



ASW SERIES IPLink USER GUIDE

Copyright®
Aisai Communication Technology Co., Ltd.
All Rights Reserved.
Release3.5 May. 2011

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 into 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.

Contents

1	Product overview	1
1.1	Introduction	1
1.2	Features and benefits	2
1.3	Operation Modes and Connection Examples	3
1.3.1	Access Point and Access Point WDS Mode	3
1.3.2	Access Point WDS Mode	3
1.3.3	Station Mode	3
1.3.4	Station WDS Mode	4
1.3.5	Router Mode	5
1.3.6	Repeater WDS Mode	6
2	Installation	7
2.1	Setup requirements	7
2.2	Hardware installation	7
2.3	Configure the IP Address	8
2.3.1	For Windows 95/98/98SE/ME/NT	8
2.3.2	For Windows XP/2000	9
3	Access the Web Interface	11
3.1	Through our Utility – uConfig	11
3.2	Access with a Web Browser	13
4	Navigation	16
4.1	Main Menu	16
4.1.1	Main Menu Bar	16
4.1.2	How to save changes.	16
4.2	Basic Network Tab	17
4.2.1	Local Area Network	17
4.2.2	Bandwidth Control	17
4.3	Basic Wireless Tab	18
4.3.1	Basic Wireless Settings	18
4.3.2	Master Parameters Settings	19
4.3.3	Slave Parameters Settings	21
4.3.4	Wireless Security	22
4.4	Advance Wireless Tab	26
4.4.1	Long Range Parameters Setup	26
4.5	Advanced Network Tab	28

4.5.1	Firewall Setup.....	28
4.5.2	Remote management and Upnp Setup.....	29
4.6	VLAN Tab.....	29
4.6.1	NO Vlan	29
4.6.2	Vlan Switch	30
4.6.3	Vlan management	30
4.7	Services Tab.....	30
4.7.1	Spanning Tree Protocol (STP) SETUP	32
4.7.2	Ping Watchdog.....	32
4.7.3	Auto-Reboot	33
4.7.4	SNMP Setup.....	33
4.7.5	NTP Setup.....	33
4.7.6	Web HTTP Security.....	34
4.7.7	Telnet Access Setup.....	34
4.7.8	SSH Access Setup.....	34
4.7.9	System Log Setup.....	34
4.8	System Tab.....	36
4.8.1	Firmware Upgrade	36
4.8.2	Host Name	36
4.8.3	Administrative and Read-only Account	37
4.8.4	Enable Read-Only Account.....	37
4.8.5	Configuration Management	37
4.8.6	Device Maintenance	38
4.9	Status Page	39
4.9.1	Status Reporting	39
4.9.2	LAN Setting	39
4.9.3	Station Connection Status Info	40
Appendix I - Network.....		42
Appendix II – Wireless with Router Mode		45
Appendix III- Advanced Settings		49
Appendix IV- Services.....		51

Release Notes:

- Release 1.0– This is the first Release
- Release 2.2– Add the vlan description
- Release 3.1– Update the firmware(V2.21-P3)
- Release 3.5–Add the reset button descption

1 Product overview

1.1 Introduction



The high-performance Wireless Network Access Point (AP) is designed for enterprise and public 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 dual polarization high gain antenna it offers a compact, rugged design for outdoor installation and excellent performance.

Moreover, its integrated Power over Ethernet (PoE) allows the access point to be used in areas where power outlets are not readily available.

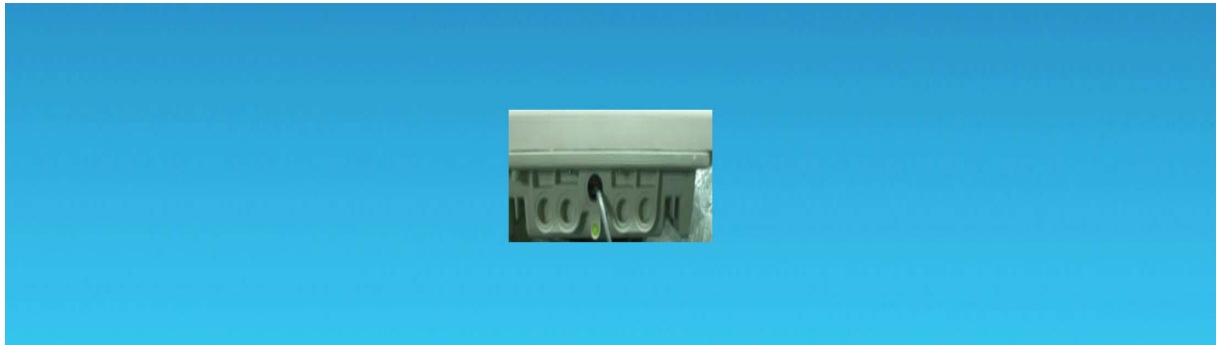
To protect your security and privacy, the access point is armed with many enhanced and latest wireless security features such as IEEE 802.11i standards, MAC Address Filtering, IEEE 802.1x Authentication and 64/128-bit WEP (Wired Equivalent Privacy) to ensure privacy for the heterogeneous mix of users 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.

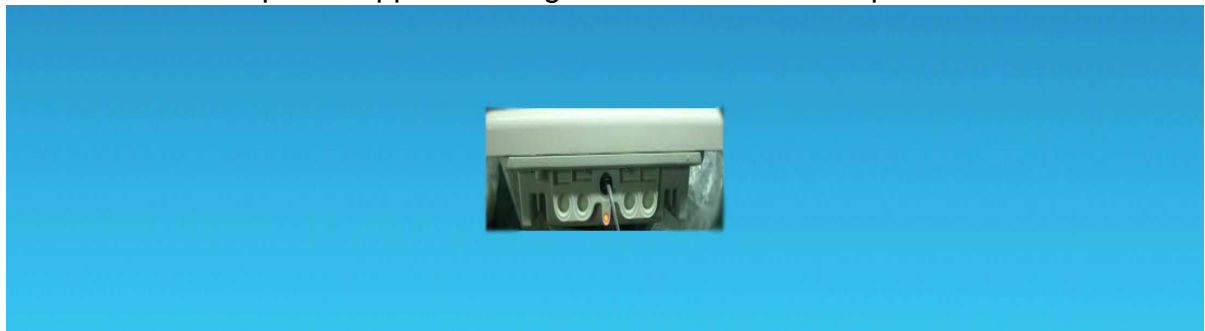
Note: The 5180MHz, 5200MHz, 5220MHz, 5240MHz are designed for indoor application, and the 5745MHz, 5765MHz, 5785MHz, 5805MHz, 5825MHz are designed for outdoor application

The antenna and the human body should be keep 20cm distance.

- **LED Description**



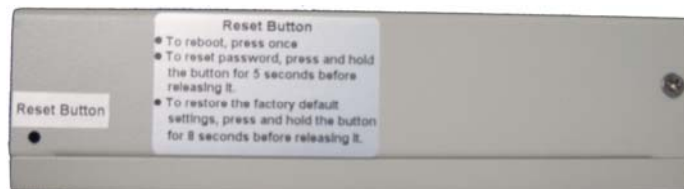
Green—indicates power applied through POE, but Ethernet port still not attached.



Amber—solid—indicates power applied and Ethernet port is attached to the POE.

Amber—flash—indicates data is passing through the Ethernet port.

- **Reset Button**



- To reboot, press once.
- To reset password, press and hold the button for 5 seconds before releasing it.
- To restore the factory default setting, press and hold the button for 8 seconds before releasing it.

1.2 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 kilometers apart while unifying the networks.

- **Virtual AP (Multiple SSID)**

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

- **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-TLS, 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.

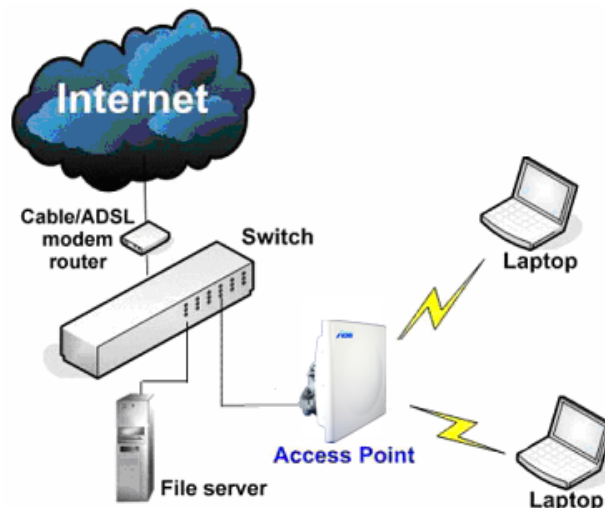
- **SSH**

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

1.3 Operation Modes and Connection Examples

1.3.1 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.



1.3.2 Access Point WDS Mode

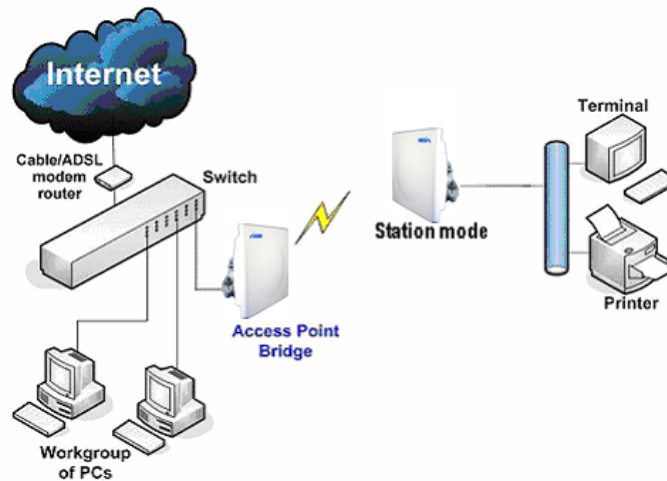
This mode is generally used for point-to-point or point-to-multi-point connection. It is mainly used with Station WDS to build the point and multi-point connections.

1.3.3 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.



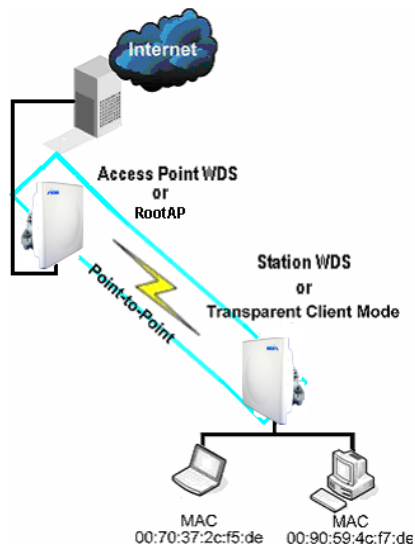
1.3.4 Station WDS Mode

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.



1.3.5 Router Mode

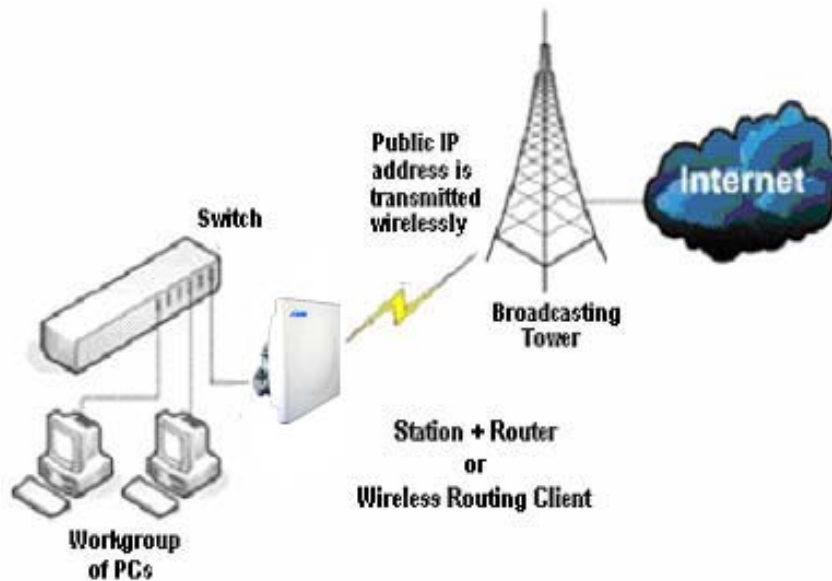
In Router Mode, the device also operates as a router.

Either the wireless or Ethernet can be setup as WAN connection to a broadband modem. Wireless as WAN is known as **Station + Router mode** (or **Wireless Routing Client** mode) and Ethernet as WAN is known as **AP + Router mode** (or **Gateway** mode). Device supports several types of broadband connections Static IP, Dynamic IP and PPPoE. For setup details refer to the respective section. The illustration below shows the Ethernet port is setup as the WAN port and the wireless connection as the LAN.

Station + Router connection example

Wireless is use to connect to the broadband.

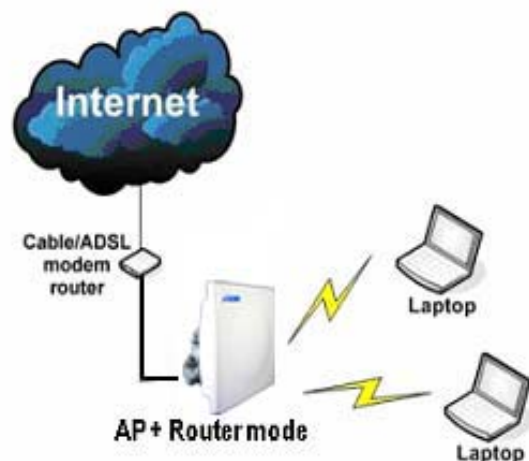
Ethernet is the local network (LAN) sharing the broadband connection.



AP + Router connection example

Ethernet is use to connect to the broadband.

Wireless is the local network (LAN) sharing the broadband connection.



Broadband Internet Access Type:

Static IP Address

Use Static IP Address you have subscribed a fixed IP or range IP addresses from your ISP.

Dynamic IP Address

With Dynamic IP Address the device automatically request IP address from modem or ISP.

PPP over Ethernet (PPPoE)

When using ADSL services provided by your ISP support PPPoE connection.

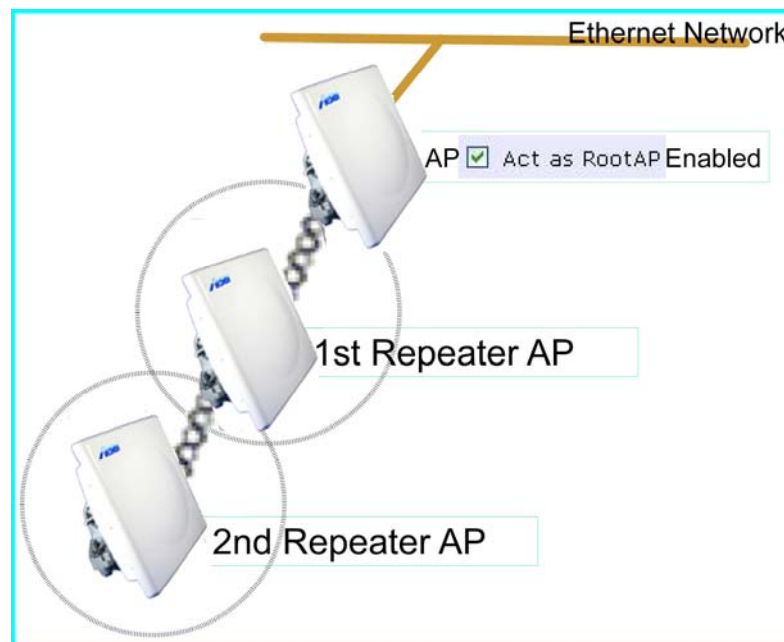
1.3.6 Repeater WDS Mode

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.**



2 Installation

2.1 Setup requirements

Before starting, please verify that the following is available:

- CAT5/5e networking cable
- At least 1 computer installed with a web browser and a wired or wireless network interface adapter.
- All network nodes installed with TCP/IP and properly configured IP address parameters.

2.2 Hardware installation

The access point can be powered using the 802.3af standard PoE Injector. This accessory supplies operational power to the wireless access point via the Ethernet cable connection.

Step 1: Use an RJ45 Ethernet cable to connect one end of the cable to the Ethernet socket of the Injector and the other end to one of the LAN ports of the accesspoint.

Warning:

When one port is used for PoE, the other port cannot connect to any other network device.



Step 2: Next, connect the RJ45 Ethernet cable attached to the standard PoE Injector to your PC's Ethernet network adapter.

Once you have finished configuring your access point, you can connect the PoE Injector's RJ45 Ethernet cable to your network device, such as to a switch or hub.



2.3 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.

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

Step 1:

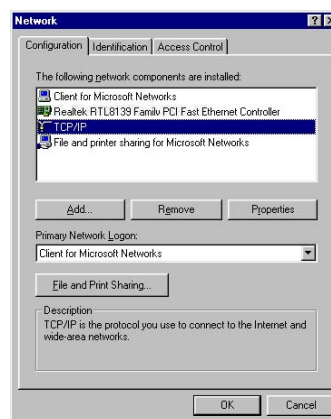
From your desktop, right-click the **Network Neighborhood** icon and select **Properties**.

Step 2:

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

Step 3:

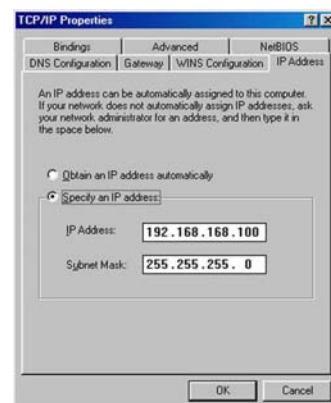
Highlight **TCP/IP** and click on the **Properties** button.



Step 4:

Select the **Specify an IP address** radio button.

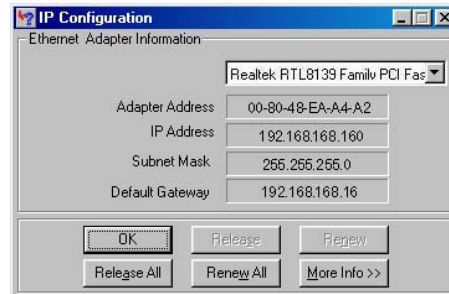
Set the IP address to 192.168.168.X and Subnet mask to 255.255.255.0, where X can be any number from 2 to 254.



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**.



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

2.3.2 For Windows XP/2000

Step 1:

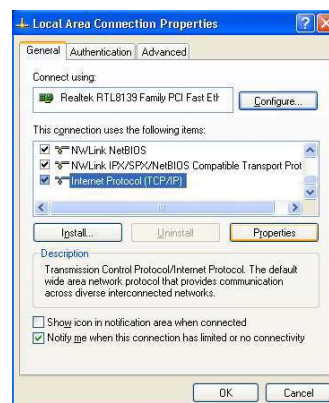
Go to your desktop, right-click on the **My Network Places** icon and select **Properties**.

Step 2:

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

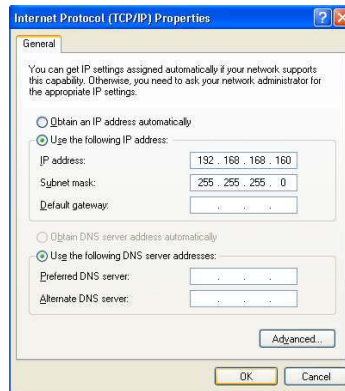
**Step 3:**

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.

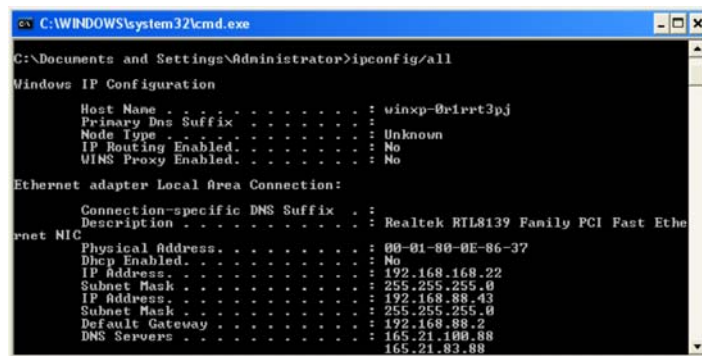


Step 5:

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.

3 Access the Web Interface

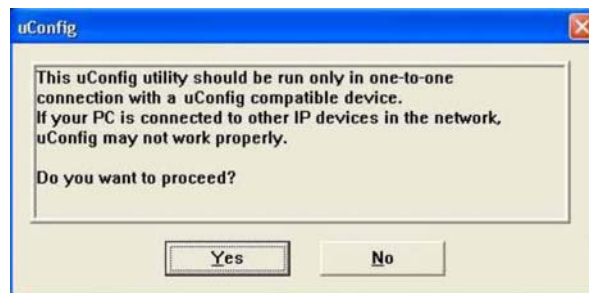
There are two methods to access to the web-based Interface of your access point:

3.1 Through our Utility – uConfig

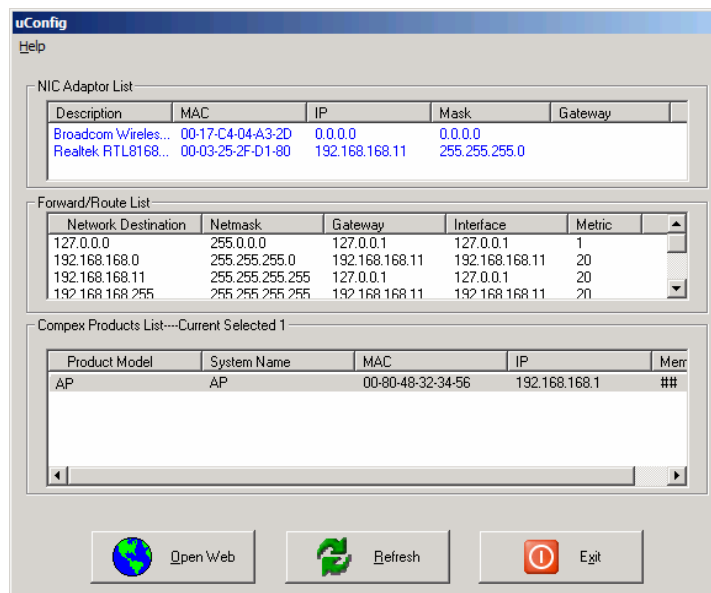
You can access to the web-based interface directly without the need to assign a different IP address to your PC.

Step 1: install the **uConfig** utility to your hard disk.

Step 2: After installation double-click on the **uConfig** icon and click on the **Yes** button.



Step 3: 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 4: 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.

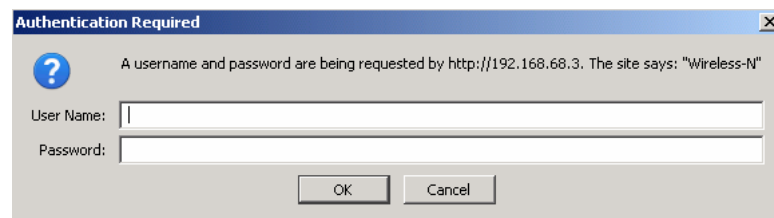


Step 5: At the login prompt, enter the User Name and Password.

The default are :

User Name : **admin**

Password : **password**



Step 6: It then opens the device home page. The Status page.

The screenshot displays the Aisai web management interface. At the top, there is a navigation bar with tabs: STATUS, BASIC WIRELESS, BASIC NETWORK, ADVANCED WIRELESS, ADVANCED NETWORK, VLAN, SERVICES, and SYSTEM. The 'STATUS' tab is currently selected.

Below the navigation bar, there are two main sections: 'MAIN' and 'VERSION'.

MAIN Section:

- Uptime: 0 Days 00:03:29
- Host Name: AP
- System Time: 01/01/2000 00:03:30

VERSION Section:

- FIRMWARE VERSION: 2.21-P3-e
- LOADER VERSION: 2.55 (build 0902)

LAN SETTING Section:

- LAN MAC: e0-c2-86-30-1e-2a
- MODE: static
- IP ADDRESS: 192.168.168.14
- GATEWAY IP ADDRESS:
- LAN cable: Plugged

Radio 1 Section:

- Wireless Mode: Station
- REMOTE AP SSID: test-tip
- Signal Strength: None
- TX Rate: None
- TX CCQ: None
- Frequency: 5.66 GHz
- Ack Timeout: 172
- MAC: e0-c2-86-30-1e-2b
- REMOTE AP MAC: E0:C2:86:30:10:82
- Noise level: 133/161 dBm
- RX Rate: None
- Channel Width: None
- Security: None

LOCAL STATION STATISTICS Section:

	Bytes	Packets	Errors
Received:	0	0	0
Transmitted:	0	0	0

LOCAL STATION ERRORS Section:

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

3.2 Access with a Web Browser

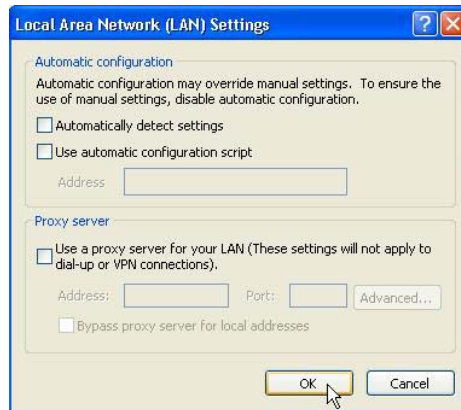
Step 1:

Launch your Web browser. e.g. MS Internet Explorer, FireFox, Netscape, etc..
For 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.

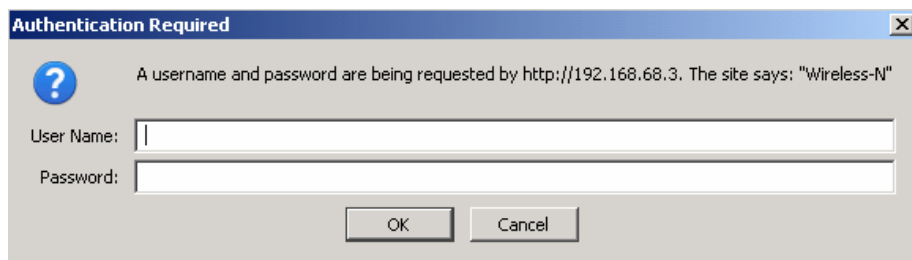
Step 4:

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.



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

MAIN

Uptime: 0 Days 00:03:29
Host Name: AP
System Time: 01/01/2000 00:03:30

[More Status](#)**VERSION**

FIRMWARE VERSION: 2.21-P3-e
LOADER VERSION: 2.55 (build 0902)

LAN SETTING

LAN MAC: e0-c2-86-30-1e-2a
MODE: static
IP ADDRESS: 192.168.168.14
GATEWAY IP ADDRESS :
LAN cable : Plugged

Radio 1

Wireless Mode: Station
REMOTE AP SSID : test-tip
Signal Strength: None [Align](#)
TX Rate: None
TX CCQ: None
Frequency: 5.66 GHz
Ack Timeout: 172

MAC: e0-c2-86-30-1e-2b
REMOTE AP MAC: E0:C2:86:30:10:82
Noise level: 133/161 dBm
RX Rate: None
Channel Width: None
Security: None
[Refresh](#)

LOCAL STATION STATISTICS

	Bytes	Packets	Errors
Received:	0	0	0
Transmitted:	0	0	0

LOCAL STATION ERRORS

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

4 Navigation

4.1 Main Menu

4.1.1 Main Menu Bar



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

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 more advanced wireless features. Advanced Network page settings for more advanced network features.

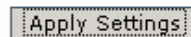
VLAN: The page setting VLAN modes : no vlan,vlan switch or vlan management.

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

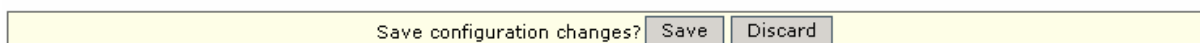
System : Page contains controls for system maintenance routines, administrator account management, device customization and configuration backup.

4.1.2 How to save changes.

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



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.

4.2 Basic Network Tab



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

[Apply Settings](#)

LOCAL AREA NETWORK

LAN Mode:

IP Address:

Netmask:

Gateway IP:

BANDWIDTH CONTROL:

Bandwidth Control: ☐ Enabled [Configure](#)

[Apply Settings](#)

4.2.1 Local Area Network

LOCAL AREA NETWORK

LAN Mode:

IP Address:

Netmask:

Gateway IP:

4.2.2 Bandwidth Control

BANDWIDTH CONTROL:

Bandwidth Control: ☐ Enabled [Configure](#)

Click f [Configure](#) from the menu bar to open the page as show below.

BANDWIDTH CONTROL SETUP

Ethernet to WirelessTraffic Limit (kbit)-Download:

Wireless to EthernetTraffic Limit (kbit)-Upload:

Bandwidth Control: Default is disabled. Check on box to enable.

This control let user set a max limited bandwidth to router.

This function let use share one high speed broadband line with several routers each limited to a maximum limited by its bandwidth control.

Download Total Rate(kbit) enter the max bandwidth limit for downloading on this router.

Upload Total Rate(kbit): enter the max bandwidth limit for uploading on this router.

4.3 Basic Wireless Tab

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

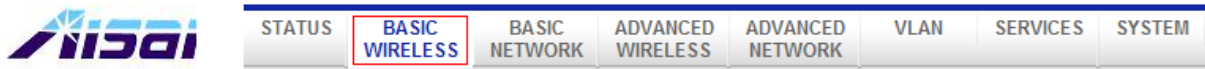


Fig 2.1 Basic Wireless Tab

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.

Enable the radio



Fig 2.2 Enable Radio Checkbox

Tick/Untick the checkbox to enable/disable the radio.

4.3.1 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 **4 modes** available.

BASIC WIRELESS SETTINGS

Wireless Mode:	Access Point WDS ▼		
Local AP-ESSID:	PTMP-1	<input type="checkbox"/> Hide SSID	
Country Code:	United States of America ▼		
Wireless Profile:	NA ▼	(Long range parameter enabled)	
Channel Spectrum Width:	20/40M ▼		
Guard Interval:	Short ▼		
Channel-Frequency:	5825M ▼	<input type="checkbox"/> Auto	Select <input type="text"/>
	<input type="button" value="Interference Analyzer"/>		
Data Rate (Mbps):	MCS 0 (15 Mbps) ▼	<input checked="" type="checkbox"/> Auto	
Transmit Power:	23 ▼	dBm Chainmask: 2x2 Dual - Aggregate Dual Chain Power	
	<input type="checkbox"/> Maximum		
	<input type="checkbox"/> Obey Regulatory Power		
Rate Aggressiveness:	0 ▼		

Access Point

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

Client:

This is a client mode that can be connected to the Access point mode. It is used to bridge the wireless connection to a Master. 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.

WDS Client:

WDS is the acronym of Wireless Distribution System. It can be connected to the **WDS Client** mode. It enables packet forwarding at layer 2 level. Unlike Slave mode, it is fully transparent at layer 2 level.

4.3.2 Master Parameters Settings

BASIC WIRELESS SETTINGS

Wireless Mode:	Access Point WDS ▼		
Local AP-ESSID:	PTMP-1	<input type="checkbox"/> Hide SSID	
Country Code:	United States of America ▼		
Wireless Profile:	NA ▼	(Long range parameter enabled)	
Channel Spectrum Width:	20/40M ▼		
Guard Interval:	Short ▼		
Channel-Frequency:	5825M ▼	<input type="checkbox"/> Auto	Select <input type="text"/>
	Interference Analyzer		
Data Rate (Mbps):	MCS 0 (15 Mbps) ▼	<input checked="" type="checkbox"/> Auto	
Transmit Power:	23 ▼	dBm Chainmask:	2x2 Dual - Aggregate Dual Chain Power
		<input type="checkbox"/> Maximum	
		<input type="checkbox"/> Obey Regulatory Power	
Rate Aggressiveness:	0 ▼		

Fig 2.3 Basic Wireless Settings

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

N/A

Wireless Profile:

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

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 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.**

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. For 5GHz frequency range some have DFS characteristics earmarked by regulations. Selecting one of these frequencies for operation may affect and delay of 2 minutes or more (possibly up to 10 minutes in some situations) for device to attempt to establish a connection.

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

The channel frequency listed as below:

5180MHz, 5200MHz, 5220MHz, 5240MHz, 5745MHz, 5765MHz, 5785MHz, 5805MHz, 5825MHz

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

Transmit Power List:

11dBm, 12dBm, 13dBm, 14dBm, 15dBm, 16dBm, 17dBm, 18dBm, 19dBm, 20dBm, 23dBm

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.

4.3.3 Slave Parameters Settings

BASIC WIRELESS SETTINGS

The screenshot shows the 'BASIC WIRELESS SETTINGS' configuration window. The settings are as follows:

- Wireless Mode:** Access Point WDS (dropdown)
- Local AP-ESSID:** PTMP-1 (text field) with a ☐ Hide SSID checkbox.
- Country Code:** United States of America (dropdown)
- Wireless Profile:** NA (dropdown) with a note '(Long range parameter enabled)'.
- Channel Spectrum Width:** 20/40M (dropdown)
- Guard Interval:** Short (dropdown)
- Channel-Frequency:** 5825M (dropdown) with an ☐ Auto checkbox and a 'Select' button next to an empty text field.
- Interference Analyzer:** A button.
- Data Rate (Mbps):** MCS 0 (15 Mbps) (dropdown) with a ☒ Auto checkbox.
- Transmit Power:** 23 (dropdown) with a **dBm** label.
- Chainmask:** 2x2 Dual - Aggregate Dual Chain Power (text field).
- ☐ Maximum checkbox.
- ☐ Obey Regulatory Power checkbox.
- Rate Aggressiveness:** 0 (dropdown)

Fig 2.4 Basic Wireless Settings

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.

Wireless Adapter mode

This option change device function like a wireless adapter installed in a computer.

This mode should only be use on one computer, like old laptops or computer aided device with only Ethernet port like printer that do not have expansion interface to add wireless interface.

It work transparently forwarding and receiving packets from wireless to the computer's ethernet port. The Ethernet port MAC address of the client computer is cloned and copied on top of this device, so the opposite connecting device will register this MAC address of the laptop or PC rather than the intermediate wireless device. This option is effective for only one computer connection. If the computer device like printer that have not option to do the setup, it should first be configured from a PC then connect to the printer.

The configuration parameters are the same as Station mode as shown above.

4.3.4 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

LOCAL AP - WIRELESS SECURITY:

Security:	WPA	
WPA Authentication:	PSK	Cipher Type: AUTO
WPA Preshared Key:	11111111	
Pri. Radius Server IP:	0.0.0.0	
Sec. Radius Server IP:	0.0.0.0	
Authentication Port:	1812	
Accounting Port:	1813	
Radius Secret Key:	private	
MAC ACL:	<input type="checkbox"/> Enabled	<input type="text"/> Add
Policy:	Allow	<input type="text"/> Remove

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 to ensure the highest transmission speed and throughput is switch on. Using TKIP cipher type device may switch to legacy maximum transmission speed of 54Mbps. And performance can only achieve up to legacy maximum performance and throughput.

WPA + EAP

LOCAL AP - WIRELESS SECURITY:

Security:	WPA	
WPA Authentication:	EAP	Cipher Type: AUTO
WPA Preshared Key:	*****	
Pri. Radius Server IP:	0.0.0.0	
Sec. Radius Server IP:	0.0.0.0	
Authentication Port:	1812	
Accounting Port:	1813	
Radius Secret Key:	private	
MAC ACL:	<input type="checkbox"/> Enabled	<input type="text"/> Add
Policy:	Allow	<input type="text"/> Remove

Fig 2.8 WPA + EAP

EAP – WPA or WPA2 with EAP (Extensible Authentication Protocol)
Firmware supported options for clients are: EAP-TLS, EAP-TTLS, 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 use this to authenticate itself into the Radius Server.

WPA + EAP_TLS, WPA-TTLS, WPA-PEAP**REMOTE AP - WIRELESS SECURITY:**

Security:	WPA	
WPA Authentication:	EAP EAP_TTLS	Cipher Type: AUTO
Preshared Key:	11111111	
Identity:	anonymous	
User Name:	user@example.com	
User Password:	password	

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

This apply 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-suplicant for EAP authentication.

User Name:

Identification credential used by the wpa-suplicant for EAP tunneled authentication in unencrypted form.

User Password:

Password credential used by the wpa-suplicant for EAP authentication

IEEE802.1x Settings

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

LOCAL AP - WIRELESS SECURITY:

The screenshot shows a configuration window titled 'LOCAL AP - WIRELESS SECURITY:'. It contains several input fields and buttons. The 'Security' dropdown is set to 'IEEE802.1X'. The 'Pri. Radius Server IP' and 'Sec. Radius Server IP' are both '0.0.0.0'. The 'Authentication Port' is '1812' and the 'Accounting Port' is '1813'. The 'Radius Secret Key' is 'private'. The 'IEEE802.1X Key Rotation' is '600' and the 'IEEE802.1X Key Length' is '64 bit'. The 'MAC ACL' checkbox is checked, and the 'Policy' dropdown is set to 'Allow'. There are 'Add' and 'Remove' buttons next to the MAC ACL field.

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. After time expired will initiate key rotation in uthentication process for higher security.

IEEE802.1x Key Length

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

WEP

LOCAL AP - WIRELESS SECURITY:

The screenshot shows the 'LOCAL AP - WIRELESS SECURITY' configuration window. It contains the following elements:

- Security:** A dropdown menu set to 'WEP'.
- Authentication Type:** Radio buttons for 'Open' (selected) and 'Shared Key'.
- Key Type:** A dropdown menu set to 'ASCII'.
- Current Key:** A dropdown menu set to 'KEY 1'.
- WEP Key 1:** An empty text input field.
- WEP Key 2:** An empty text input field.
- WEP Key 3:** An empty text input field.
- WEP Key 4:** An empty text input field.
- WEP Key 1 Length:** A dropdown menu set to '64 bit'.
- WEP Key 2 Length:** A dropdown menu set to '64 bit'.
- WEP Key 3 Length:** A dropdown menu set to '64 bit'.
- WEP key 4 Length:** A dropdown menu set to '64 bit'.
- MAC ACL:** A checkbox labeled 'Enabled' which is unchecked.
- Policy:** A dropdown menu set to 'Allow'.
- Buttons:** 'Add' and 'Remove' buttons are located at the bottom right.

Fig 2.6 WEP

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

**** Note: Operating with WEP security will lower the performance significantly with 802.11n radio. Not recommended for Access Point and Access Point WDS mode operation. May use WEP ONLY when connecting with standard 11 and 54Mbps (legacy) 802.11a/b/g bands radio.**

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-bit** – 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.

4.4 Advance Wireless Tab



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



LONG RANGE PARAMETERS (RADIO 1)

Long Range Parameters: ☒ Enable

Beacon Interval:

RTS Threshold: ☐ off

Fragmentation Threshold: ☐ off

Distance: meters

Slot Time(us):

ACK Timeout(us): ☒ Auto Adjust for Slottime, ACK Timeout, CTS Timeout

CTS Timeout (us):

OTHER SETTINGS (RADIO 1)

Noise Immunity: ☒ Enable

Signal Strength Indicator (RSSI): LED1: LED2: LED3: LED4:

Radio Off with No Ethernet: ☐ Enabled

Station Isolation: ☐ Enabled

Chainmask Selection:

4.4.1 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):

Signal Strength Indicator (RSSI):	LED1: <input type="text" value="10"/>	LED2: <input type="text" value="20"/>	LED3: <input type="text" value="30"/>	LED4: <input type="text" value="40"/>
-----------------------------------	--	--	--	--

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)

4.5 Advanced Network Tab

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

***Note:** This tab will not open when in device is in Bridge mode.
To open page, first enabled Router mode in Basic Network

Firewall Setup:

Firewall: ☐ Enabled Configure

Remote Management Setup:

Remote HTTP/HTTPS : ☒ Enabled

Remote HTTP Port :

UPNP Setup:

UPnP: ☐ Enabled Apply Settings

4.5.1 Firewall Setup

Firewall							
	On	Comment	Policy	IP Type	Source IP/Mask	Src Port	Destination IP/Mask Des Port
1.	<input checked="" type="checkbox"/>	Web server	ACCEPT	TCP	0.0.0.0	80	192.168.168.10 81
2.	<input checked="" type="checkbox"/>	Ftp server	ACCEPT	TCP	0.0.0.0	21	192.168.168.11 21
3.	<input checked="" type="checkbox"/>	Block 445 port	DENY	TCP	0.0.0.0	445	0.0.0.0 445
4.	<input checked="" type="checkbox"/>	Block 135	DENY	UDP	0.0.0.0	135	0.0.0.0 135
5.	<input checked="" type="checkbox"/>	Block 136	ACCEPT	UDP	0.0.0.0	136	0.0.0.0 136
6.	<input checked="" type="checkbox"/>	Block 137	ACCEPT	UDP	0.0.0.0	137	0.0.0.0 137
7.	<input checked="" type="checkbox"/>	Block 138	ACCEPT	UDP	0.0.0.0	138	0.0.0.0 138
8.	<input checked="" type="checkbox"/>	Block 139	ACCEPT	UDP	0.0.0.0	139	0.0.0.0 139
9.	<input checked="" type="checkbox"/>	Internet Printer share	ACCEPT	TCP	206.123.27.99	631	192.168.168.12 631
10.	<input type="checkbox"/>		ACCEPT	TCP			
11.	<input type="checkbox"/>		ACCEPT	TCP			
12.	<input type="checkbox"/>		ACCEPT	TCP			
13.	<input type="checkbox"/>		ACCEPT	TCP			
14.	<input type="checkbox"/>		ACCEPT	TCP			
15.	<input type="checkbox"/>		ACCEPT	TCP			
16.	<input type="checkbox"/>		ACCEPT	TCP			
17.	<input type="checkbox"/>		ACCEPT	TCP			
18.	<input type="checkbox"/>		ACCEPT	TCP			
19.	<input type="checkbox"/>		ACCEPT	TCP			
20.	<input type="checkbox"/>		ACCEPT	TCP			

Apply Cancel

Firewall Setup: Default is disabled. Check on box to enable.
For configuration refer to 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 to check

Source IP/Mask: enter the source IP address and Netmask

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;

Src Port: enter the source port number in rule check

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: enter the destination IP and Netmask

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;

Des Port: enter the destination port in rule check

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

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

4.5.2 Remote management and Upnp Setup

REMOTE MANAGEMENT SETUP:

Remote HTTP/HTTPS : ☒ Enabled

Remote HTTP Port :

UPNP SETUP:

UPnP: ☐ Enabled

Apply Settings

UPNP: Default is disabled. Check on box to enabled.

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

For security reason this service should not be open.

Recommend to setup manually open all port service through **Port Forwarding** service.

4.6 VLAN Tab

Click VLAN tab from menu to open the page below.

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



4.6.1 NO Vlan

Apply Settings

VLAN MODES

- ☒ No Vlan
- ☐ Vlan Switch
- ☐ Vlan Management

4.6.2 Vlan Switch

[Apply Settings](#)

VLAN MODES

☐ No Vlan

☒ Vlan Switch

☐ Vlan Management

ETHERNET VLAN

Default VLAN ID: ▼

VLAN ID	Tag	
	Tag ▼	Add

RADIO 1 VLAN

Main
VAP1
VAP2
VAP3

Default VLAN ID: ▼

VLAN ID	Tag	
	Tag ▼	Add

4.6.3 Vlan management

[Apply Settings](#)

VLAN MODES

☐ No Vlan

☐ Vlan Switch

☒ Vlan Management

VLAN MANAGEMENT

VLAN ID	IP ADDRESS	
		Add

Management IP	VLAN ID	IP ADDRESS
		

[Apply Settings](#)

4.7 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.

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

SPANNING TREE PROTOCOL (STP) SETUP

Enable STP:	<input type="checkbox"/>	
Root Priority:	<input type="text" value="32768"/>	(Range : 0 to 65536)
Root Hello Time:	<input type="text" value="2"/>	(Range : 1 to 10)
Root Forward Delay:	<input type="text" value="15"/>	(Range : 4 to 30)
Root Maximum Age:	<input type="text" value="20"/>	(Range : 6 to 40)
<input type="button" value="Apply"/>		

PING WATCHDOG

Enable Ping Watchdog:	<input type="checkbox"/>	
IP Address To Ping:	<input type="text" value="192.168.168.1"/>	
Ping Interval:	<input type="text" value="5"/>	seconds
Startup Delay:	<input type="text" value="60"/>	seconds
Failure Count To Reboot:	<input type="text" value="5"/>	
<input type="button" value="Apply"/>		

AUTO-REBOOT

Auto Reboot Mode:	<input type="text" value="Disabled"/>
<input type="button" value="Apply"/>	

SNMP SETUP

Enable SNMP:	<input type="checkbox"/>	
Read Password:	<input type="text" value="public"/>	
Engine ID:	<input type="text" value="800007e5BD00002704"/>	
Enable SNMP Trap:	<input type="checkbox"/>	
Trap Destination IP:	<input type="text" value="192.168.168.1"/>	
Community:	<input type="text" value="public"/>	
<input type="button" value="Apply"/>		

NTP SETUP

Select Your Time Zone:	GMT-07:00 (Mountain Time (US & Canada), ...)
Enable NTP Client:	<input type="checkbox"/>
Custom Time Server:	time.nist.gov
Known Time Server:	bonehed.lcs.mit.edu
<input type="button" value="Apply"/>	

WEB SERVER

Web server mode:	HTTP
HTTPS Port:	80
<input type="button" value="Apply"/>	

TELNET SERVER

Enable Telnet Server:	<input checked="" type="checkbox"/>
Server Port:	23
<input type="button" value="Apply"/>	

SSH SERVER

Enable SSH Server:	<input type="checkbox"/>
Server Port:	22
<input type="button" value="Apply"/>	

SYSTEM LOG

Enable System Log:	<input type="checkbox"/>
Logging IP/Domain Name:	192.168.168.1
Logging Port:	514
<input type="button" value="Apply"/>	

4.7.1 Spanning Tree Protocol (STP) SETUP**SPANNING TREE PROTOCOL (STP) SETUP**

Spanning Tree Protocol:	<input type="checkbox"/> Enabled	
Root Priority:	32768	(Range : 0 to 65536)
Root Hello Time:	2	(Range : 1 to 10)
Root Forward Delay:	15	(Range : 4 to 30)
Root Maximum Age:	20	(Range : 6 to 40)

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

Root Priority: Default value is 32768. Smaller value has 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 lower time can caused high overheads to the network.

4.7.2 Ping Watchdog

PING WATCHDOG

Enable Ping Watchdog:	<input type="checkbox"/>
IP Address To Ping:	<input type="text" value="192.168.168.1"/>
Ping Interval:	<input type="text" value="5"/> seconds
Startup Delay:	<input type="text" value="60"/> seconds
Failure Count To Reboot:	<input type="text" value="5"/>
<input type="button" value="Apply"/>	

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.

4.7.3 Auto-Reboot**AUTO-REBOOT**

Auto Reboot Mode:	<div> <div>Disabled</div> <div> <div>Disabled</div> <div>By Hour</div> <div>By Time</div> </div> </div>
-------------------	---

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.

4.7.4 SNMP Setup**SNMP SETUP**

Enable SNMP:	<input checked="" type="checkbox"/>
Read Password:	<input type="text" value="public"/>
Engine ID:	<input type="text" value="800007e5BD00002704D000007c"/>
Enable SNMP Trap:	<input type="checkbox"/>
Trap Destination IP:	<input type="text" value="192.168.168.1"/>
Community:	<input type="text" value="public"/>
<input type="button" value="Apply"/>	

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.

4.7.5 NTP Setup

NTP SETUP

Select Your Time Zone:	GMT-07:00 (Mountain Time (US & Canada), ...)
Enable NTP Client:	<input checked="" type="checkbox"/>
Custom Time Server:	time.nist.gov
Known Time Server:	bonehed.lcs.mit.edu
<input type="button" value="Apply"/>	

Select Your Time Zone: Select from list the country you reside.

Enable NTP Client: Default is disabled. Check on box to enable.

Custom Time Server: Default is "time.nist.gov" Enter preferred time server domain or IP

Known Time Server: You can also select one from this list as your new time server.

4.7.6 Web HTTP Security**WEB SERVER**

Web server mode:	HTTP
HTTPS Port:	80
<input type="button" value="Apply"/>	

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.

4.7.7 Telnet Access Setup**TELNET SERVER**

Enable Telnet Server:	<input checked="" type="checkbox"/>
Server Port:	23
<input type="button" value="Apply"/>	

Enable Telnet Server: Default is enabled. Remove check on box to disable.

Server Port: Default is 23. Enter new preferred port number.

4.7.8 SSH Access Setup**SSH SERVER**

Enable SSH Server:	<input type="checkbox"/>
Server Port:	22
<input type="button" value="Apply"/>	

Enable SSH Server: Default is disabled. Check on box to enable.

Server Port: Default is 22. Enter new preferred port number.

4.7.9 System Log Setup

SYSTEM LOG

Enable System Log:	<input type="checkbox"/>
Logging IP/Domain Name:	<input type="text" value="192.168.168.1"/>
Logging Port:	<input type="text" value="514"/>
	<input type="button" value="Apply"/>

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.

4.8 System Tab

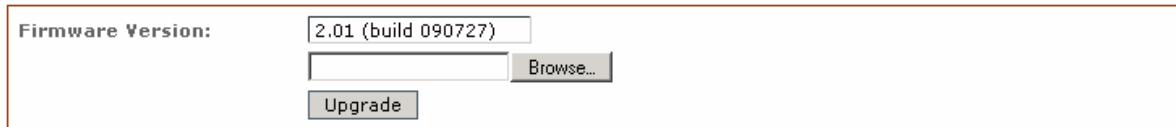
Click **System** tab from menu to open the page below.

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

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.

4.8.1 Firmware Upgrade

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.

4.8.2 Host Name

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.

4.8.3 Administrative and Read-only Account

ADMINISTRATIVE ACCOUNT

Administrator Username:	<input type="text" value="admin"/>
Current Password:	<input type="password"/>
New Password:	<input type="password"/>
Verify New Password:	<input type="password"/>
<input type="button" value="Apply"/>	

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.

4.8.4 Enable Read-Only Account

READ-ONLY ACCOUNT

Enable Read-Only Account:	<input checked="" type="checkbox"/>
Read-Only Username:	<input type="text" value="guest"/>
Password:	<input type="password"/>
<input type="button" value="Apply"/>	

Read-Only Username

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

4.8.5 Configuration Management

CONFIGURATION MANAGEMENT

Backup Configuration:	<input type="button" value="backup..."/>
Upload Configuration:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Restore"/>	

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.

4.8.6 Device Maintenance

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.

4.9 Status Page

STATUS	BASIC WIRELESS	BASIC NETWORK	ADVANCED WIRELESS	ADVANCED NETWORK	SERVICES	SYSTEM
--------	----------------	---------------	-------------------	------------------	----------	--------

Refresh

MAIN

Uptime:	0 Days 02:15:51
Host Name:	JJ
System Time:	01/01/2000 02:15:52

VERSION

FIRMWARE VERSION:	2.00 (build 090713)
LOADER VERSION:	2.56 (build 0612)

LAN SETTING

LAN MAC:	00-80-48-65-ad-ce
MODE:	static
IP ADDRESS:	192.168.168.6
GATEWAY IP ADDRESS :	
Pri.DNS IP :	10.10.10.10
Sec.DNS IP :	20.20.20.20

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 WDS	MAC:	00-80-48-65-ad-cf
LOCAL AP SSID :	TY_Test	LOCAL AP MAC:	00-80-48-65-ad-cf
Frequency:	5.745 GHz	Security:	WPA2
			More...

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.

4.9.1 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.

4.9.2 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

WAN MAC: displays the MAC address of the device 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 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.

4.9.3 Station Connection Status Info

Click  at the bottom of the Status page to view client connection statistics.

RADIO 1				
Wireless Mode:	<input type="text" value="Access Point WDS"/>	MAC:	<input type="text" value="00-80-48-65-ad-cf"/>	
LOCAL AP SSID :	<input type="text" value="TY_Test"/>	LOCAL AP MAC:	<input type="text" value="00-80-48-65-ad-cf"/>	
Frequency:	<input type="text" value="5.745 GHz"/>	Security:	<input type="text" value="WPA2"/>	
			<input type="button" value="More..."/>	
CONNECTED STATIONS				
MAC ADDRESS	SIGNAL STRENGTH	Tx RATE	Rx RATE	CHANNEL WIDTH
LOCAL AP STATISTICS				
	Bytes	Packets	Errors	
Received:	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	
Transmitted:	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	
LOCAL AP ERRORS				
RX Invalid NWID:	<input type="text" value="0"/>	TX Excessive Retries:		<input type="text" value="0"/>
RX Invalid Crypt :	<input type="text" value="0"/>	Missed Beacons :		<input type="text" value="0"/>
RX Invalid Frag:	<input type="text" value="0"/>	Other Errors:		<input type="text" value="0"/>
<input type="button" value="Select VAP"/>				

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:

20MHz – is the standard channel spectrum width (selected by default).

40MHz – the widest channel spectrum width required to connect to an 802.11a network which supports Static Turbo feature

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.

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

Bridge operating mode is selected by default as it is widely used by 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.

Router operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation – wireless clients will be on different IP subnet. Router mode will block broadcasts while it is not transparent. Device supports Multicast packet pass-through in Router mode. Router can act as DHCP server and use 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 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.

DHCP Fallback IP:

In case the Bridge is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here. In case the IP settings of the devices are unknown, they can be access with the help of the *UConfig utility*. The *UConfig Utility* should be started on the administrator PC which resides on the same network segment as the device.

Device will return to the default IP configuration (192.168.168.1/255.255.255.0) if the *Reset to defaults* routine is initiated.

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, UDP, P2P) 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 – Wireless with Router Mode

This section provides more details on wireless with router function.

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

- Wireless interface and all the wireless clients connected are considered as the internal LAN and the Ethernet interface is dedicated for the connection to the external network while the device is operating in AP/AP WDS wireless mode;
- Wireless interface and all the wireless clients connected is considered as the external network and the all the network devices on LAN side as well as the Ethernet interface itself is considered as the internal network while the device is operating in Station/Station WDS mode.

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

AP-Router mode Network Settings

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

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

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

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

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

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

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

Gateway IP address should be from the same address space (on the same network segment) as the device's external network interface (Wireless interface in the Station case and 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 to IP addresses. These fields identify the server IP addresses where the DNS requests are forwarded by the device.

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

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

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

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables nat table, while the device is operating in Router mode. Please refer to the [iptables tutorial](#) for detailed description of the NAT functionality in Router mode.

Static routes should be specified in order the packets should pass-through the based device if the NAT is disabled in while operating in Router network mode.

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

Range Start/End: This range determines the IP addresses given out by the DHCP server to client devices on the internal network which use dynamic IP configuration.

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

DHCP Fallback IP: In case the external network interface of the Router is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here. In case the IP settings of the device are unknown, they can be retrieved with the help of the UConfig utility and should be started on the administrator PC which resides on the same network segment as the device.

Port Forwarding Settings

Port Forwarding: Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for number of applications such as FTP servers, gaming, etc. where different host systems need to be seen using a single common IP address/port. Port Forwarding rules can be set in Port Forwarding window, which is 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 which 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 which is connected to the internal network. The specified port will be accessible from the external network;

Type is the L3 protocol (IP) type which needs to be forwarded from the internal network. Public Port is the TCP/UDP port of the based device which will accept and forward the connections from the external network to the host connected to the internal network.

Comments is the informal field for the comment of the particular port forwarding entry. Few words about the particular port forwarding entry purpose are saved there usually. Enabled flag enables or disables the effect of the particular port forwarding entry. All the added firewall entries are saved in system configuration file, however only the enabled port forwarding entries will be active during the system operation.

New entries in port forwarding can be saved by activating Save button or discarded by activating

Cancel button in the Port Forwarding configuration window.

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

Bridge mode Firewall Configuration Settings

Firewall functionality on any router interface can be enabled using the "Enable Firewall" option. Router Firewall rules can be configured, enabled or disabled while using Firewall configuration window which is opened with the "Configure" button. Firewall entries can be specified by using the following criteria:

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

IP Type sets which particular L3 protocol type (ICMP, TCP, UDP, P2P) should be filtered;

Source IP/mask 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 device operation.

New entries in Firewall can be saved by activating Apply Setting and Save Changes 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 iptables filter table, 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 which enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers. Select the IP Address option PPPoE to configure a PPPoE tunnel in order to connect to an ISP.

Only the external network interface can be configured as PPPoE client as all the traffic will be sent via this tunnel. The IP address, Default gateway IP and DNS server IP address will be obtained from the PPPoE server after PPPoE connection is established. Broadcast address is used for the PPPoE server discovery and tunnel establishment.

Valid authorization credentials are required for the PPPoE connection:

PPPoE Username – username to connect to the server (must match the configured on the PPPoE server);

Password – password to connect to the server (must match the configured on the PPPoE server);

PPPoE MTU/MRU – the size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for the data encapsulation

while transferring it through the PPP tunnel;

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

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

DMZ IP: connected to the internal network host, specified with the DMZ IP address will be accessible from the external network.

With a multicast design, applications can send one copy of each packet and address it to the group of computers that 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 which need to receive them. Common Routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however provides the multicast traffic pass-through functionality.

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

Appendix III- 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 802.11 data rates include 1, 2, 5.5, 11 Mbps for IEEE 802.11b mode and 6, 9, 12, 18, 24, 36, 48, 54Mbps for IEEE 802.11a/g mode. 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 interferers.

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 IV- Services

This section provides more details on the system management services.

Ping WatchDog

The ping watchdog sets the device to continuously ping a user defined IP address (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.



The information contained in this document is subject to change without notice and does not represent a commitment on the part of Aisai Communication Technology Co., Ltd. The information in this document is believed to be accurate and reliable; however, Aisai assumes no responsibility or liability for any errors or inaccuracies that may appear in the document.

All rights reserved. No part of this document may be reproduced or used in any form or by any means, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement of Aisai Communication Technology Co., Ltd.

Aisai Communication Technology Co., Ltd.

Technical Support Information

Tel: +86-755-26815616

Fax: +86-755-26815615

Website: www.aisaicom.com

E-mail: tech_support@aisai.com.cn

Copyright®
Aisai Communication Technology Co., Ltd.
All Rights Reserved, 2010