
Access Point and Access Point WDS Mode 16
Access Point WDS Mode 16
Station Mode 17
Station WDS Mode 18
Repeater WDS Mode 19
Configure the IP Address **19**
For Windows 95/98/98SE/ME/NT 20
For Windows XP/2000 21
Access the Web Interface **23**
Access with uConfig 23
Access with Web Browser 26
Navigation **29**
Main Menu Bar 29
How to save changes 29
Basic Network Tab **30**
Network Mode: Bridging 30
LAN Setup 30
Basic Wireless Tab **33**
Basic Wireless Settings 33
Wireless Mode 33
Access Point Parameters Settings 34
Station Parameters Settings 36
Wireless Security 38
Virtual Access Point (VAP) 43

Advance Wireless Tab 44
Long Range Parameters Setup 44
Services Tab 46
Ping Watchdog 47
Auto-Reboot 47
SNMP Setup 48
NTP Setup 48
Web HTTP Security 48
Telnet Access Setup 49
SSH Access Setup 49
System Log Setup 49
System Tab 50
Firmware Upgrade 50
Host Name 51
Administrative and Read-only Account 51
Configuration Management 52
Device Maintenance 52
Status Page 54
Status Reporting 54
Station Connection Info 56
More Status 58
VLAN Tab 59
VLAN Switch 59
VLAN Management 60
Appendix I - Network 61
Appendix II- Advanced Settings 64
Appendix III- Services 67
Appendix IV- VLAN Setup examples 69
A) Tagged Wireless VLAN to Tagged Ethernet VLAN Setup 69
B) Untagged Wireless VLAN to Tagged Ethernet VLAN setup 70
C) Tagged VLAN Pass-Through 70

Overview

Introduction

The high-performance Wireless Network Access Point (AP) is designed for industrial and enterprise access applications. Embedded with the Atheros chipset, it boasts network robustness, stability and wider network coverage. Based on 802.11n (Draft 2.0), the access point supports high-speed data transmission of up to 300Mbps.

The access point is capable of operating in different modes, which makes it suitable for a wide variety of wireless applications, including long-distance deployments.

Designed with externals R-SMA connectors offering excellent electrical performance and compatible with R-SMA antennas, the access point can be used for a wide variety of wireless applications and allows you to position the wireless antenna in a better signal-broadcasting location for improved wireless coverage and signal strength or simply in a more convenient location.

To protect your security and privacy, the access point is armed with many enhanced and 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 access point also incorporates a unique set of advanced features such as: Virtual AP to deliver multiple services; Long-Range parameter fine-tuning which provide the access point with the ability to auto-calculate parameters such as slot time, ACK time-out and CTS time-out to achieve a longer range.

Features and Benefits

Point-to-Point & Point-to-MultiPoint Support

Point-to-Point and Point-to-MultiPoint communication between different buildings enables you to bridge wireless clients that are kilometres apart while unifying the networks.

Virtual AP (Multiple SSID)

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

Highly Secured Wireless Network

The access point supports the highest available wireless security standard: IEEE802.11i compliant. The access point also supports IEEE 802.1x for 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 exclusive 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 CLI (Command Line Interface) for control and monitoring.

SSH

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

Hardware Installation

DIN-Rail Installation

Each AP has a DIN-Rail kit on rear panel. The DIN-Rail kit helps AP to fix on the DIN-Rail. It is easy to install the AP on the DIN-Rail:

Step 1: Slant the AP and mount the metal spring to DIN-Rail.

Step 2: Push the AP toward the DIN-Rail until you heard a “click” sound.

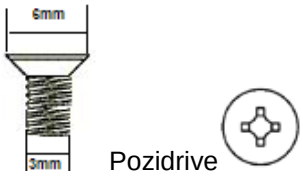
Wall Mount Installation

Each AP has another installation method to fix the AP. A wall mount panel can be found in the package. The following steps show how to mount the AP on the wall:

Step 1: Remove DIN-Rail kit.

Step 2: Use 6 screws that can be found in the package to combine the wall mount panel.

**** The screws specification shows in the following two pictures. In order to prevent the AP from any damage, the screws should not be larger than the size of that used in the APN-210N.***



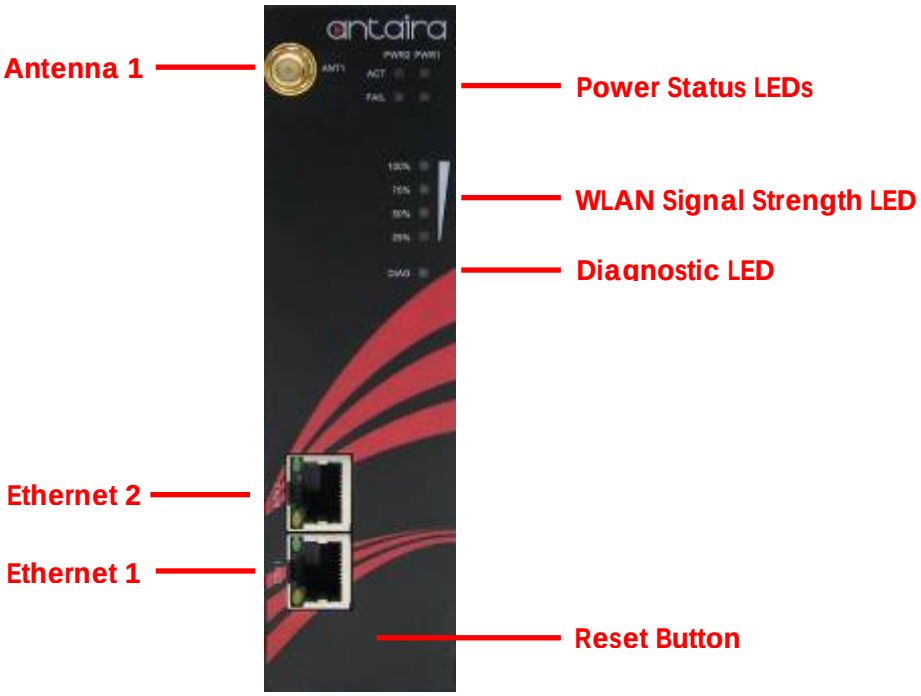
Step 3: Mount the combined AP on the wall.

Hardware Overview

Front Panel

The following table describes the labels on the APN-210N

Port	Description
10/100 RJ-45 fast Ethernet ports	2 10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation Default Setting : Speed: auto
ANT 1	Reversed SMA connector for external antenna
Reset	Reset unit (Momentary press button) Reset to factory default (Press and hold for 10 sec.)



Front Panel of the APN-210N

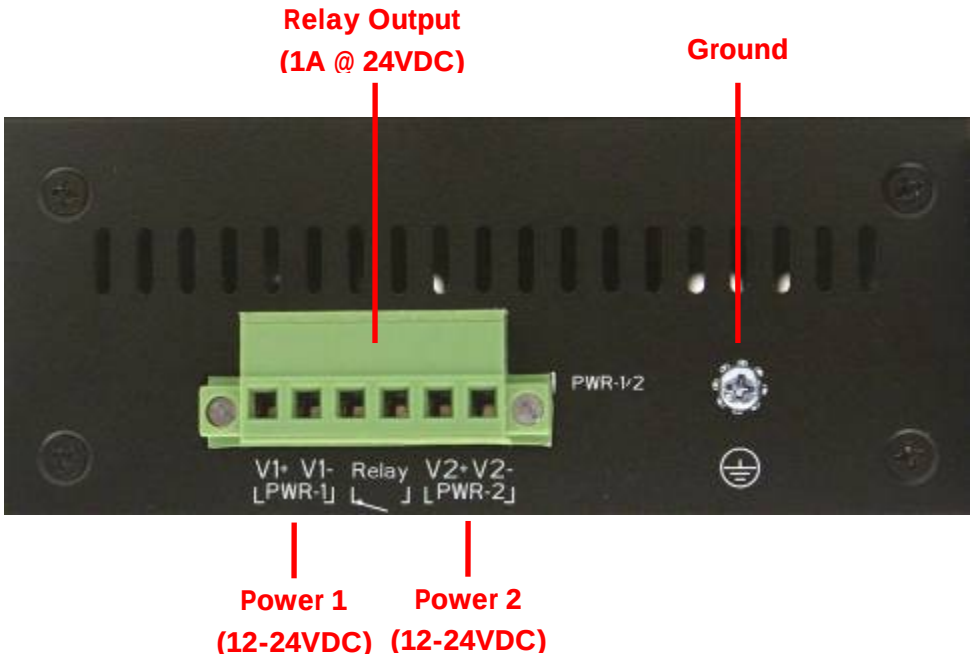
Front Panel LEDs

LED	Color	Status	Description
PWR1	Green/Red	Green	DC power 1 active
		Red	DC power 1 fail/non active
PWR2	Green/Red	Green	DC power 2 active
		Red	DC power 2 fail/non active
WLAN Strength	Green/Red	Red	LED 1 < 25%
		Green	LED 2 < 50%
		Green	LED 3 < 75%
		Green	LED 4 ≤ 100%
Diag	Green	Blinking	Unit not ready/Boot sequence
		Off	Unit ready
10/100Base-T(X) Fast Ethernet ports			
ETH 1	Yellow	On	Port link up at 10Mbps
ETH 2	Green	On	Port link up at 100Mbps

Top Panel

The top panel components of the APN-210N are showed as below:

**Terminal block includes: PWR1, PWR2 (12 ~ 24V DC) and Relay output (1A@24VDC)*

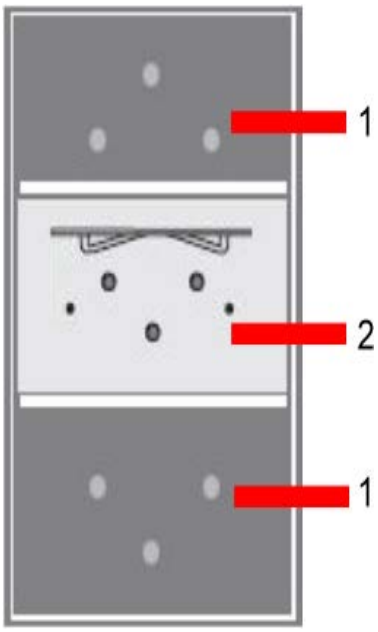


Top panel of the APN-210N

Rear Panel

The rear panel components of the APN-210N are showed as below:

1. Screw holes for wall mount kit.
2. DIN-Rail kit



Rare panel of the APN-210N

Cables and Antennas

Ethernet Cables

The APN-210N WLAN AP has standard Ethernet ports. 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	UTP 100 m (328 ft)	RJ-45

10BaseT/100BaseTX Pin Assignments

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.

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

The APN-210N AP support 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.

MDI/MDI-X pins assignment

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

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

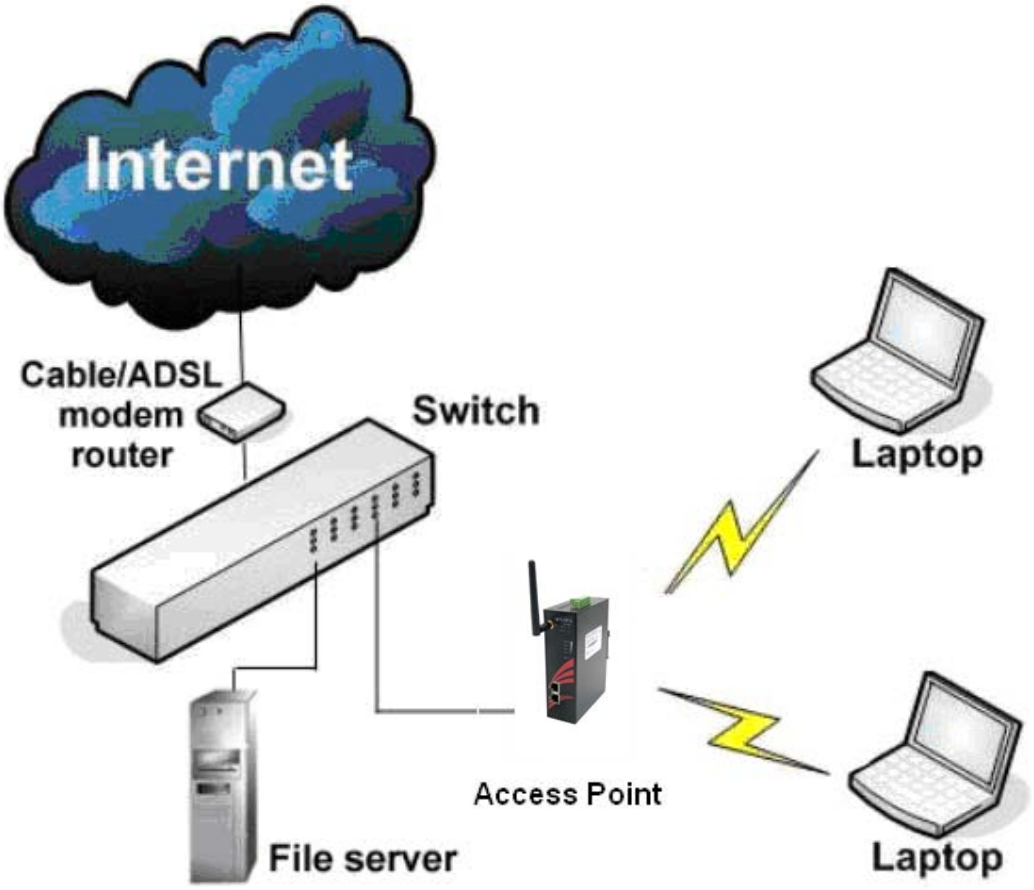
Wireless Antenna

2.4GHz antennas are used for the APN-210N and connected with reversed SMA connectors. External antennas also can be applied with this connectors.

Operation Modes & Connection Examples

Access Point and Access Point WDS Mode

The Access Point Mode is the default mode of the device. It enables the bridging of wireless clients to wired network infrastructure and enables transparent access and communication with each other.
The illustration below shows a typical resources sharing application example using this device. The wireless users are able to access the file server connected to the switch, through the access point in Access Point Mode.



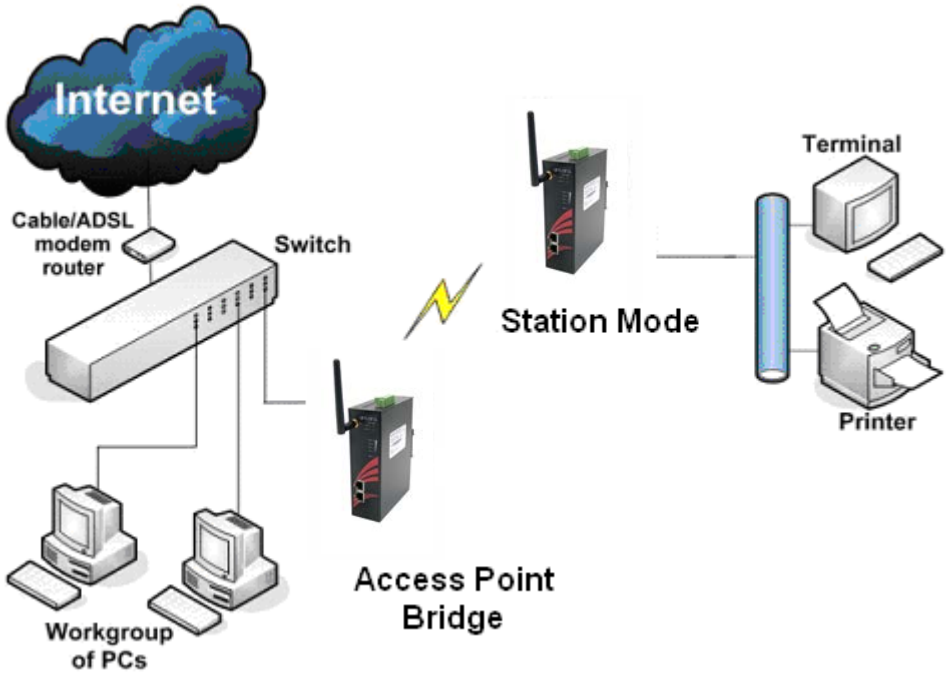
Access Point WDS Mode

This is mode is generally use for point-to-point or point-to-multi-point connection.
It is mainly use with Station WDS to build the point and multi-point connections.

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 this client device, and the wireless Ethernet network connected at the access point.

In this example the workgroup PCs on the ethernet network connected to the Station device can access the printer across the wireless connection to the access point where the printer is connected.

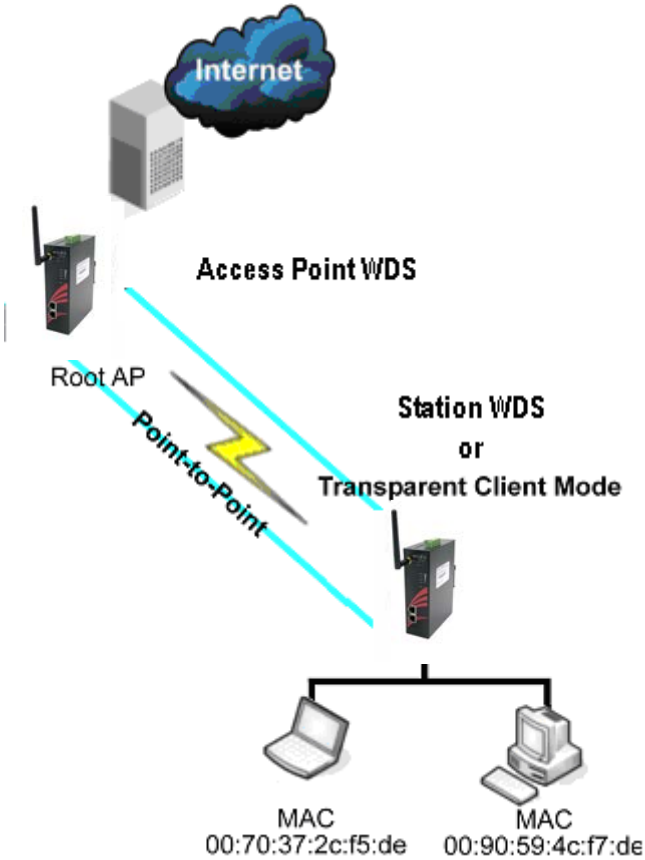


Station WDS Mode

Station WDS mode is similar to Station mode. The difference is Station WDS must connect to access point configured to Access Point WDS (or RootAP) mode. Station WDS is mainly use for point-to–point connection between 2 buildings or locations as far as several kilometer away.

Point-to-Point	Point-to-MultiPoint
An access point setup as Access Point WDS (or RootAP) and 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.



Repeater WDS Mode

Repeater WDS Mode to mainly to extend the wireless range and coverage of the wireless network allowing access and communications over places generally difficult for wireless clients to connect to the network.

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

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

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

Configure the IP Address

After setting up the hardware you need to assign an IP address to your PC so that it is in the same subnet as the access point.

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**.

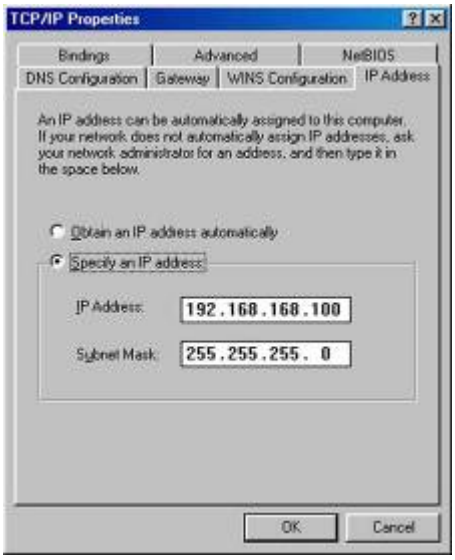
Step 3:

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**.

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

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.

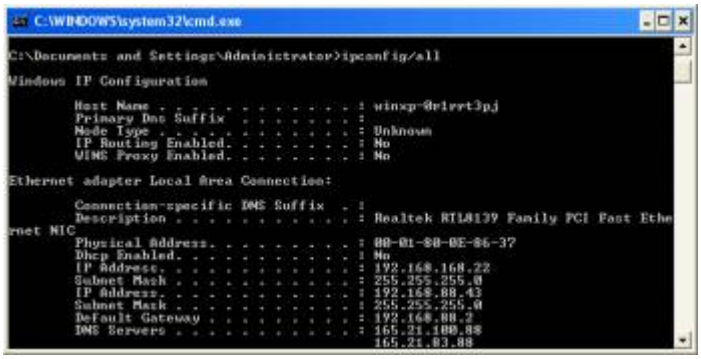
Set the IP address to 192.168.168.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 254.

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.

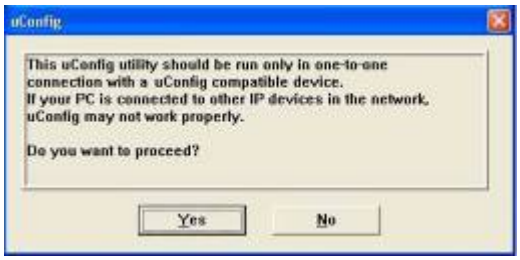
Access the Web Interface

Access with uConfig

The UConfig utility provides direct access to the web interface.

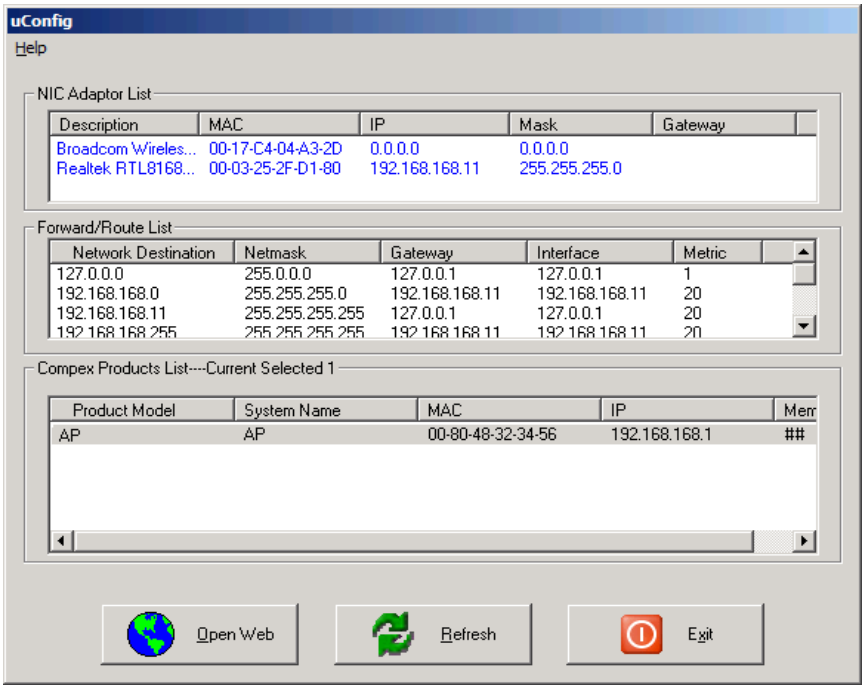
Step 1:

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.

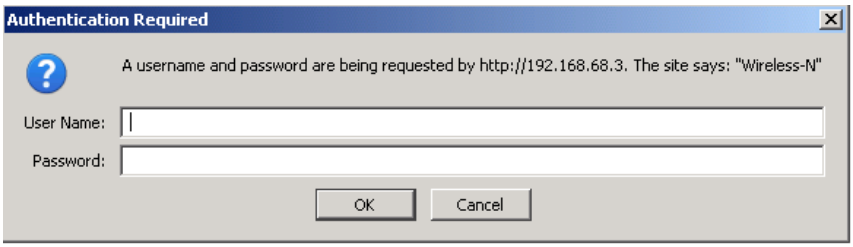


Step 3:

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.

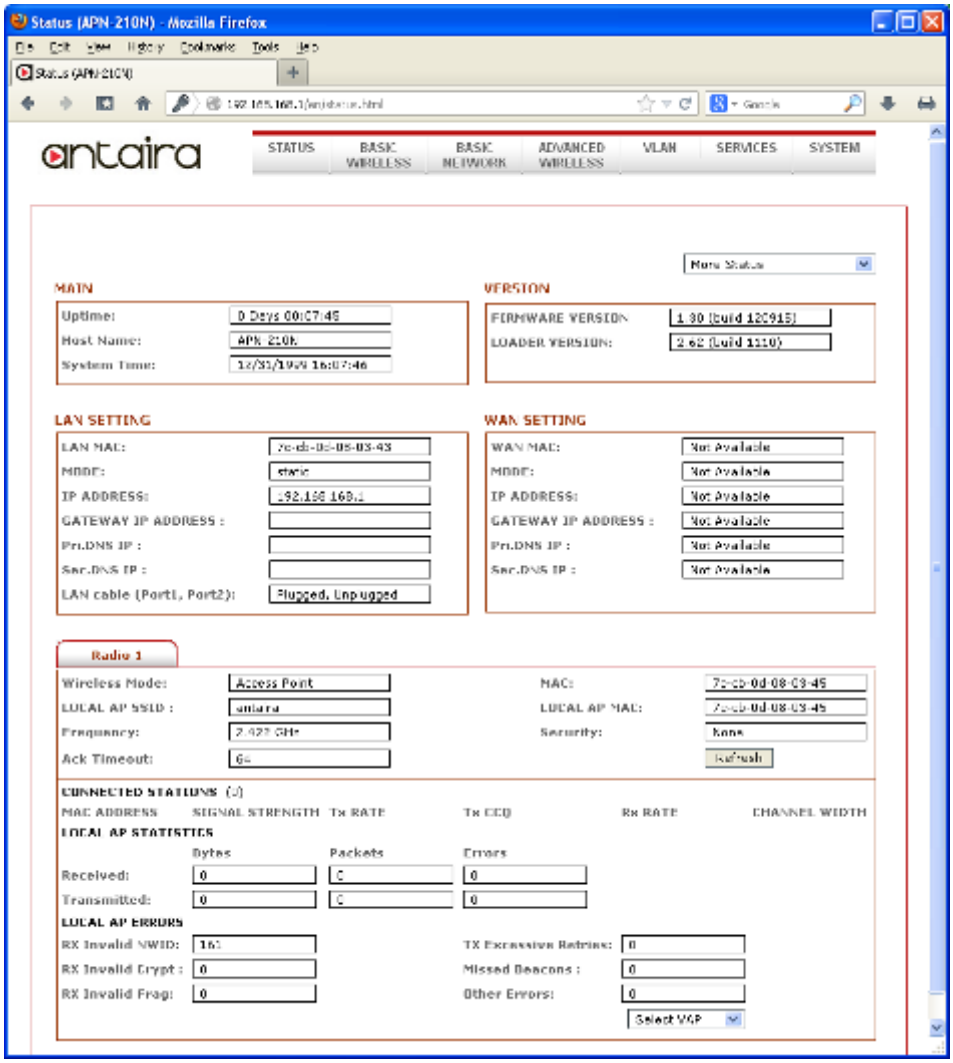
Step 4:

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 home page. The Status page.



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:

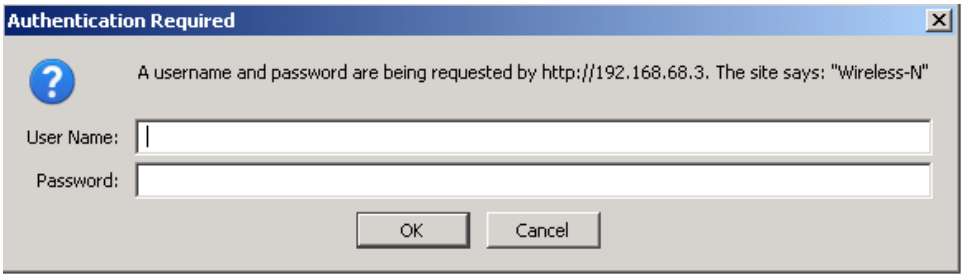
Open the **Connections** tab and in the **LAN Settings** section disable all the option boxes. Click on the **OK** button to update the changes.

Step 3:

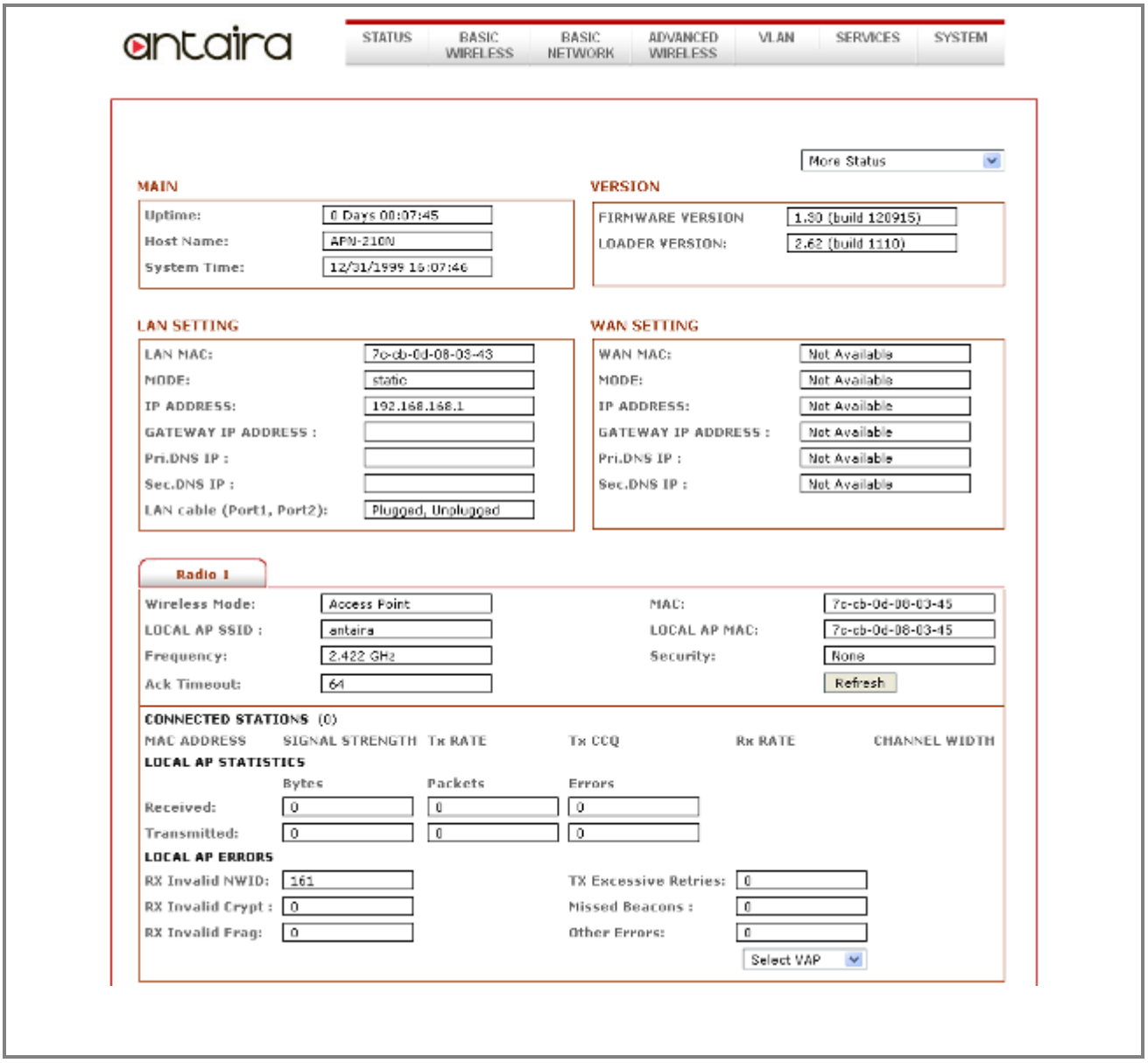
At the **Address** bar type in http://192.168.168.1 and press **Enter** on your keyboard.

Step 4:

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



It then opens the device home page. The Status page.


antaira
STATUS
BASIC WIRELESS
BASIC NETWORK
ADVANCED WIRELESS
VLAN
SERVICES
SYSTEM
More Status
MAIN
Uptime: 0 Days 00:07:45
Host Name: APN-210N
System Time: 12/31/1999 16:07:46
VERSION
FIRMWARE VERSION 1.30 (build 120915)
LOADER VERSION: 2.62 (build 1110)
LAN SETTING
LAN MAC: 7c-cb-0d-08-03-43
MODE: static
IP ADDRESS: 192.168.168.1
GATEWAY IP ADDRESS :
Pri.DNS IP :
Sec.DNS IP :
LAN cable (Port1, Port2): Plugged, Unplugged
WAN SETTING
WAN MAC: Not Available
MODE: Not Available
IP ADDRESS: Not Available
GATEWAY IP ADDRESS : Not Available
Pri.DNS IP : Not Available
Sec.DNS IP : Not Available
Radio 1
Wireless Mode: Access Point
LOCAL AP SSID : antaira
Frequency: 2.422 GHz
Ack Timeout: 64
MAC: 7c-cb-0d-08-03-45
LOCAL AP MAC: 7c-cb-0d-08-03-45
Security: None
Refresh
CONNECTED STATIONS (0)
MAC ADDRESS SIGNAL STRENGTH Tx RATE Tx CCQ Rx RATE CHANNEL WIDTH
LOCAL AP STATISTICS
Bytes Packets Errors
Received: 0 0 0
Transmitted: 0 0 0
LOCAL AP ERRORS
RX Invalid NWID: 161
RX Invalid Crypt : 0
RX Invalid Frag: 0
TX Excessive Retries: 0
Missed Beacons : 0
Other Errors: 0
Select VAP

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 for advanced wireless features. Advanced Network page settings for more details of these features.

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.

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

How to save changes

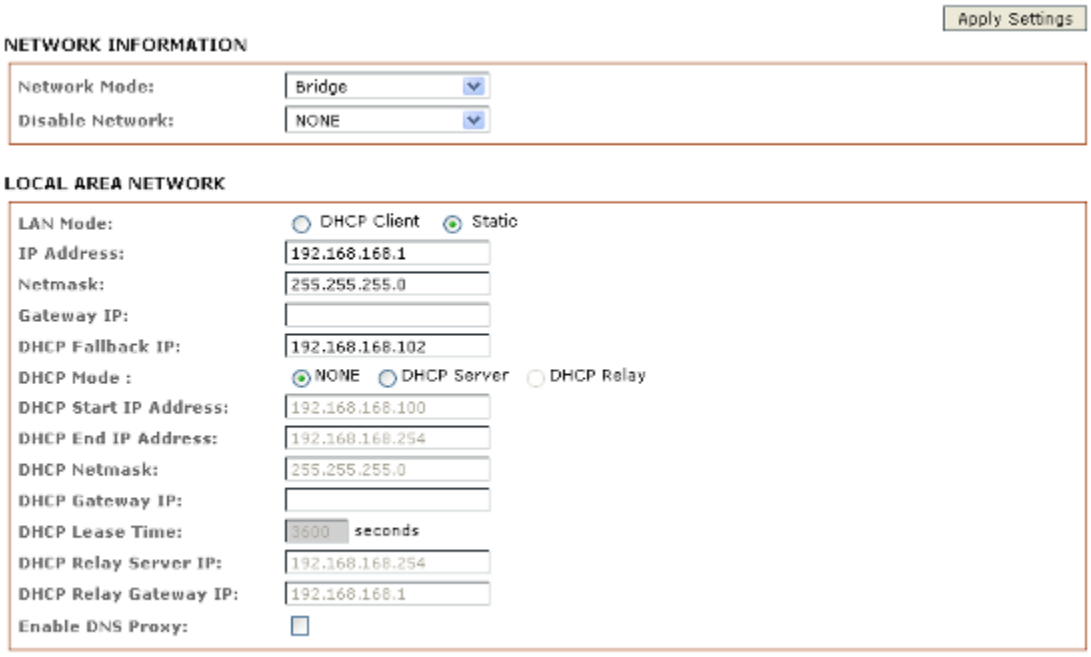
After made changes from each respective setup page, click this bu

Next the prompt below appear. You are asked to confirm if you want to save the change permanently to device flash.

Click **Save** will write all configuration changes to flash.
Click **Discard** will discard all changes made.
If not sure what changes were made earlier, recommend to discard and reconfigure again.

Basic Network Tab

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



Network Mode: Bridging

Network Mode:

Bridge mode (default)

LAN Setup

LAN Mode:

Static: (default) lets you enter a specific IP address for the device.

Default IP address is 192.168.168.1

DHCP Client: when set let device learn the IP address automatically from the network.

Netmask:

Let you 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 the device is connected.

Primary DNS IP: (optional)

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

Secondary DNS IP: (optional)

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

DHCP Mode:

None: function disabled

DHCP Server: Check to enable. Device act IP address distribution server automatically issue IP address and other network information to the DHCP Client request them.

DHCP Relay: check to enable. Enter the IP address of the remote DHCP server where the DHCP Client request will be relayed to.

DHCP Start IP Address:

Enter the starting IP address to be issue.

DHCP End IP Address:

Enter the last IP address the server will issue.

Netmask:

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

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

DHCP Lease Time: (default is **3600** seconds or 1hour)

Enter the new lease time in seconds.

DHCP Server Relay IP:

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

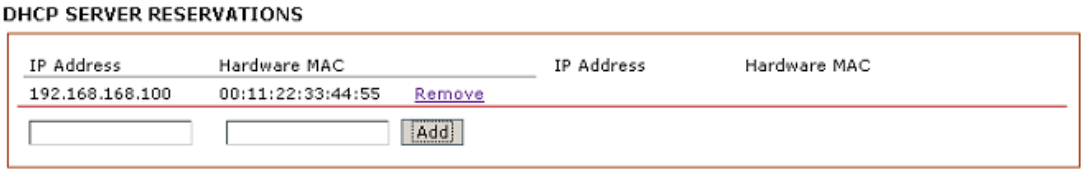
DHCP Gateway Relay IP:

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

Enable DNS Proxy:

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

DHCP Reservations



Click **Add** to enter for each device the IP address and MAC address.
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 addresses entry is for device operation to resolve domain name to reach certain servers like internet time server and other services that use domain name.
* Note:- Ensure device gateway IP is also set that to allow device to access to internet.

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

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

Bandwidth Control between Ethernet and Wireless

An entry of value “0” means no bandwidth flow limit between the 2 interfaces.
An entry of “2000” means 2000Kbit or 2Mbit limit traffic flow between the 2 interfaces.
Default is “0”

Basic Wireless Tab

Under the tab, there is the selection of 4 radios.

Fig 2.1 Basic Wireless Tab

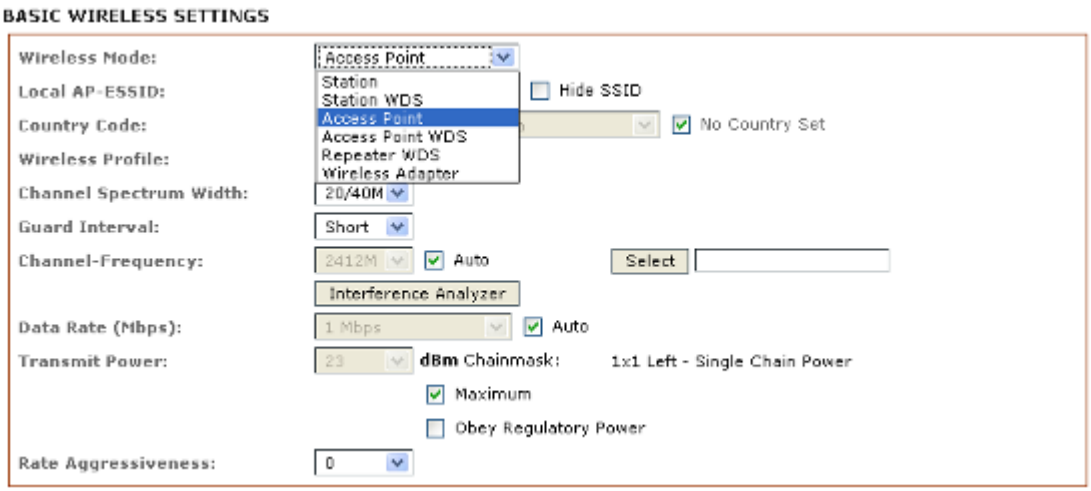
Currently device support only one 802.11n radio card. Select **RADIO 1** to configure. Basic Wireless Tab contains all the wireless setup, which is necessary for the operator to setup the wireless part of the link.

Basic Wireless Settings

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

Wireless Mode

There are **5 modes** available.



Access Point

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

Access Point WDS

This mode can be connected to Station WDS mode. Using WDS protocol, it

allows a client or station device to bridge wireless traffic transparently.

Station:

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

Station WDS:

WDS is the acronym of Wireless Distribution System. It can be connected to the **Access Point WDS** mode. It enables packet forwarding at 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.

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 as necessary.

***Note:- for Repeater WDS:**
ESSID must be the same for the Remote AP and the Local AP. The channels used Repeater to link to another Repeater will follow the Access Point WDS connection selected channel.

Access Point Parameters Settings

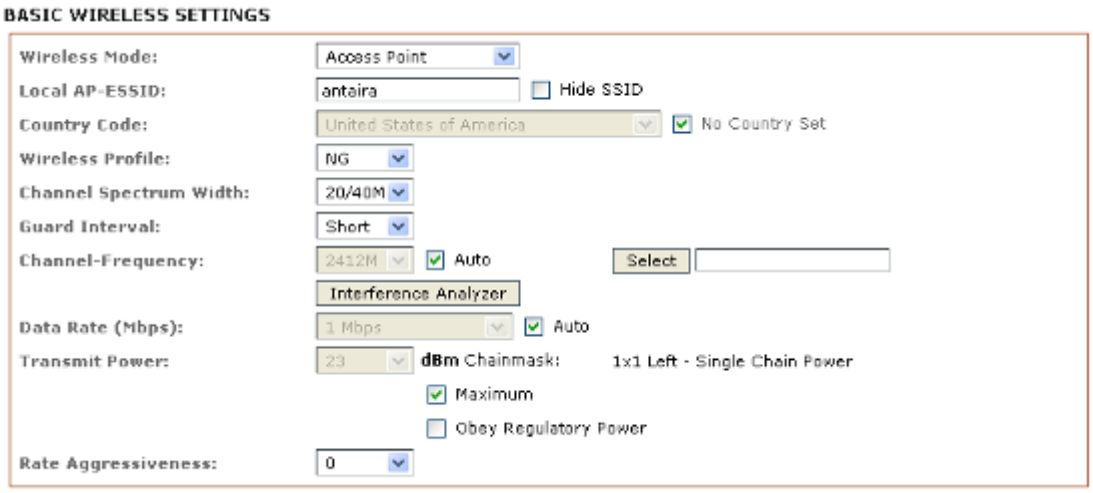


Fig 2.3 Basic Wireless Settings (Access Point/ Access Point WDS)

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 only.

Country Code

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

No Country Set*:*

Option when checked, only the frequency range are available.

11n 2.4GHz is 2412-2462MHz.

Wireless Profile:

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

Channel Spectrum Width

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

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

Channel – Frequency

This is frequency selection you can set for device to operate on. The frequency range available depends on the country domain you select in Country Code.

Auto*:* When checked, during startup, device automatically select 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.

6 – 54Mbps are Legacy Rates

MCS0 to MCS7 are 802.11n rates, which uses only 1 stream.

MCS8 to MCS15 are 802.11n rates, which uses 2 streams.

Auto*:* The data rate selected will follow an advanced rate algorithm that takes into

condition the amount of errors at the data rate and fine tune 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 if this new frequency have higher power output permitted by regulation, the power previously selected low power level will remains unchanged. You need to readjust the power level to in order to take advantage higher output power available for the channel

.

Rate Aggressiveness

Allows user to reduce or increase transmit rate while still remain in Fully Auto Algorithm. There are 2 scenarios that Rate Aggressiveness is useful. Environment might be noisy at times. Lower the throughput will ensure better stability. Rate Aggressiveness allows device to reduce the transmit rate, so range or power can be higher.

Choose a range of value from -3, -2, -1 Environment might be free of interference. But the fully auto algorithm might give low throughput. Increase Rate Aggressiveness will increase transmit rate in this case to get higher throughput. Choose a range of value from +3, +2, +1.

Station Parameters Settings

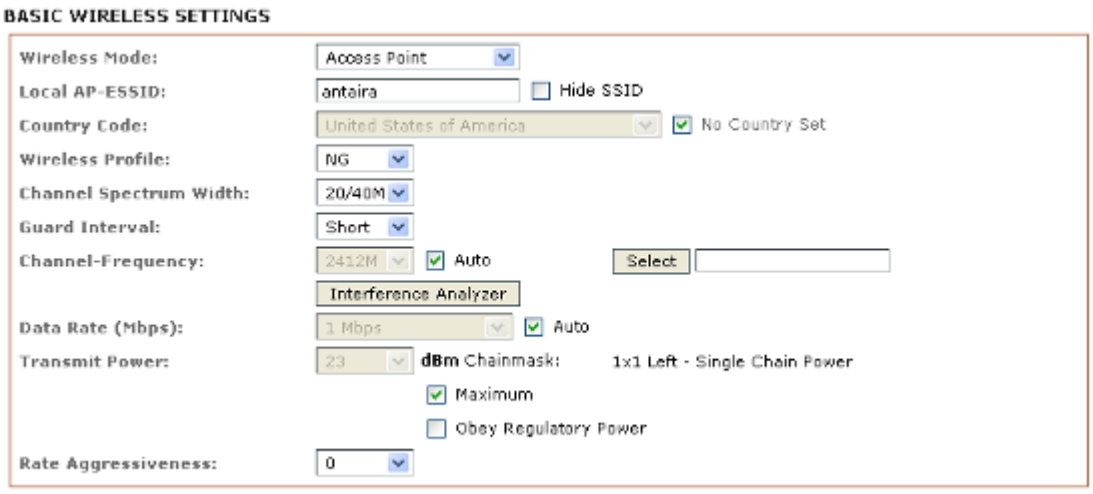


Fig 2.4 Basic Wireless Settings (Station/Station WDS)

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

Wireless Mode: Station

Remote AP-ESSID

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

Site Survey

Site Survey will search for the available wireless networks in range on all the supported channels and will allow you to select one for association. In case the selected network uses encryption, you'll need to set security parameters in 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. Site Survey channel scan list can be modified using the Channel Scan List control.

Remote AP – Lock to MAC

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

Remote AP - Preferred MAC

Enter the preferred MAC address of the access point you want device to connect when it first startup. Up to max of 4 MAC addresses can be entered. Priority is from top to bottom. In the event all preferred MAC addresses are not available, device will then pick the matching SSID access point with the strongest signal.

Country Code

Different countries have different power levels and also frequency selections. To ensure device operation follows regulatory compliance rules, the operator should make sure that correct country code where device will be used, is selected. The channel list, output power limits, IEEE 802.11 and Channel Spectrum Width modes will be tuned according to the regulations of the selected country. **Station setting must match AP country code setting.**

No Country Set*:*

Option when checked, only the frequency range are available.
11n 2.4GHz is 2412-2462MHz.

Wireless Profile:

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

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

Channel Spectrum Width

20M represents the data transmitted at a bandwidth of 20MHz. 20/40MHz represents the data transmitted at either 20MHz or 40MHz. In very noisy environment it automatically fall back to 20MHz to be more resilient to the interference. In situation when auto fall back did not happened, manually changing channel spectrum width to

20MHz will to help reduce interference on the link and improve performance.

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

** **Station setting must match AP Channel Spectrum Width setting.**

Maximum : checking this box will result in maximum Tx output power overriding regulation.
Obey Regulatory Power : checking this box will obey Tx output regulatory power by country.

Channel Scan List

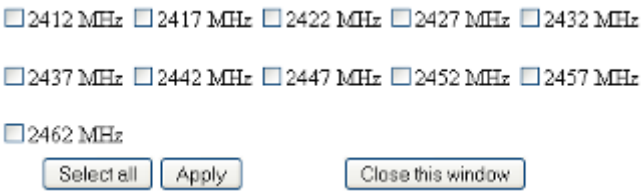


Fig 2.5 Channel Scan List (In US Country Code)

According to the availability of channels in the country codes, the operator can select which channels to be scanned when scanning for an Access Point. Then the scanned channels will appear on the Site Survey.

Wireless Security

All the wireless security settings are set under this section.
The operation of the Keys is the same for ALL the Wireless modes.

WPA or WPA2 Authentication

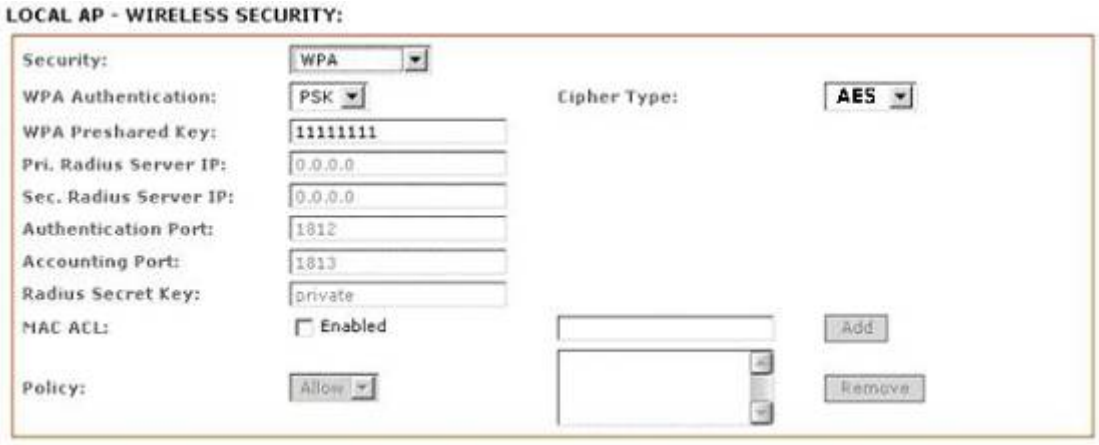


Fig 2.7 WPA (Access Point/Access Point WDS/Repeater WDS)

WPA PSK

PSK (Default) – WPA or WPA2 with Pre-shared Key method.

Cipher Type

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

AES - Advanced Encryption Standard (AES) algorithm.

AUTO (Default) – Automatically select between both algorithms.

Preshared Key

This option is available when **WPA** or **WPA2**, with **PSK** selected.

The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

***** Important:**

802.11n network using WPA authentication should use AES cipher type for connection. Only AES allows highest transmission speed and throughput operation.

Using TKIP cipher type device will limit maximum transmission speed of up to 54Mbps only.

WPA + EAP

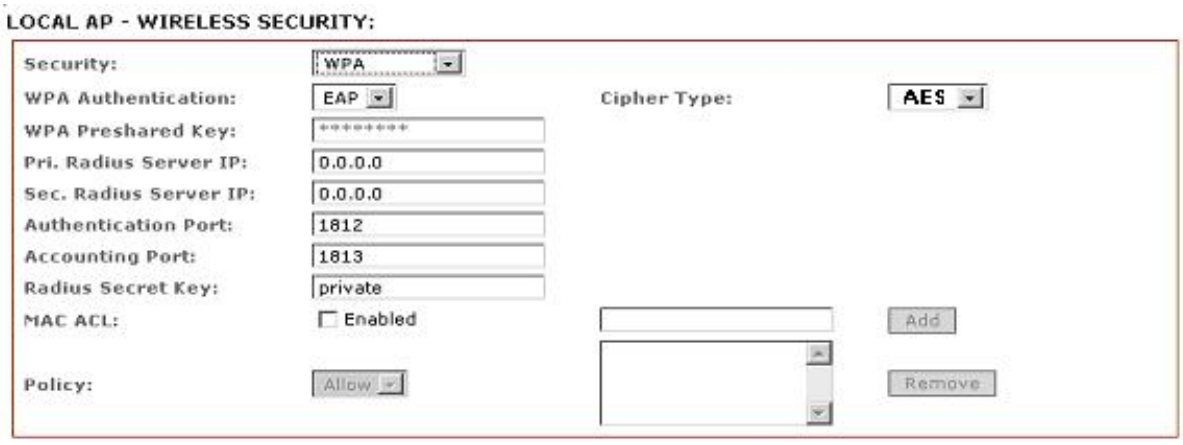


Fig 2.8 WPA + EAP

EAP – WPA or WPA2 with EAP (Extensible Authentication Protocol)

Firmware supported options for clients are: EAP-TTLS and EAP-PEAP

Cipher Type

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

AES - Advanced Encryption Standard (AES) algorithm.

AUTO (Default) – Automatically select 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. Default is 1812.

Accounting Port

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

Radius Secret Key

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

WPA EAP-TTLS and WPA EAP-PEAP

Fig 2.8 WPA (Station /Station WDS/Repeater WDS)

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

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 unencrypted form.

User Password:

Password credential used by the wpa-supplicant for EAP authentication

IEEE802.1x Settings

The operation of the Keys is the same for ALL the modes.

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

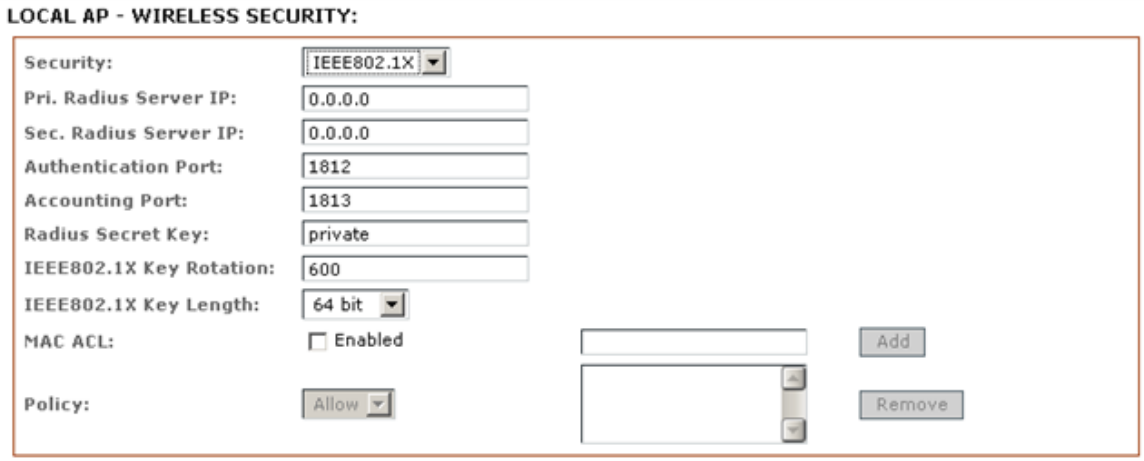


Fig. 2.8 IEEE802.1X (Access Point/Access Point WDS/ Repeater WDS)

This option apply to the following modes only, when WPA EAP or IEEE802.1x .

Access Point, Access Point WDS, Repeater WDS modes

Primary Radius Server IP

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

Secondary Radius Server IP

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

Authentication Port

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

Accounting Port

Enter Radius server Accounting Port to use. Default is 1813.

Radius Secret Key

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

IEEE802.1x Key Rotation

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

IEEE802.1x Key Length

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

WEP

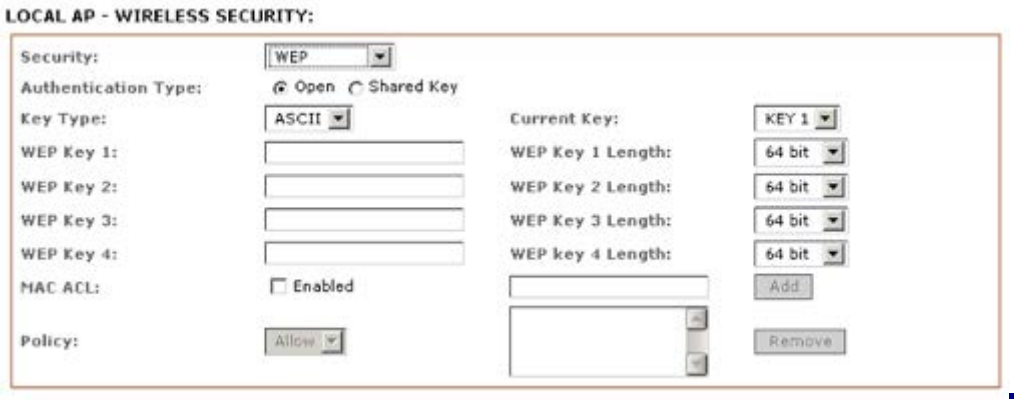


Fig 2.6 WEP

The operation of the Keys is the same for ALL the modes.

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

Authentication Type:

Open Authentication – (Default) No authentication. Recommend to use this standard option over shared authentication.

Shared Authentication – May not be compatible with all Access Point. 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. 4 different WEP keys can be configured at the same time, but only one is used.

WEP Key:

WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used.

WEP Key Length:

64-bit (selected by default) or 128-bit WEP Key length should be selected if WEP security method is used. The 128-bit option will provide higher level of security.

For **64-bi**t – specify WEP key as 5 HEX (0-9, A-F or a-f) pairs (e.g. 00112233AA) or 5 ASCII characters.

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

Virtual Access Point (VAP)

Virtual AP (VAP) implements mSSID (Multi-SSID) whereby a single wireless card can be setup with up to 3 virtual SSID of BSSID connections. Each VAP can be set with different security authentication mode.

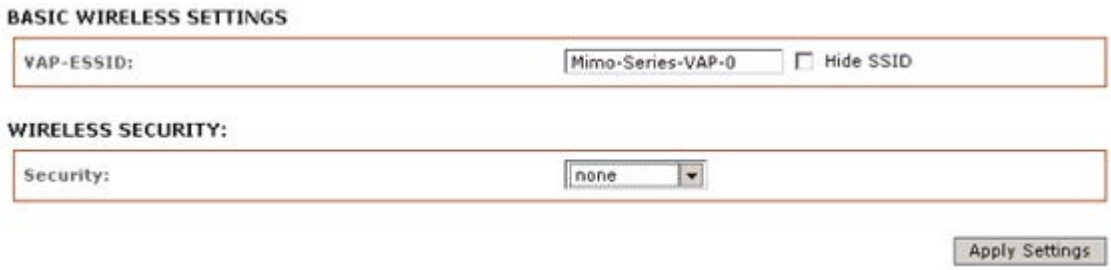


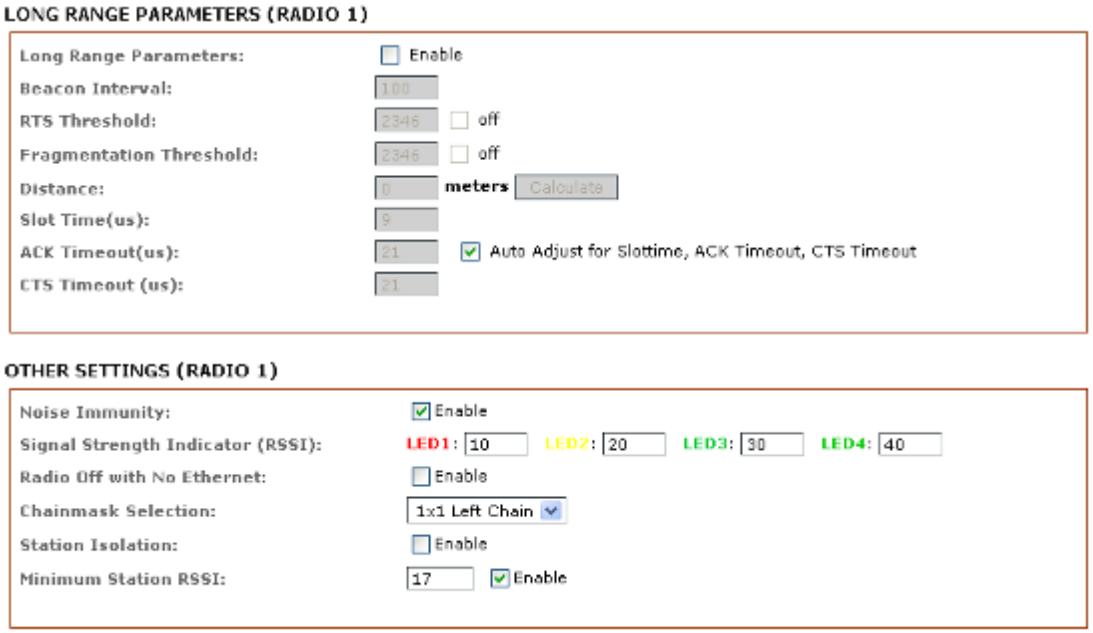
Fig 2.11 Virtual AP (Only Available in Access Point/ Access Point WDS Mode)

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

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

Advance Wireless Tab

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



Long Range Parameters Setup

Advanced wireless page let you setup outdoor long distant connection parameters.

Long Range Parameters:

Check to enable parameters.

Beacon Interval: (default is 100 ms)

Define the time interval (in millisecond) the beacon to broadcast.

Recommend to use default.

RTS Threshold: (Default is **OFF**)

Fragmentation Threshold: (Default is **OFF**)

Distance:

Enter the distant in meters the device is to connect with the opposite device. Then click **Calculate.** The close approximate values for Slot Time, ACK Timeout, CTS Timeout will be calculated. Fine tuning can be further adjusted for the best environment conditions to achieve best performance and better link reliability.

Noise Immunity:

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

Signal Strength Indicator (RSSI):

The default values are LED1-Red (10), LED2-Yellow (20), LED3-Green (40)
Each LEDs when turn on indicates the RSSI signal strength has hit over the value.
e.g. When LED1 and LED2 light up it indicate the RSSI is greater than 20.
When all 4 LEDs light up it indicate RSSI is greater than 40.
For long distant installation when signal strength expected to be about 20-30, the values can be
adjusted to display over this new range.
e.g. the LEDs values can be adjusted as follows:

LED1 (RSSI value=7)
LED2 (RSSI value=15)
LED3 (RSSI value=22)
LED4 (RSSI value=27)

Station Isolation :

When checked, prevent wireless clients on same AP from discovering other clients.

Chainmask Selection :

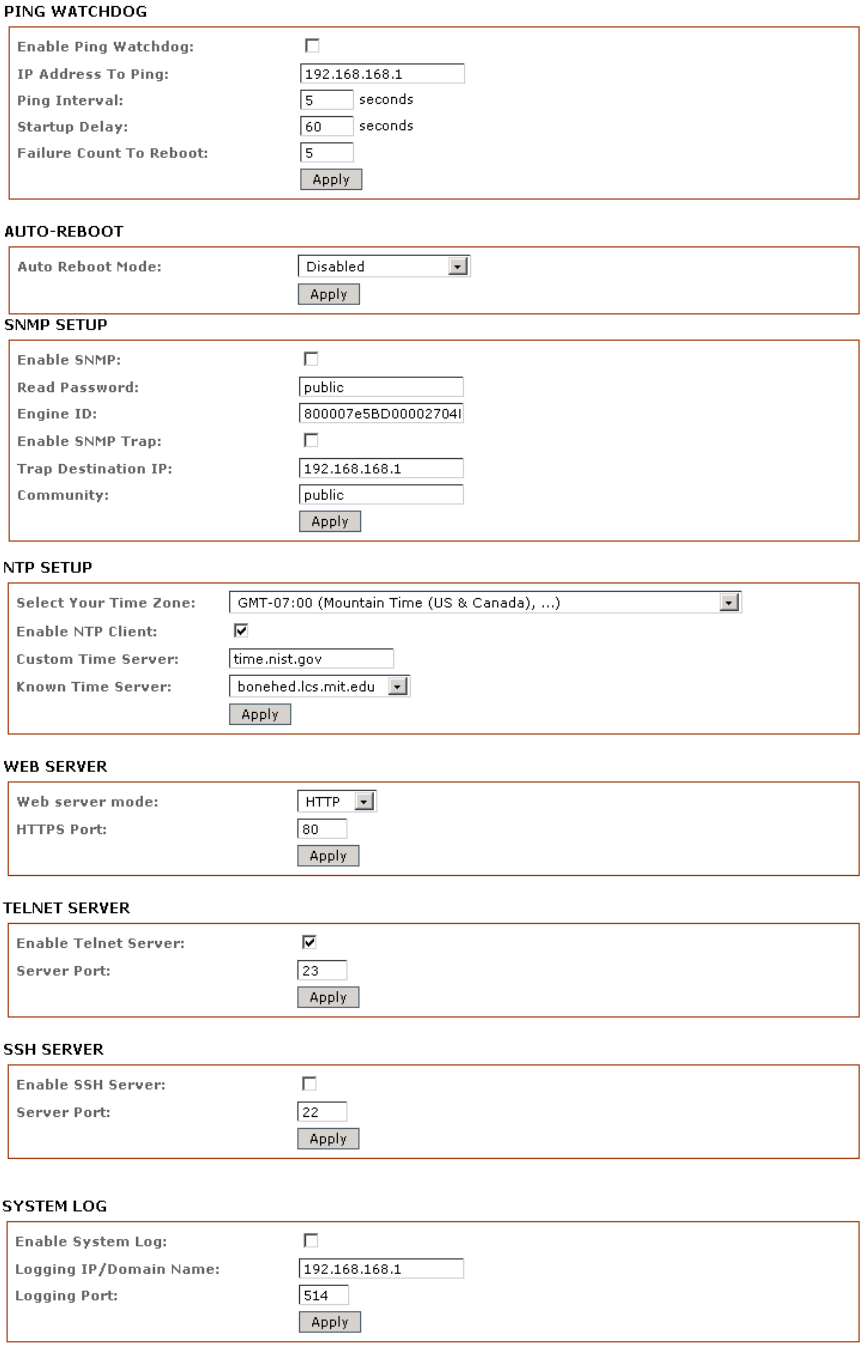
Available is: **1x1 Left Chain**

1x1 Left Chain radio card to operate with 1transmit and 1 receive stream and both transmit /receive on the left port of radio card only.

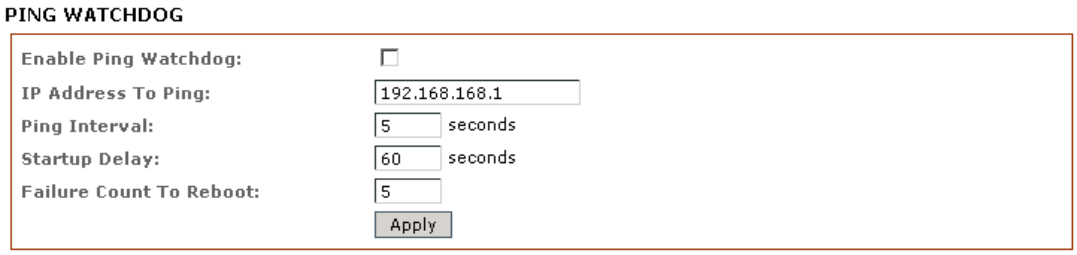
Services Tab

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

Services section provides varieties of useful and enhanced functions to help assist device operations.



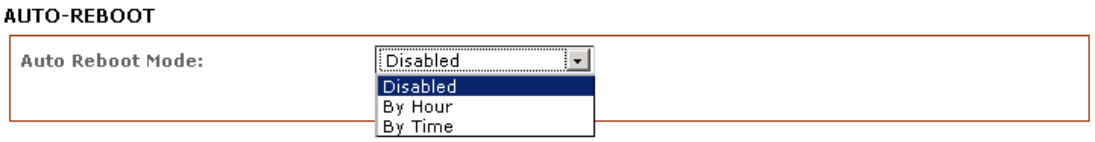
Ping Watchdog



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

IP Address To Ping: Target IP address do ping test monitor.
Ping Interval: Default is 5 seconds (minimum). This is Ping test duration.
Startup Delay: Default is 60 seconds(minimum).
One time delay after device startup.
Failed Count To Reboot: Default is 5. This is the number of ping failure count before device kick in the reboot process.

Auto-Reboot

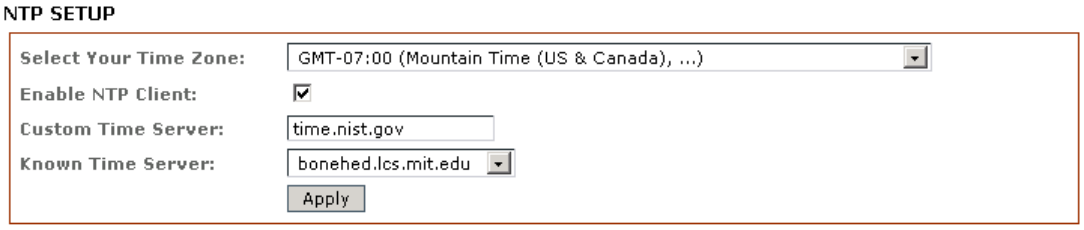


Auto-Reboot Mode: Default is disabled. Select By Hour or By Time check.
This mode lets you preset a timer to automatically force a reboot.
Timer can in fixed number of hours or at a specified time of day.
By Hour: Enter the number of hours device need to run before kick start reboot process.
By Time: Enter the specific time of day in hh:mm (24-hour format) to kick start reboots process.

SNMP Setup

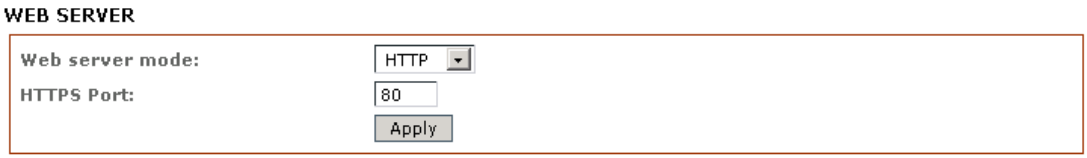
Enable SNMP: Default is disabled. Check on box to enable.
Read Only Password: Password to query device.
Engine ID: Default is 800007e5BD00002704D000007c
Enable SNMP Trap: Default is disabled. Check on box to enable.
Trap Destination IP: Enter the IP to send the info when trap is triggered.
Community: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

NTP Setup



Enable NTP Client: Default is disabled. Check on box to enable.
Select Your Time Zone: Select from list the country you reside.
Custom Time Server: Default is “time.nist.gov“ Enter preferred time server domain/IP
Known Time Server: You can also select one from this list as your new time server.

Web HTTP Security



Web Server Mode: Default is HTTP. Option is HTTP and HTTPs
HTTP(s) Port: Default is 80 for HTTP and 413 for HTTPs.
Enter a new preferred port number.

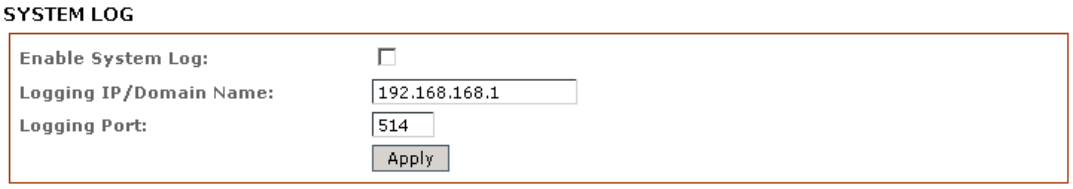
Telnet Access Setup

Enable Telnet Server: Default is enabled. Remove check on box to disable.
Server Port: Default is 23. Enter new preferred port number.

SSH Access Setup

Enable SSH Server: Default is disabled. Check on box to enable.
Server Port: Default is 22. Enter new preferred port number.

System Log Setup

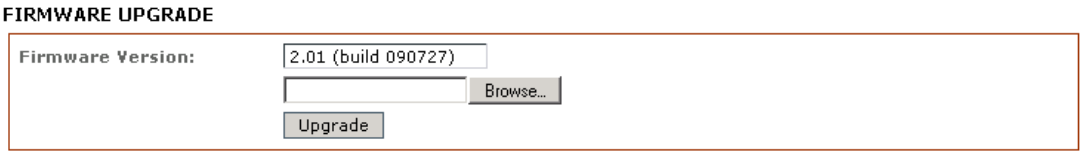


Enable System Logging: Default is disabled. Check on box to enable.
Logging IP /Domain Name: Enter destination IP address of device to receive log.
Logging Port: Default is 514. Enter the new preferred port number.

System Tab

The System Page contains Administrative options. This page enables 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.

Firmware Upgrade



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

Firmware version: displays the version of the current firmware of the device system.

Upgrade: button opens the Firmware Upload window if activated.

Current Firmware: displays the version of the device firmware which is currently operating.

Firmware File: activate Browse button to navigate to and select the new firmware file. The full path to the new firmware file location can be specified there. New firmware file is transferred to the system after Upload button is activated.

Close this window – button cancels the new firmware upload process if activated.

Upgrade button should be activated in order to proceed with 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 backup the system configuration and the Support Info file before uploading the new configuration.

Close this window – button closes the firmware upgrade window if activated.
This action will not cancel the firmware upgrade process.

Host Name

Host Name is the system wide device identifier. It is reported by SNMP Agent to authorized management stations. Host Name will be represented in popular Router Operating Systems registration screens and discovery tools.
Host Name: specifies the system identity.
Change button saves the Host Name if activated.

Administrative and Read-only Account

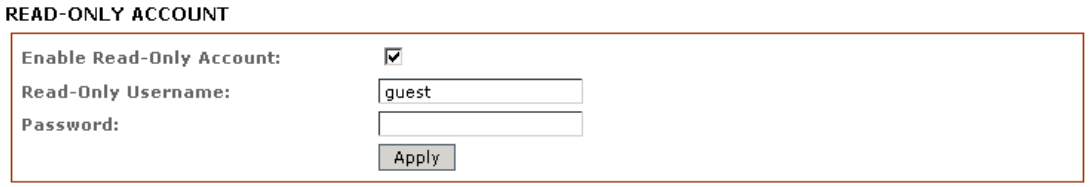
In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first system setup:
Administrator Username: specifies the name of the system user.
Current Password: administrator is required to enter a current password. It is required for Password or Administrator Username change routine.

Default administrator login credentials:

- User Name: **admin**
- Password: **password**

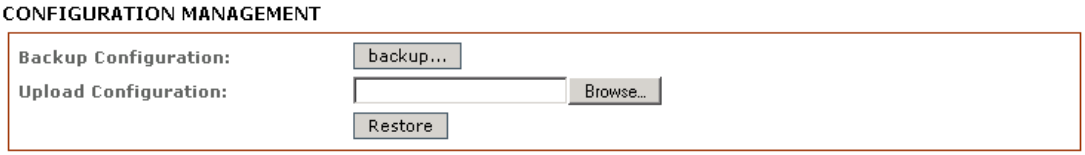
New Password: new password used for administrator authentication should be specified.
Verify Password: new password should be re-entered to verify its accuracy.
Click Change button to save the changes.

Enable Read-Only Account



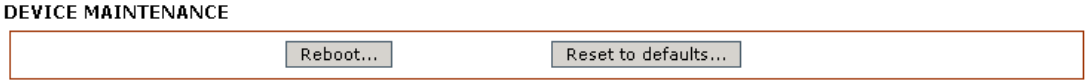
Read-Only Username
Password: new password used for read-only administrator authentication should be specified.

Configuration Management



Backup Configuration: click Download button to export the current configuration to a file.
Upload Configuration: click 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 new configuration file to the system.
New configuration will be effective after the Apply button is activated and system reboot cycle is completed. Previous system configuration is deleted after Apply button is activated. It is highly recommended to backup the system configuration before uploading the new configuration.
Use only configuration backups of the same type device - configuration backed up from PowerStation2 suits only PowerStation2, but not LiteStation2 or LiteStation5! Behavior may be unpredictable when mixing configurations from different type devices.

Device Maintenance



The controls in this section are dedicated for the device maintenance routines: rebooting, resetting, generating of the support information report.

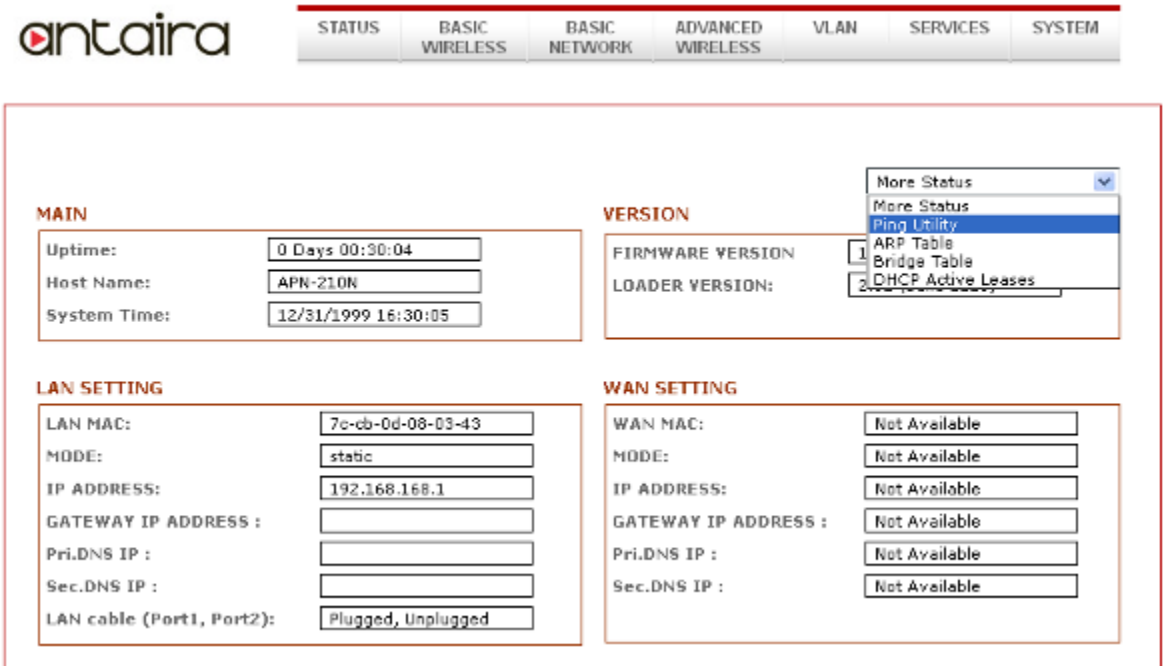
Reboot: activate Reboot control in order to initiate full reboot cycle of the device. Reboot effect is the same as the hardware reboot which is similar to the power off - power on cycle. The system configuration is not modified after the reboot cycle completes. Any non-applied changes will be lost.

Reset to Defaults: activate Reset to Defaults control in order to initiate reset the device

to factory defaults routine. Reset routine initiates 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 system 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 backup the system configuration before the Reset to Defaults is initiated.

Status Page



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

Status Reporting

Main

Uptime: displays device up time since boot up. The time is expressed in days, hours, minutes and seconds.
Host Name: displays the assigned device host name (ID).

System Time: display device current date and time. Accurate system date and time is retrieved from the internet services using NTP (Network Time Protocol) if device is setup and connected to internet. Otherwise, the date and time update from device own 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 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

Not available in APN-210N units

Radio

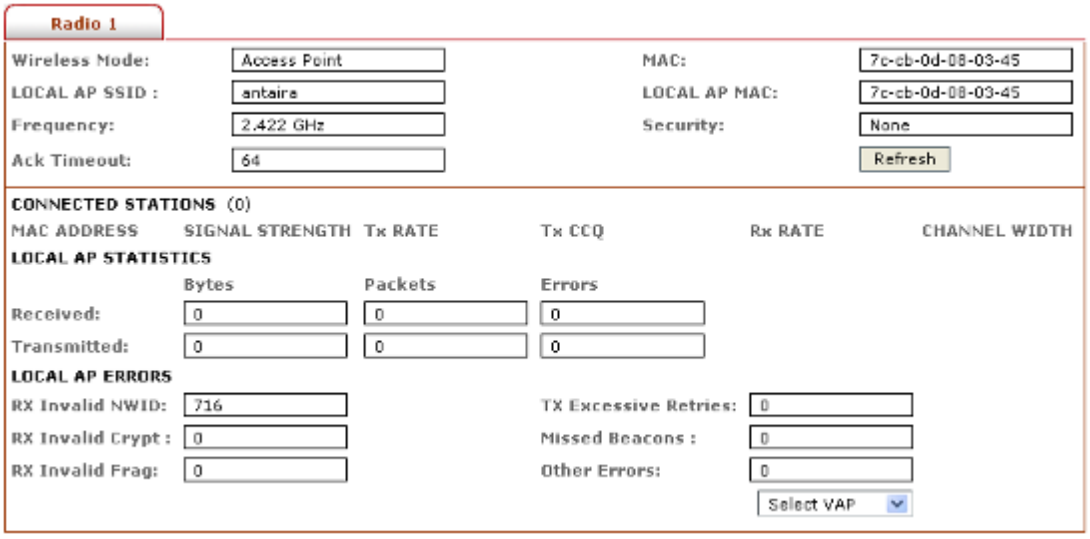
Wireless Mode: displays the current operating mode of the device.
Local AP SSID: displays the current SSID (Service Set Identifier) of device when operates in access point mode.
Frequency: displays current operating frequency running in device.
WLAN MAC: displays the MAC address or BSSID of the current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

Clients Connection Status in AP Status Info

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

Below is an example of a client's connection status info.

Click Refresh to refresh client connection statistics and status page

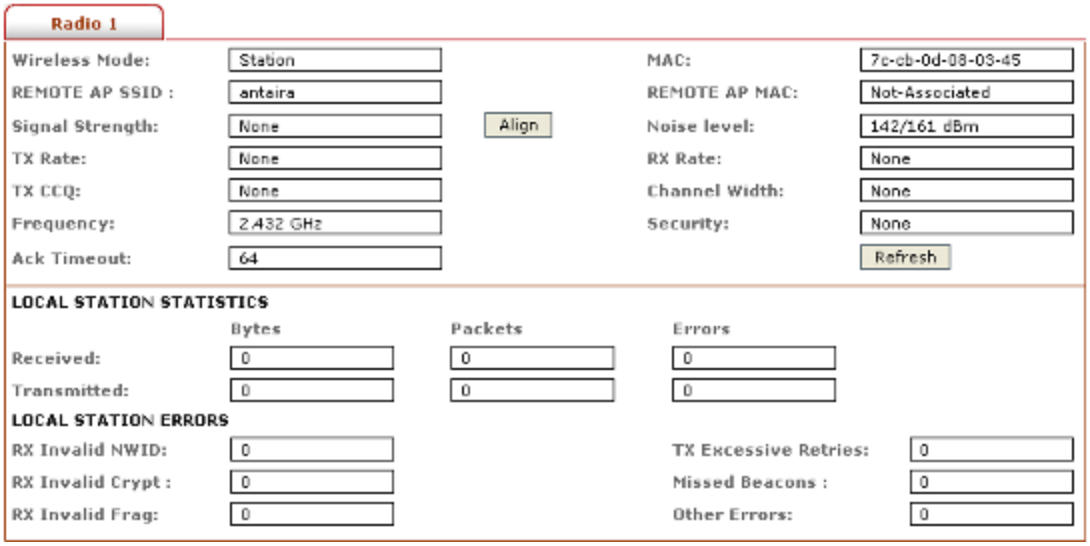


Signals strength at the left and right port of radio card can be view with more accurately while adjusting the antenna to get a more balanced reception.

Station Connection Info

Status Info

Click Refresh to refresh client connection statistics and status page.



WLAN Connected Status:

MAC Address: displays the MAC address of the current active WLAN card.

Signal Strength: displays the received wireless signal level of 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.

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 the connection;

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

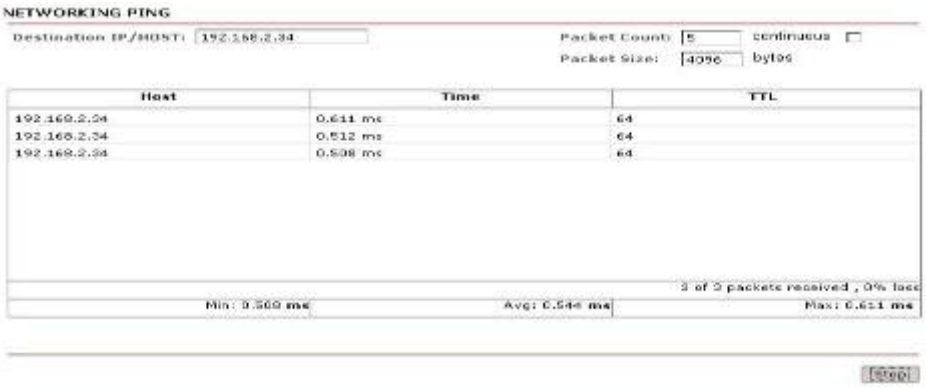
Missed beacons value represents the number beacons (management packets sent at regular intervals by the Access Point) which were missed by the client. This can indicate that the wireless client is out of range.

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

More Status

In More Status option contains some useful tools and additional status pages.

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



ARP Table display a list of MAC addresses of the connected devices

ARP TABLE

IP address	HW type	Flags	HW address	Mask	Device
192.168.168.190	0x1	0x2	00:21:9B:10:6A:78	*	br0

Bridge Table display a list the devices connect to the bridge interface

BRIDGE TABLE

Port No	Mac Address	Is Local	Agein Timer
1	00:06:b1:08:ff:e8	no	25.18
1	00:12:3f:a4:4b:6d	no	119.57
1	00:13:20:5d:1d:fa	no	8.29
1	00:13:20:67:d5:d8	no	8.29
1	00:13:d4:2f:68:26	no	64.97
1	00:16:76:b7:5d:52	no	1.80
1	00:1a:a0:8e:dc:7b	no	30.66
1	00:21:9b:10:6a:78	no	0.12
1	00:24:e8:11:95:e5	no	28.87
1	02:01:00:00:00:00	no	0.44

DHCP Active Lease Table display a list of IPs addresses leased to all computers.

DHCP ACTIVE LEASES

HOST NAME	IP ADDRESS	HARDWARE MAC	LEASE EXPIRED TIME
STATION-4	192.160.00.214	00-00-48-15-5D-E1	FRI DEC 31 17:03:32 1999

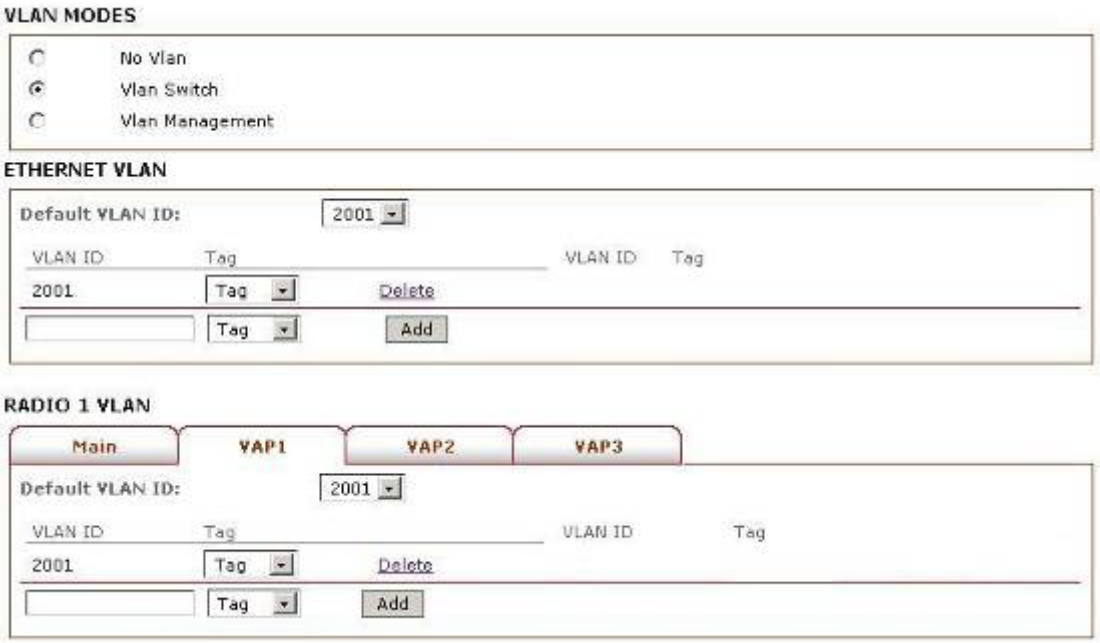
Close

VLAN Tab

This setup lets you create virtual local network connection through the device Ethernet only and over wireless connections.
By default **VLAN** mode is disabled and checked on **No VLAN**

VLAN Switch

To setup VLAN network check on **VLAN Switch**



To add a Tag VLAN ID for 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 device interface port can cause lost of connection to device 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 device. If this happened, use the device Reset button to clear the config and reconfigure. Refer Reset button operations section.

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

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

Example:
Assuming there are 2 VLAN ID groups, 2001 and 2002 setup in AP device.
One entry in VLAN Management has VLAN ID 2001 with masquerade IP address 192.168.168.20
Another entry in VLAN Management has VLAN ID 2002 with masquerade IP address 192.168.168.10
You can only select one of the 2 entries to be the active VLAN ID and IP address.
If VLAN ID 2001 group is selected, then 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 other ID group say, VLAN ID 2002, mark the radio button under Management IP, then click Apply and Saved.

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

Appendix I - Network

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

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

Network Mode Selections

Network Mode: 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 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 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.

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 efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment which has the same IP address space. WLAN and LAN interfaces form the virtual bridge interface while acting as the bridge ports. The bridge has assigned IP settings for management purposes:

Bridge IP Address:
The device can be set for static IP or can be set to obtain an IP address from the 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 by 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 Static Bridge IP Address mode is selected. This IP will be used for the device management purposes.
IP Address and Netmask settings should consist with the address space of the network

segment where device resides. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space, the device will become unreachable.

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

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

Primary/Secondary DNS IP:

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

Primary DNS server IP address should be specified for the device management purposes. 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 network and 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 as there is no sense for the bridge to participate in the Spanning Tree Protocol in this case.

Bridge mode Firewall Configuration Settings

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

Firewall entries can be specified by using the following criteria: Interface the interface (WLAN or LAN) where filtering of the incoming/passing-through packets is processed; IP Type sets which particular L3 protocol type (ICMP, TCP, and UDP) should be filtered; Source IP/mask is the source IP of the packet (specified within the packet header), usually

it is the IP of the host system which sends the packets; Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is 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), usually it is 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), usually it is the port of the host system application which the packet is addressed to.
Comments is the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.
On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in system configuration file, however only the enabled firewall entries will be active during the system operation.

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

Appendix II- Advanced Settings

This section provides more detail explanation on advanced setting for routing and wireless settings.
The Advanced options page allows you to manage advanced settings that influence on the device performance and behavior. The advanced wireless settings are dedicated for more technically advanced users who have a sufficient knowledge about wireless LAN technology. These settings should not be changed unless you know what effect the changes will have on your device.

Advanced Wireless Setting

The 802.11a/g data rates include 6, 9, 12, 18, 24, 36, 48, 54Mbps.
The 802.11n data rates are the MCS (Modulation Coding Scheme) rates.

MCS0 to MCS7 are 802.11n rates, which 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 as generally lower data rates are more immune to noise while higher rates are less immune, but are capable of higher throughput.

Rate Aggressiveness:

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

Noise Immunity option 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: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or 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. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately. System uses Request to Send/Clear to Send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending a RTS frame first while data is send only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS which provides clear media for the requesting station to send the data. CTS collision control management has time interval defined

during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.
Fragmentation Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or 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. Because of sending smaller frames, collisions are much less likely to occur. However lower values of the Fragmentation Threshold will result lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

Station Isolation: This option allows packets only to be sent from the external network to the CPE and vice verse (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 layer 2 (MAC) and layer 3 (IP) level. This is effective for the associated stations and WDS peers also.

Acknowledgement Timeout

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

Distance: specify the distance value in miles (or kilometers) using slider or enter the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.
ACK Timeout: specify the ACK Timeout. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set timeout it re-sends the frame. The performance drops because of the too many data frames are re-send, thus if the timeout is set too short or too long, it will result poor connection and throughput performance.
Changing the ACK Timeout"== value will change the Distance to the appropriate distance value for the ACK Timeout.
Auto: Adjust control and enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm described above. It is not recommended to use Auto Adjust option for long range links if the signal level is low or the high level of interference is present.
If two or more stations are located at the considerably different distance from the Access Point, the highest ACK Timeout for the farthest station should be set at the AP side. It is not recommended to use Auto Adjust option for Point-to-Multipoint connections as it will not warrant highest network performance in all the use cases.

Signal Strength LED Settings

LED Thresholds Configuration

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

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

LED 1 (Red) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 2 (Yellow) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 3 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 4 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.

Configuration example: if the Signal Strength fluctuates around RSSI 15-30, the LED Thresholds can be adjusted to the RSSI values 15, 20, 25, 30.

Appendix III- Services

This section provides more details on the system management services.

Ping WatchDog

The ping watchdog sets the device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the device will automatically reboot. This option creates a kind of "fail-proof" mechanism.
Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the device.

Enable Ping Watchdog: control will enable Ping Watchdog Tool.
IP Address To Ping: enter the target host IP address to monitor.
Ping Interval: specify time interval (in seconds) between to send the ICMP “echo requests”.
Startup Delay: specify initial time delay (in seconds) from device startup or reboot to start sending 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 received continuously, the Ping Watchdog Tool will reboot the device.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. Device contains an SNMP agent which allows it to communicate to SNMP manage applications for network provisioning.
SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of management information between network devices). SNMP Agent allows network administrators to monitor network performance, find and solve network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

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

Contact: specify the identity or contact in case an emergency situation arise.
Location: specify the physical location of the device.

NTP Client, Web, Telnet, SSH Server

NTP Client: The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the device system time. System Time is reported next to the every System Log entry while registering system events if Log option is enabled.
Web Server: the following the device Web Server parameters can be set there:
Use Secure Connection (HTTPS): If checked 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 the device Telnet Server parameters can be set there:
Enable Telnet Server: Enables Telnet access to the device.
Server Port: Telnet service TCP/IP port setting.

SSH Server: the following the device SSH Server parameters can be set there:
Enable SSH Server: Enables SSH access to the device.
Server Port: SSH service TCP/IP port setting.

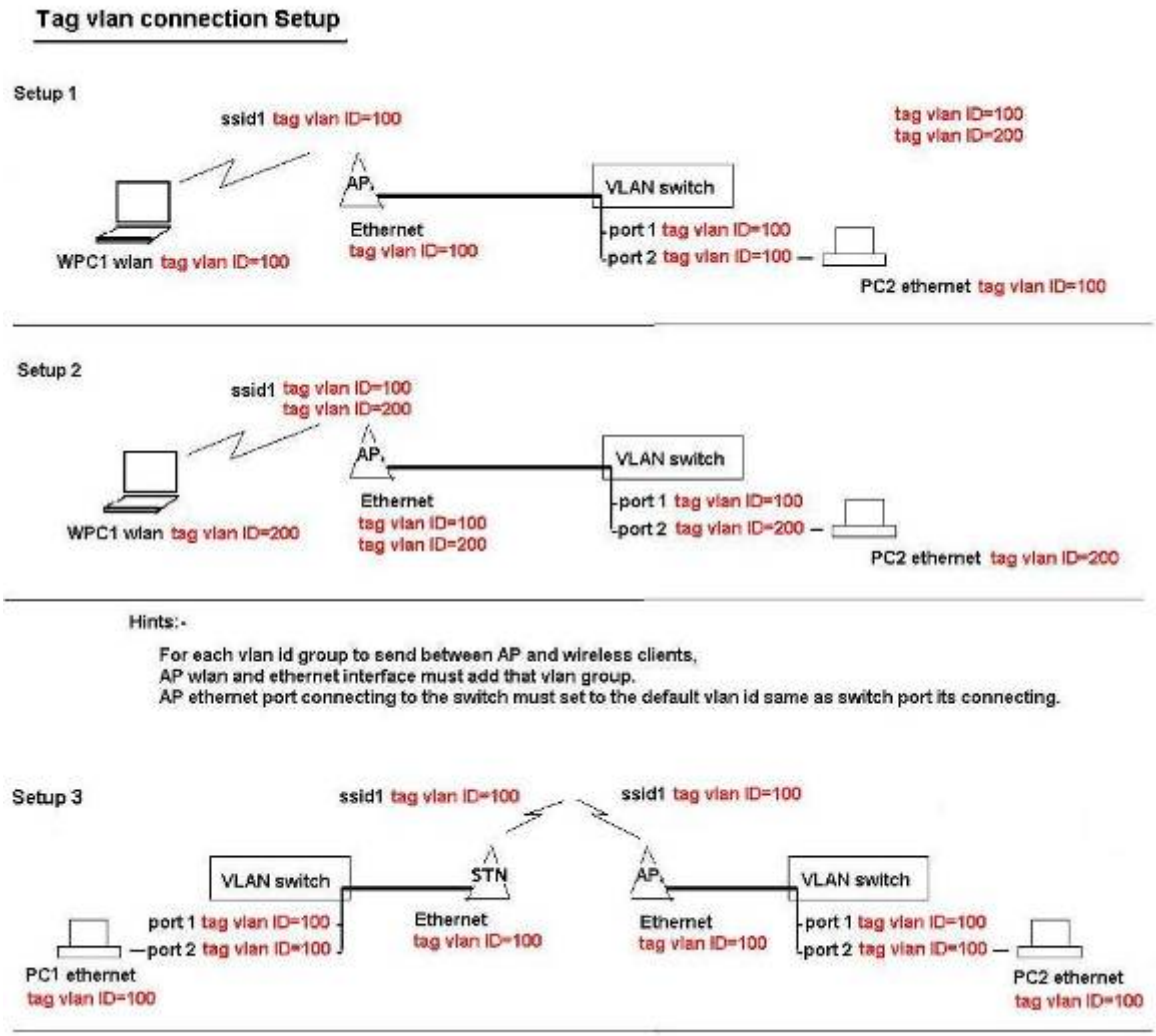
System Log

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

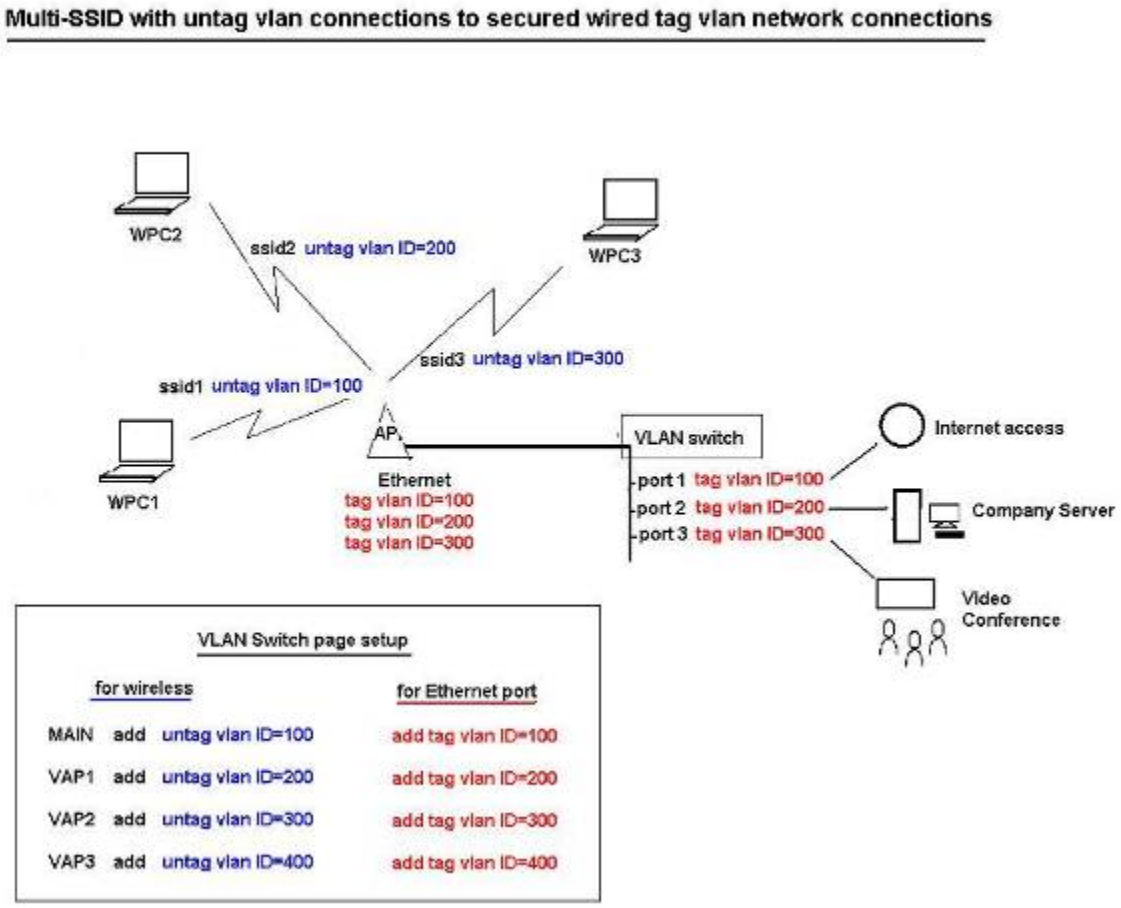
Remote Log IP Address is the host IP address where syslog messages should be sent. Remote host should be configured properly to receive syslog protocol messages.
Remote Log Port is the TCP/IP port of the host syslog messages should be sent. "514" is the default port for the commonly used system message logging utilities
.
Every logged message contains at least a *System Time* and a Host Name. Usually a particular service name which generates the system event is specifies also within the message. Messages from different services have different context and different level of the details. Usually *error*, *warning* or *informational* system services messages are reported. The more detailed system messages are reported, the greater volume of log messages will be generated.

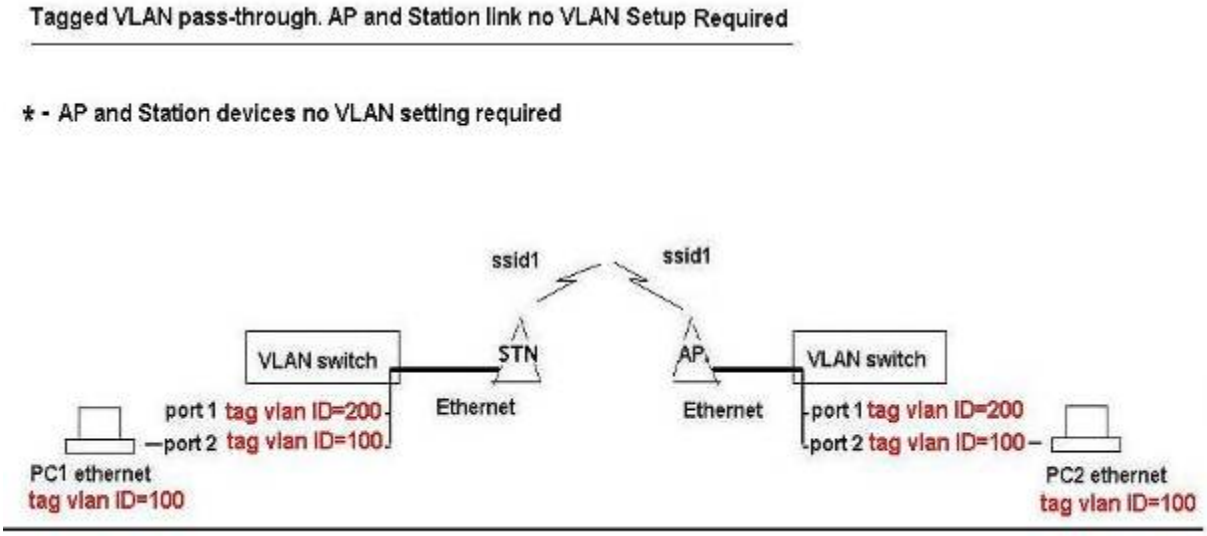
Appendix IV- VLAN Setup examples

A) Tagged Wireless VLAN to Tagged Ethernet VLAN Setup



B) Untagged Wireless VLAN to Tagged Ethernet VLAN setup



C) Tagged VLAN Pass-Through

AP and Station link No VLAN Setup Required