- **ACK Timeout :** ACK timeout is in the range of **1~255** and set in unit of ***microsecond***. The default value is **32** microsecond.

  All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughputs become low due to excessively high re-transmission.

  ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval :** Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1~255**. The default is **1**.

  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256~2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

  With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

- **Pkt_Aggregate :** By default, it's "***Enable***"

  Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.

- **IEEE802.11H (DFS) :** By default, it's "***Disable***". To ***Enable*** is to use IEEE802.11H(DFS)

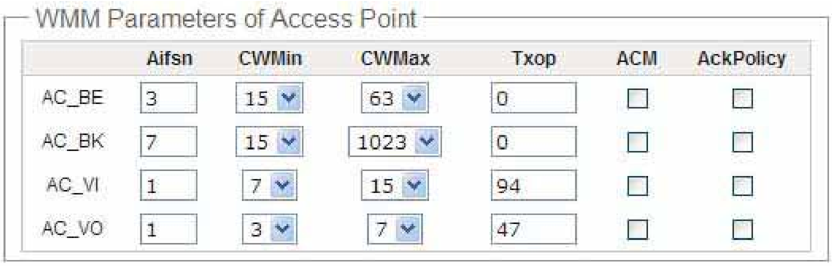
  With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

DFS Channels	52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

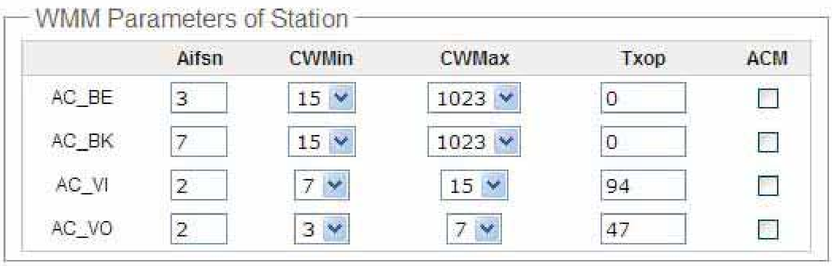
*The Channel **52-140** is DFS channel. If tuen on IEEE802.11H, AP Will have **60** sec to do channel available check, and will not send beacon and can not be connected. When WCB1200H2PX detect radar(5GHz) signal, the AP will switch channel and stop beacon trasmit between **15** sec.*

- **WMM :** By default, it's "***Disable***". To ***Enable*** is to use WMM and the WMM parameters should appears.



WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□



WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

WMM Parameters of Access Point : *This affects traffic flowing from the access point to the client station*

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM :** Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy :** Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"

  When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

  When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ ***WMM Parameters of Station :*** *This affects traffic flowing from the client station to the access point.*

Queue	Data Transmitted Clients to AP	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.

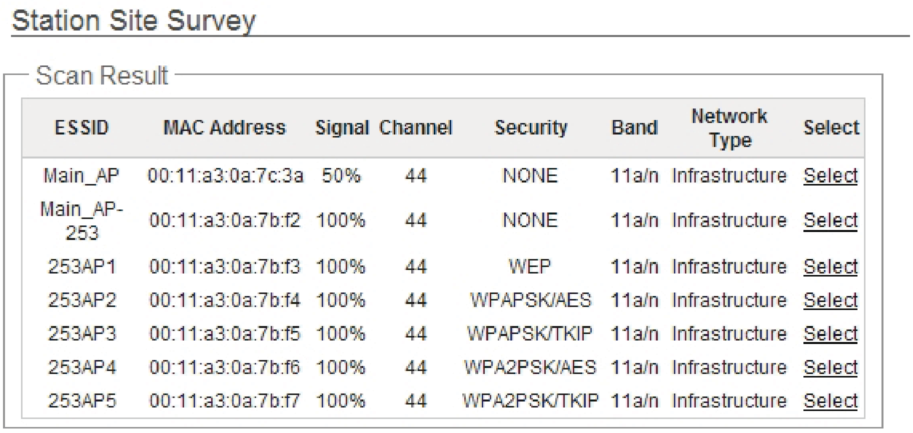
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM :** Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **Repeater AP**.

Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with.

Please click on **Wireless -> Site Survey**. Below depicts an example for site survey.



Station Site Survey

Scan Result

ESSID	MAC Address	Signal	Channel	Security	Band	Network Type	Select
Main_AP	00:11:a3:0a:7c:3a	50%	44	NONE	11a/n	Infrastructure	Select
Main_AP-253	00:11:a3:0a:7b:f2	100%	44	NONE	11a/n	Infrastructure	Select
253AP1	00:11:a3:0a:7b:f3	100%	44	WEP	11a/n	Infrastructure	Select
253AP2	00:11:a3:0a:7b:f4	100%	44	WPAPSK/AES	11a/n	Infrastructure	Select
253AP3	00:11:a3:0a:7b:f5	100%	44	WPAPSK/TKIP	11a/n	Infrastructure	Select
253AP4	00:11:a3:0a:7b:f6	100%	44	WPA2PSK/AES	11a/n	Infrastructure	Select
253AP5	00:11:a3:0a:7b:f7	100%	44	WPA2PSK/TKIP	11a/n	Infrastructure	Select

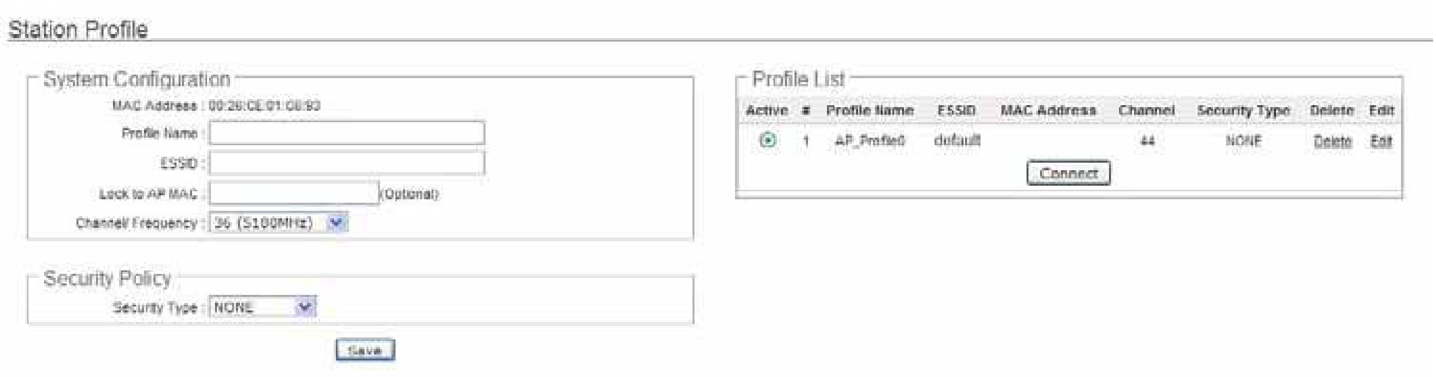
- **ESSID : Available** Extend Service Set ID of surrounding Access Points.
- **MAC Address :** MAC addresses of surrounding Access Points.
- **Signal :** Received signal strength of all found Access Points.
- **Channel :** Channel numbers used by all found Access Points.
- **Security :** Security type by all found Access Points.
- **Band :** Wireless band used by all found Access Points.
- **Network Type :** Network type used by all found Access Points.
- **Select :** Click “**Select**” to configure settings and associate with chosen AP.

*While clicking “Select” button in the Site Survey Table, the “**ESSID**” and “**Security Type**” will apply in the **Wireless Profile** Setup. However, more settings are needed including Security Key.*

Create Wireless Profile

The administrator can configure station profiles via this page.

Please click on **Wireless -> Wireless Profile** and follow the below setting.



Station Profile

System Configuration

MAC Address : 00:26:CE:01:08:93

Profile Name :

ESSID :

Lock to AP MAC : (Optional)

Channel/ Frequency : 36 (5180MHz)

Security Policy

Security Type : NONE

Profile List

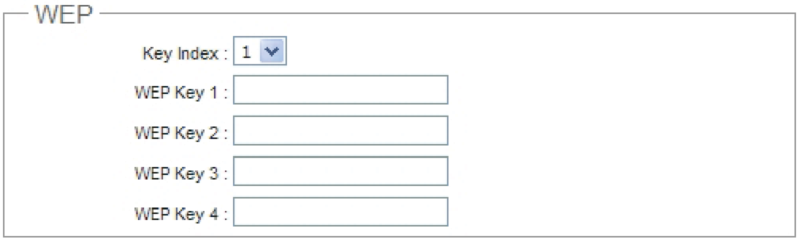
Active	#	Profile Name	ESSID	MAC Address	Channel	Security Type	Delete	Edit
●	1	AP_Profile0	default		44	NONE	Delete	Edit

- **MAC Address :** The MAC address of the Wireless Station is displayed here.
- **Profile Name :** Set different profiles for quick connection uses.
- **ESSID :** Assign Service Set ID for the wireless system.
- **Lock to AP MAC :** This allows the station to always maintain connection to a particular AP with a specific MAC address. This is useful as sometimes there can be few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to MAC address and not roam between several Access Points with the same ESSID.
- **Channel/Frequency :** Select the desired channel range.

> *In **CPE+AP** or **Client Bridge+Universal Repeater** mode, the Sation's channel must be **same** with AP. If* TEW-676APBO *configure different channel with AP,* TEW-676APBO ***unable*** *connect to AP.*

- **Security Type :** Select the desired security type from the drop-down list; the options are “**NONE**” “**OPEN**”, “**SHARED**”, “**WPA-PSK**” and “**WPA2-PSK**”.

➔ **OPEN / SHARED :** OPEN and SHARED require the user to set a WEP key to exchange data.



WEP

Key Index : 1

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

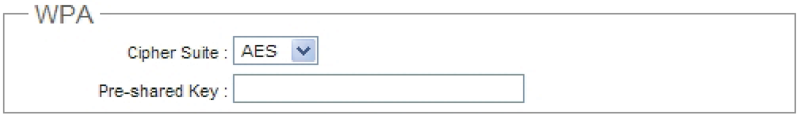
WEP Key 4 :

✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.

✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	**Hex**	**ASCII**
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

➔ **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.



WPA

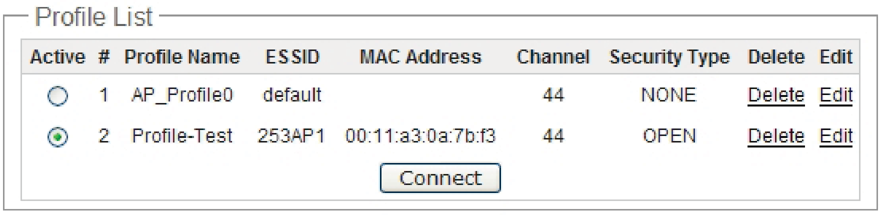
Cipher Suite : AES

Pre-shared Key :

✓ **Cipher Suite :** Select the desired cipher suite from the drop-down list; the options are **AES** and **TKIP**

✓ **Pre-shared Key :** Enter the information for pre-shared key; the key can be either entered as a 256-bit secret in **64 HEX** digits format, or **8 to 63 ASCII** characters.

■ **Profile List :** The user can manage the created profiles for home, work or public areas. Below depict an example for Profile List



Profile List

Active	#	Profile Name	ESSID	MAC Address	Channel	Security Type	Delete	Edit
○	1	AP_Profile0	default		44	NONE	Delete	Edit
●	2	Profile-Test	253AP1	00:11:a3:0a:7b:f3	44	OPEN	Delete	Edit

➔ Click “”**Edit**” an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click “**Save**” button to save the profile.

➔ Click “**Delete**” to remove profile.

➔ Click and Select a profile from list, then click the “**Connect**” button to connecting to the wireless network with the profile setting. After clicking “**Connect**” button, the system should be jump to **Remote AP Page**, you can verify connecting status on **Remote AP Page**.

*When you click “**Save**” button on this page, the system will connect to specify AP and jump to **Remote AP Page***

If tuen on IEEE802.11H and TEW-676APBO *connect AP with DFS channel **52-140**,* TEW-676APBO *Will have **60** sec to do channel available check, and will not send beacon and can not be connected.*

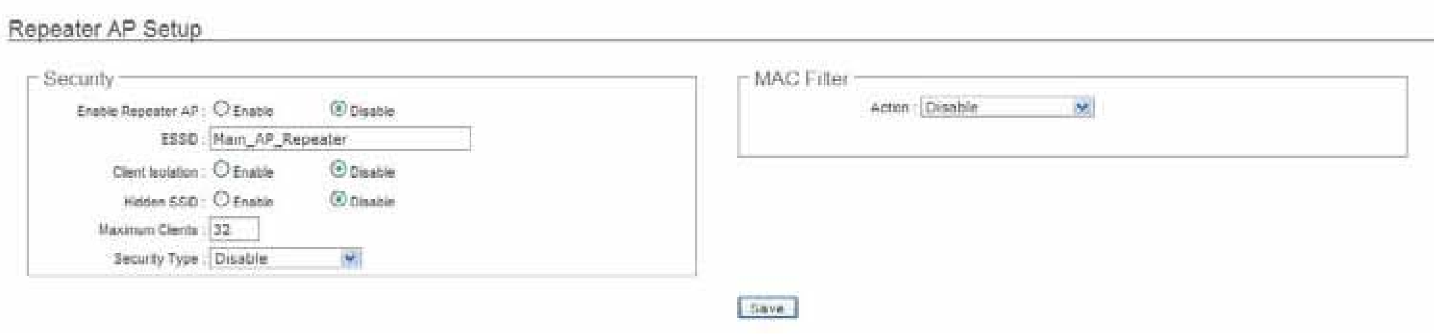
Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Wireless LAN Network Creation

The network manager can configure related wireless settings, **Repeater AP Setup, Security Settings,** and **MAC Filter Settings**.

Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and MAC Filter settings.



Repeater AP Setup

Security

Enable Repeater AP : ○ Enable ● Disable

ESSID : Main_AP_Repeater

Client Isolation : ○ Enable ● Disable

Hidden SSID : ○ Enable ● Disable

Maximum Clients : 32

Security Type : Disable

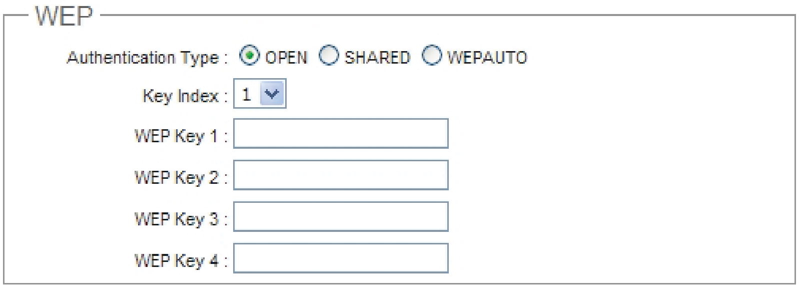
MAC Filter

Action : Disable

- **Enable Repeater AP :** By default, it’s “**En*able***” for repeater AP. Select “***Enable***” to activate Repeater AP or click “***Disable***” to deactivate this function
- **ESSID :** Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP's clients associated with the specified AP.
- **Client Isolation :** By default, it’s “***Disable***”.

  Select “**Enable”**, all clients will be isolated from each other, which means they can’t reach each other.
- **Hidden SSID :** By default, it’s “***Disable***”.

  Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It’s suggested to enable it after AP security settings are archived and setting of AP's clients could make to associate to it.
- **Maximum Clients :** The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this Repeater AP.
- **Security Type :** Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
  - ➔ **Disable :** Data are unencrypted during transmission when this option is selected.
  - ➔ **WEP :** Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.



WEP

Authentication Type : ● OPEN ○ SHARED ○ WEPAUTO

Key Index : 1

WEP Key 1 :

WEP Key 2 :

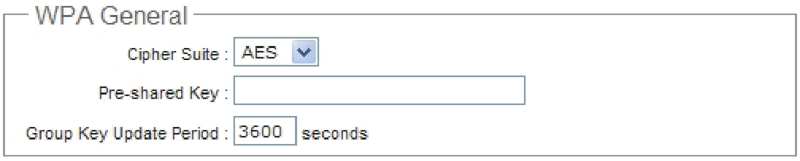
WEP Key 3 :

WEP Key 4 :

- ✓ **Authentication Method :** Enable the desire option among ***OPEN***, ***SHARED*** or ***WEPAUTO***.
- ✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	**Hex**	**ASCII**
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

➔ **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.



WPA General

Cipher Suite : AES

Pre-shared Key :

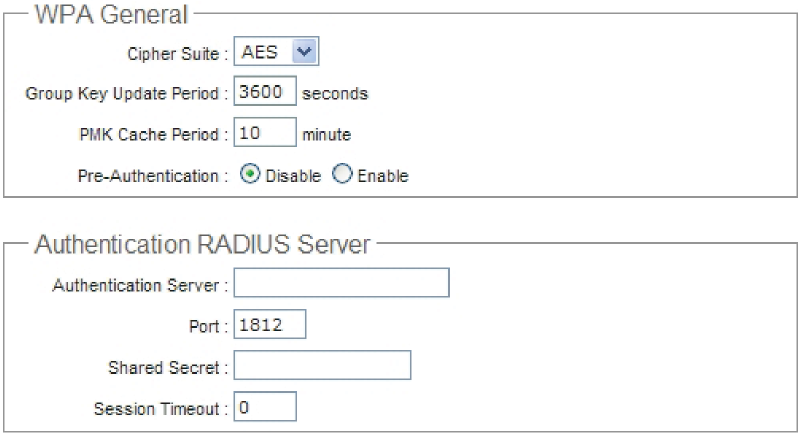
Group Key Update Period : 3600 seconds

- ✓ **Cipher Suite :** By default, it is **AES**. Select either AES or TKIP cipher suites
- ✓ **Pre-shared Key :** Enter the pre-shared key; the format shall go with the selected key type.

Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

- ✓ **Group Key Update Period :** By default, it is **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

➔ **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this is selected.



WPA General

Cipher Suite : AES

Group Key Update Period : 3600 seconds

PMK Cache Period : 10 minute

Pre-Authentication : ● Disable ○ Enable

Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

Session Timeout : 0

✓ **WPA General Settings :**

- **Cipher Suite :** By default, it is AES. Select either AES or TKIP cipher suites
- **Group Key Update Period :** By default, it's **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- **PMK Cache Period :** By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- **Pre-Authentication :** By default, it's "Disable". To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.

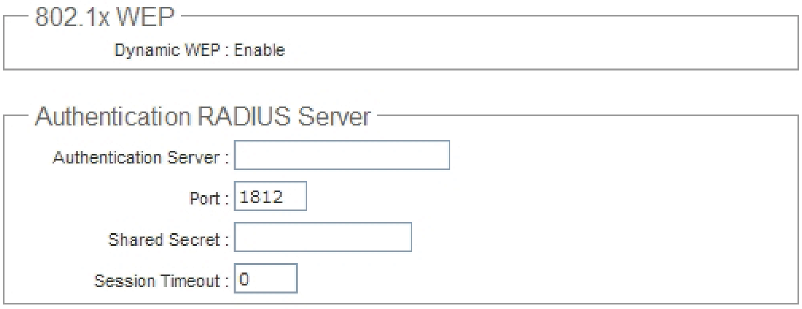
PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise

✓ **Radius Server Settings :**

- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60** *seconds*. The default is **0** to disable re-authenticate service.

  Amount of time before a client will be required to re-authenticate.

- **WEP 802.1X :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.



802.1x WEP

Dynamic WEP : Enable

Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

Session Timeout : 0

✓ **Radius Server Settings :**

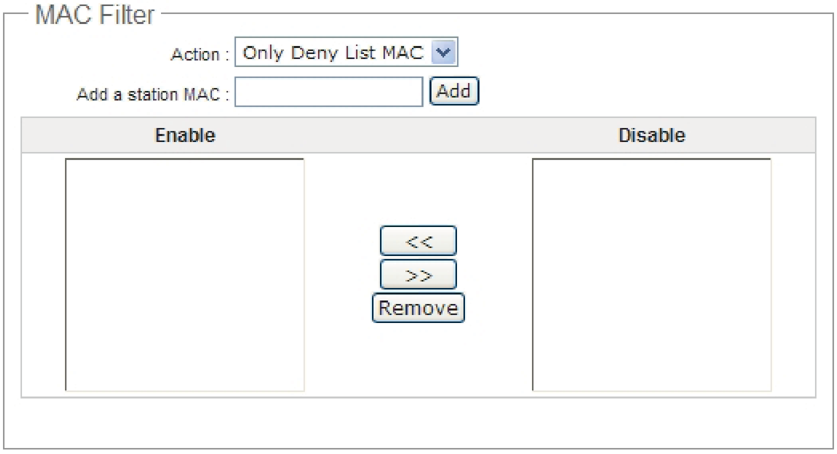
- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60** *seconds*. The default is **0** to disable re-authenticate service.

  Amount of time before a client will be required to re-authenticate.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Wireless MAC Filter Setup

Continue **6.3.1 Repeater AP Setup** section, the administrator can allow or reject clients to access Repeater AP.



MAC Filter

Action : Only Deny List MAC

Add a station MAC :

- **MAC Filter Setup :** By default, it's "***Disable***". Options are **Disable, Only Deny List MAC or Only Allow List MAC**.

  Two ways to set MAC filter rules :

  ➔ **Only Allow List MAC**.

  The wireless clients in the "**Enable**" list will be **allowed** to access the Access Point; All others or clients in the "**Disable**" list will be **denied**.

  ➔ **Only Deny List MAC**.

  The wireless clients in the "**Enable**" list will be **denied** to access the Access Point; All others or clients in the "**Disable**" list will be **allowed**.

- **Add a station MAC :** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the "**Enable**" List.

There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons**.**

Click ***Reboot*** button to activate your changes

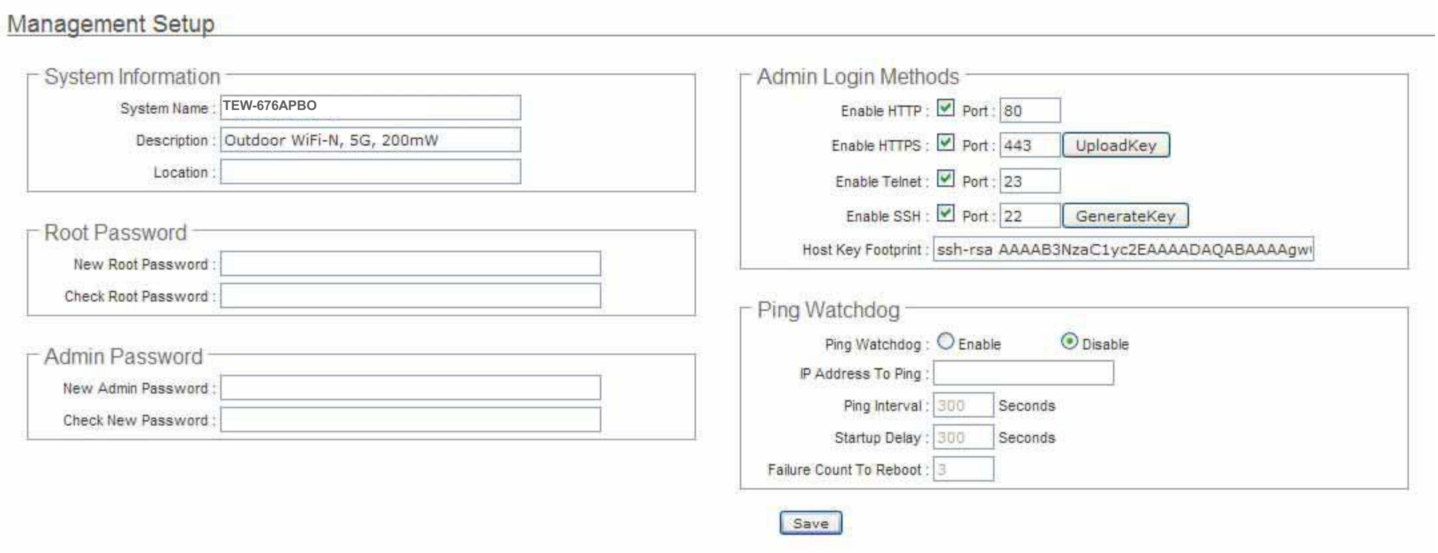
MAC Access Control is the weakest security approach. WPA or WPA2 security method is highly recommended.

System Management

Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.



Management Setup

System Information

System Name : TEW-676APBO

Description : Outdoor WiFi-N, 5G, 200mW

Location :

Root Password

New Root Password :

Check Root Password :

Admin Password

New Admin Password :

Check New Password :

Admin Login Methods

Enable HTTP : ☑ Port : 80

Enable HTTPS : ☑ Port : 443 UploadKey

Enable Telnet : ☑ Port : 23

Enable SSH : ☑ Port : 22 GenerateKey

Host Key Footprint : ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgw

Ping Watchdog

Ping Watchdog : ○ Enable ● Disable

IP Address To Ping :

Ping Interval : 300 Seconds

Startup Delay : 300 Seconds

Failure Count To Reboot : 3

- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default one.
  - ➔ **Description :** Provide description of the system.
  - ➔ **Location :** Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to ***Appendix D. Network manager Privileges***.

- **Root Password :** Log in as a root user and is allowed to change its own, plus admin user's password.
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Password :** Log in as a admin user and is allowed to change its own,
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Login Methods :** Only **root** user can enable or disable system login methods and change services port.

➔ **Enable HTTP :** Check to select HTTP Service.

➔ **HTTP Port :** The default is 80 and the range is between 1 ~ 65535.

➔ **Enable HTTPS :** Check to select HTTPS Service

➔ **HTTPS Port :** The default is 443 and the range is between 1 ~ 65535.

*If you already have an SSL Certificate, please click “**UploadKey**” button to select the file and upload it.*

➔ **Enable Telnet :** Check to select Telnet Service

➔ **Telnet Port :** The default is 23 and the range is between 1 ~ 65535.

➔ **Enable SSH :** Check to select SSH Service

➔ **SSH Port :** Please The default is 22 and the range is between 1 ~ 65535.

*Click “**GenerateKey**” button to generate RSA private key. The “host key footprint” gray blank will display content of RSA key.*

- **Ping Watchdog :** The ping watchdog sets the TEW-676APBO 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 TEW-676APBO 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 :** specify an IP address of the target host which will be monitored by Ping Watchdog Tool.

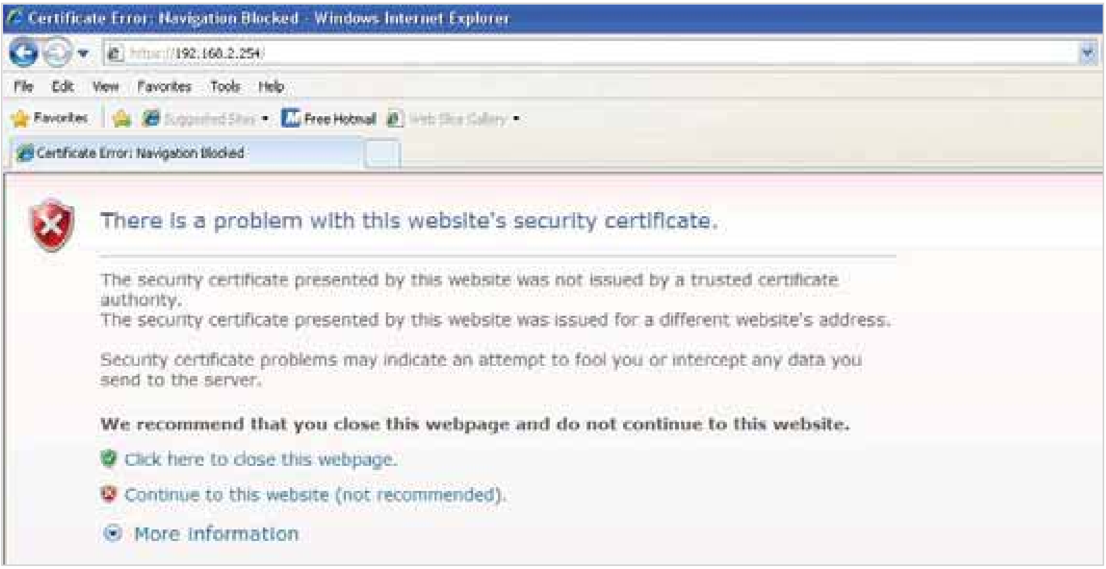
  ➔ **Ping Interval :** specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool. Default is **300** seconds.

  ➔ **Startup Delay :** specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** 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.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (https://192.168.2.254). There will be a "Certificate Error", because the browser treats system as an illegal website.



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.2.254/
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

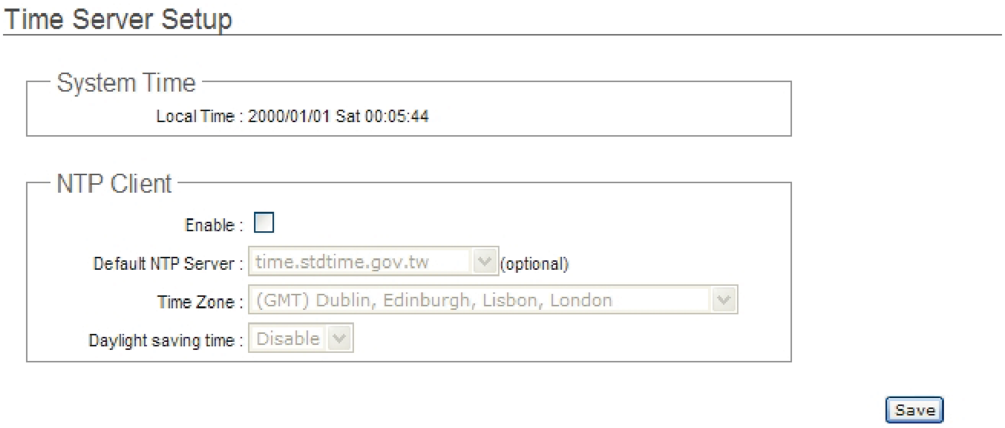
More information

Click "***Continue to this website***" to access the system's WMI. The system's Overview page will appear.

Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.



Time Server Setup

System Time

Local Time : 2000/01/01 Sat 00:05:44

NTP Client

Enable : □

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight saving time : Disable

- **Local Time :** Display the current system time.

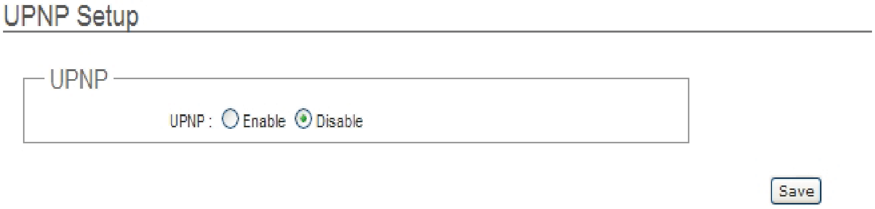
- **NTP Client :** To synchronize the system time with NTP server.
  - ➔ **Enable :** Check to select NTP client.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Select a desired time zone from the drop-down list.
  - ➔ **Daylight saving time :** Enable or disable Daylight saving.

If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.



UPNP Setup

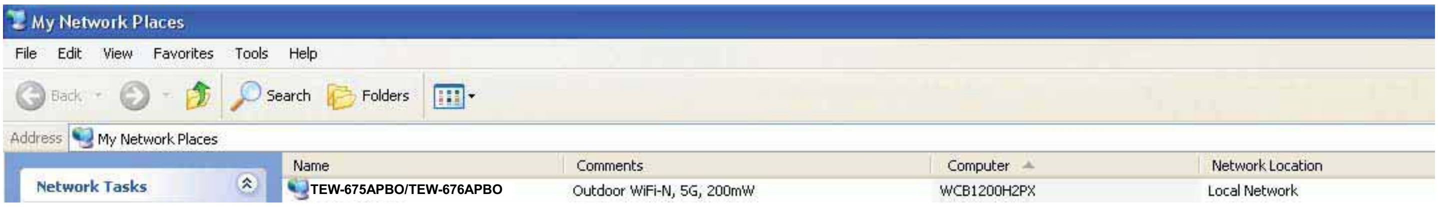
UPNP

UPNP : ○ Enable ● Disable

- **UPnP :** By default, it's "***Disable***". Select "**Enable**" or "***Disable"*** of UPnP Service.

Click ***Save*** button to save changes and click ***Reboot*** button to activate changes

For UPnP to work in Windows XP, the "TEW-676APBO" must be available in "***My Network Places***", as shown here: (your specific model may vary)

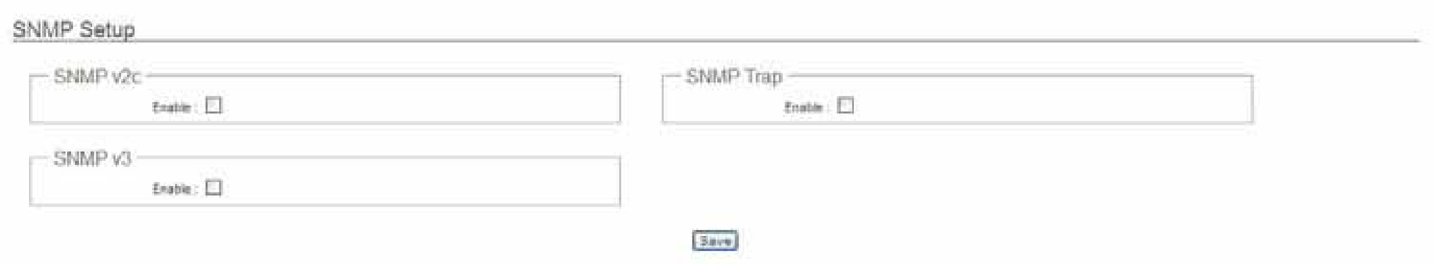


Name	Comments	Computer	Network Location
TEW-675APBO/TEW-676APBO	Outdoor WiFi-N, 5G, 200mW	WCB1200H2PX	Local Network

Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.



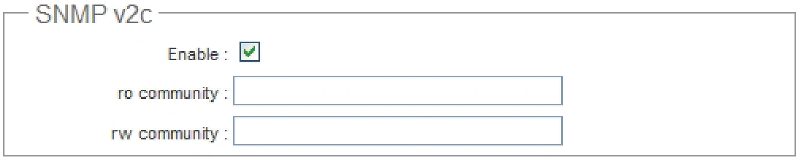
SNMP Setup

SNMP v2c
Enable : □

SNMP Trap
Enable : □

SNMP v3
Enable : □

- **SNMP v2c Enable:** Check to enable SNMP v2c.

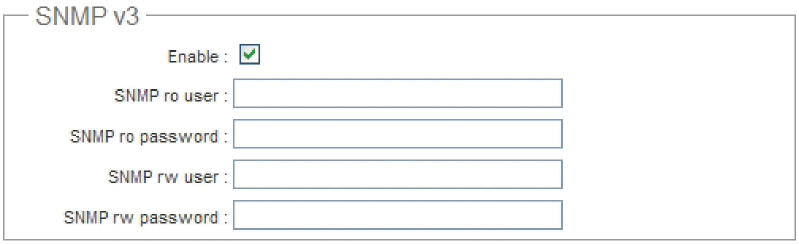


SNMP v2c
Enable : ☑
ro community :
rw community :

- ➔ **ro community :** Set a community string to authorize read-only access.
- ➔ **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

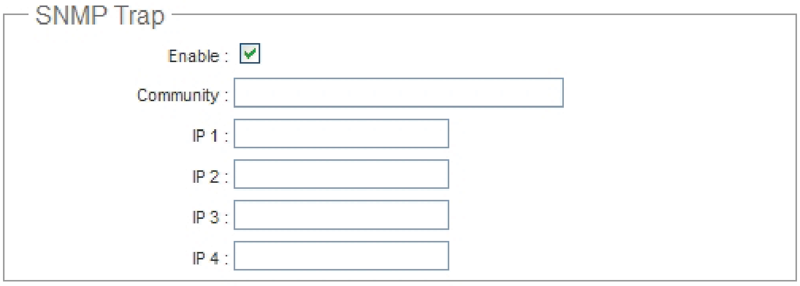
SNMPv3 supports the highest level SNMP security.



SNMP v3
Enable : ☑
SNMP ro user :
SNMP ro password :
SNMP rw user :
SNMP rw password :

- ➔ **SNMP ro user :** Set a community string to authorize read-only access.
- ➔ **SNMP ro password :** Set a password to authorize read-only access.
- ➔ **SNMP rw user :** Set a community string to authorize read/write access.
- ➔ **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.



SNMP Trap

Enable : ☑

Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

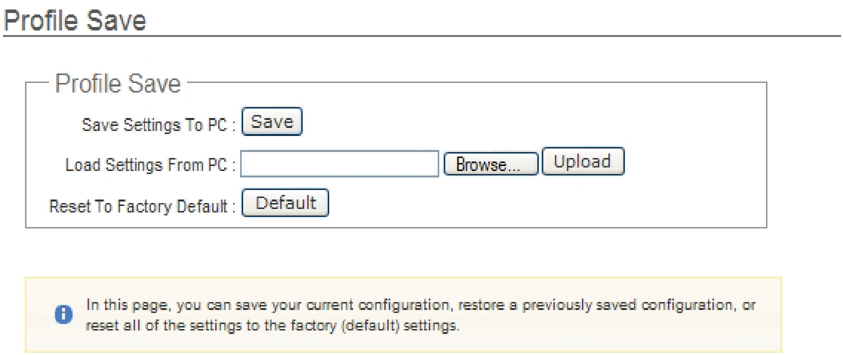
- ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

Click ***Save*** button to save changes and click ***Reboot*** button to activate.

Backup / Restore and Reset to Factory

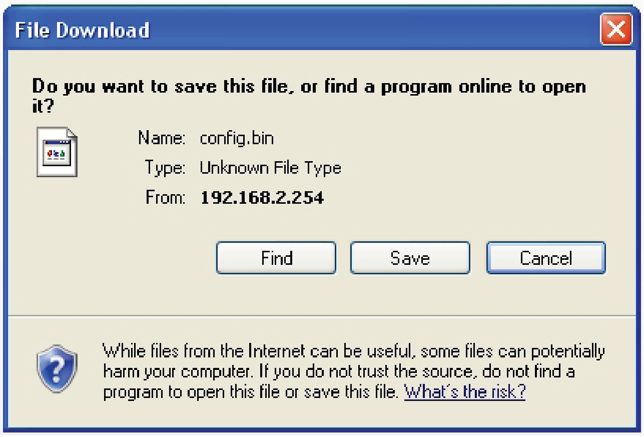
Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.



In this page, you can save your current configuration, restore a previously saved configuration, or reset all of the settings to the factory (default) settings.

- **Save Settings to PC :** Click ***Save*** button to save the current configuration to a local disk.



Do you want to save this file, or find a program online to open it?

Name: config.bin

Type: Unknown File Type

From: 192.168.2.254

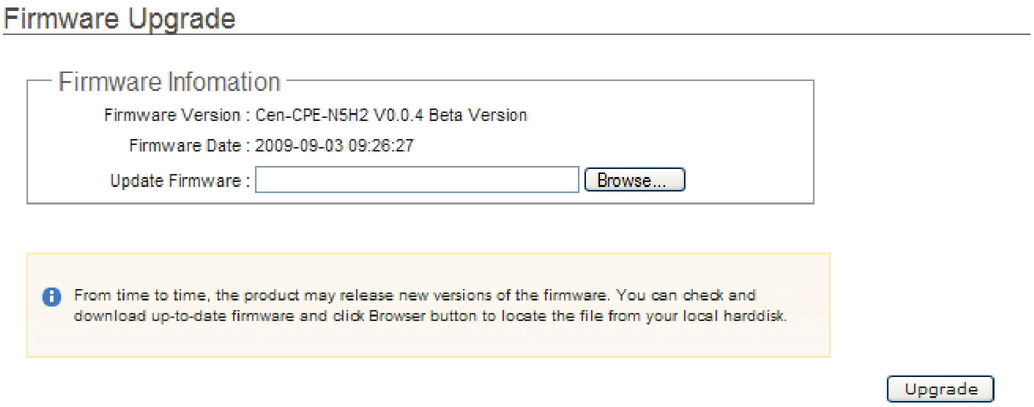
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click ***Browse*** button to locate the new firmware, and then click ***Upgrade*** button to upgrade.



Firmware Upgrade

Firmware Infomation

Firmware Version : Cen-CPE-N5H2 V0.0.4 Beta Version

Firmware Date : 2009-09-03 09:26:27

Update Firmware :

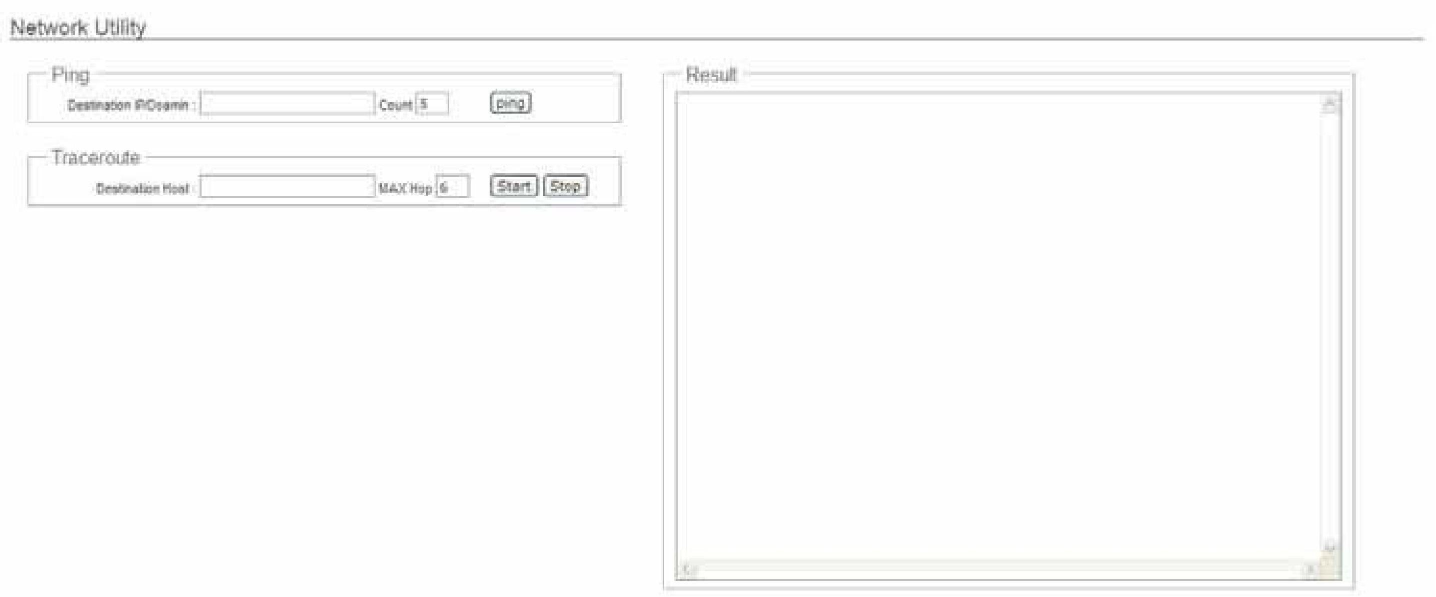
From time to time, the product may release new versions of the firmware. You can check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.

1. *To prevent data loss during firmware upgrade, please back up current settings before proceeding.*
2. *Do not interrupt during firmware upgrade including power on/off as this may damage system.*
3. *Never perform firmware upgrade over wireless connection or via remote access connection.*

Network Utility

The administrator can diagnose network connectivity via the PING and TRACEROUTE utility.

Please click on **Utilities -> Network Utility** and follow the below setting



Destination IP/Doamin :
Count 5

Destination Host :
MAX Hop 6

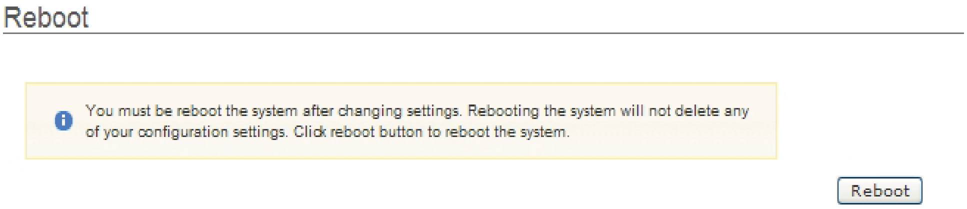
- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - ➔ **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - ➔ **Count :** By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

- **Traceroute :** Allows tracing the hops from the TEW-676APBO device to a selected outgoing IP

  address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click Stop button to stopped test
  - ➔ **Destination Host :** Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
  - ➔ **MAX Hop :** Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

Reboot

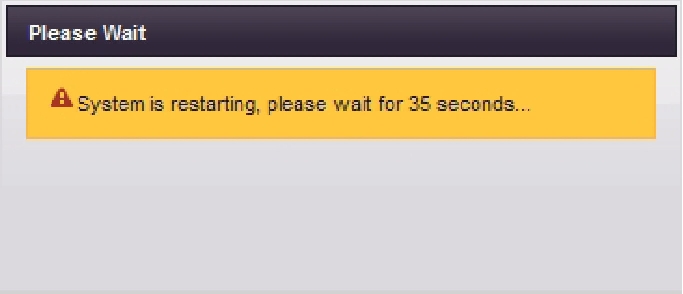
This function allows user to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.



Reboot

You must be reboot the system after changing settings. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



Please Wait

System is restarting, please wait for 35 seconds...

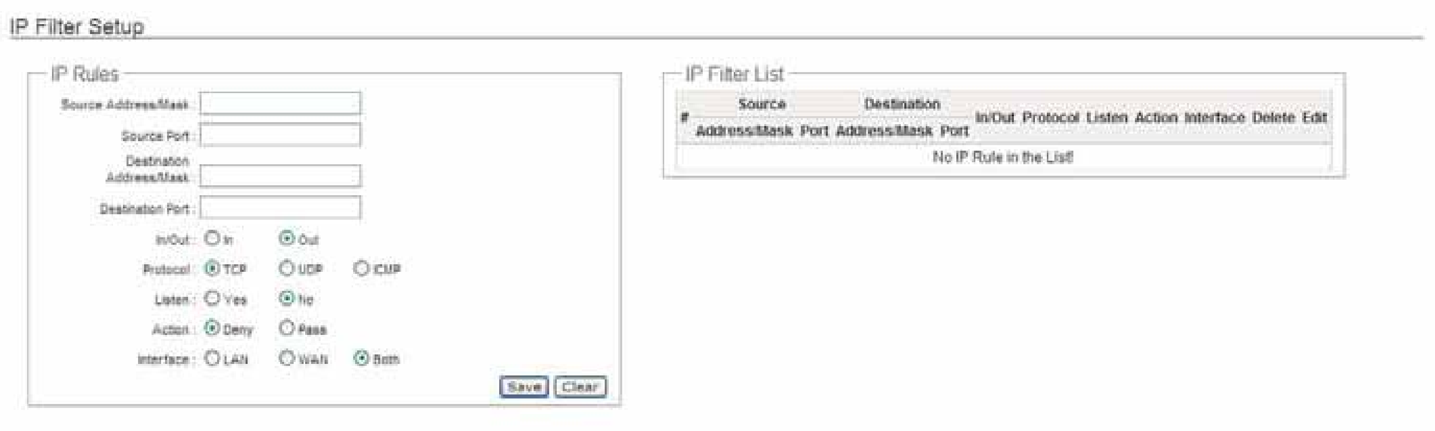
The **System Overview** page appears upon the completion of reboot.

Access Control List

IP Filter Setup

Allows to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports.   Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules.

Please click on **Advance -> IP Filter Setup** and follow the below setting.



IP Filter Setup

IP Rules

Source Address/Mask :
Source Port :
Destination Address/Mask :
Destination Port :
In/Out : ○ In ● Out
Protocol : ● TCP ○ UDP ○ ICMP
Listen : ○ Yes ● No
Action : ● Deny ○ Pass
Interface : ○ LAN ○ WAN ● Both

IP Filter List

#	Source		Destination		In/Out	Protocol	Listen	Action	Interface	Delete	Edit
	Address/Mask	Port	Address/Mask	Port							
No IP Rule in the List!											

- **Source Address/Mask :** Enter desired source IP address and netmask; i.e. 192.168.2.10/32.
- **Source Port :** Enter a port or a range of ports as ***start:end***; i.e. port 20:80
- **Destination Address/Mask :** Enter desired destination IP address and netmask; i.e. 192.168.1.10/32
- **Destination Port :** Enter a port or a range of ports as ***start:end***; i.e. port 20:80
- **In/Out :** Applies to Ingress or egress packets
- **Protocol :** Supports ***TCP***, ***UDP*** or ***ICMP***.
- **Listen :** Click ***Yes*** radial button to match TCP packets only with the SYN flag.
- **Active :** ***Deny*** to drop and ***Pass*** to allow per filter rules
- **Interface :** The interface that a filter rule applies

All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

Click "**Save**" button to add IP filter rule. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. Click ***Reboot*** button to activate your changes.

When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

➔ **Example 1 :** Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

Rule	**Source**		**Destination**		**In/Out**	**Protocol**	**Listen**	**Action**	**Side**
	IP/Mask	**Port**	**IP/Mask**	**Port**					
1	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN

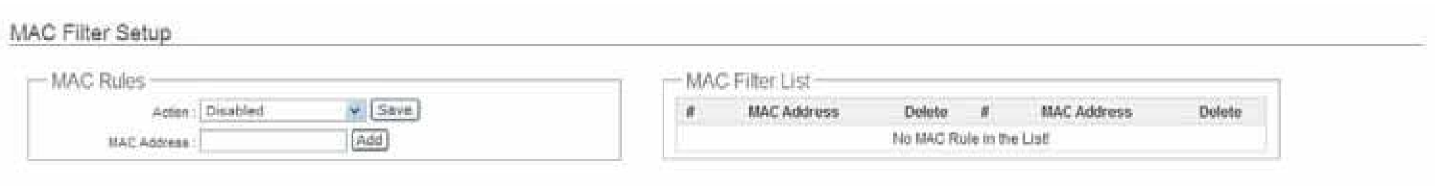
➔ **Example 2 :** All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won’t make any difference.

Rule	**Source**		**Destination**		**In/Out**	**Protocol**	**Listen**	**Action**	**Side**
	IP/Mask	**Port**	**IP/Mask**	**Port**					
1	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN
2	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	pass	LAN

MAC Filter Setup

Allows to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important to note that MAC filter rules have precedence over IP Filter rules.

Please click on **Advance -> MAC Filter Setup** and follow the below setting.



MAC Filter Setup

MAC Rules

Action : Disabled [Save]

MAC Address : [Add]

MAC Filter List

#	MAC Address	Delete	#	MAC Address	Delete
No MAC Rule in the List!					

- **MAC Filter Rule :** By default, it's "***Disable***". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**. Click ***Save*** button to save your change.

  Two ways to set the MAC Filter List:

  ➔ **Only Allow List MAC**.

  The wireless clients in the MAC Filter List will be **allowed** to access to Access Point; All others will be denied.

  ➔ **Only Deny List MAC**.

  The wireless clients in the MAC Filter List will be **denied** to access to Access Point; All others will be allowed.

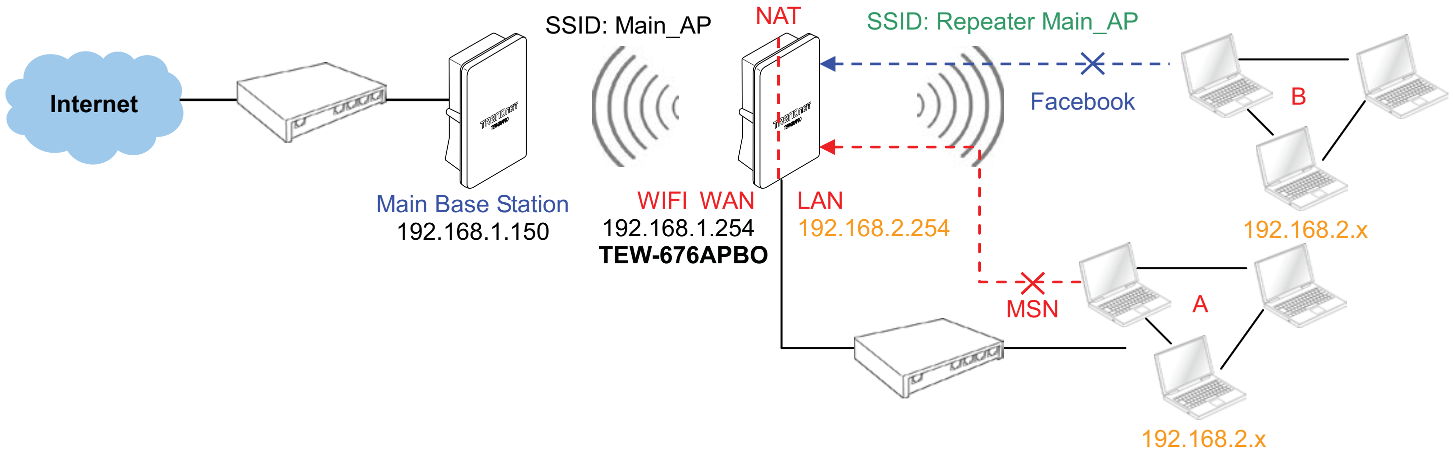
- **MAC Address :** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.

There are a maximum of **20** clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Delete** buttons***.***

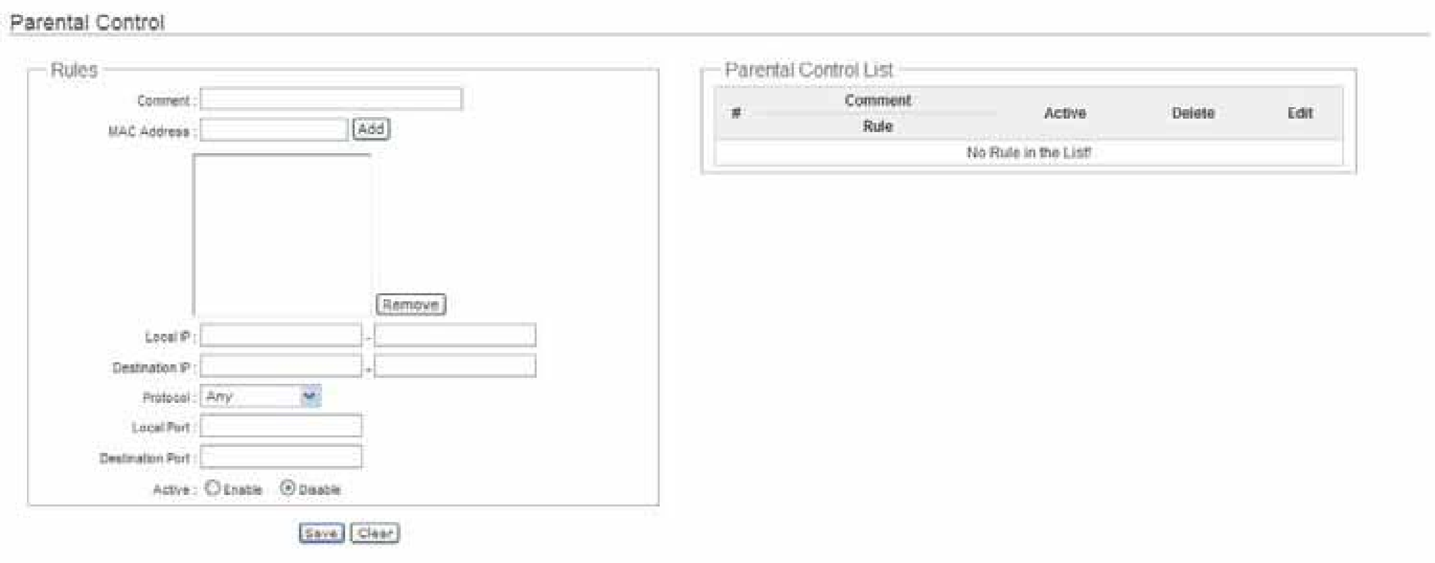
Click ***Reboot*** button to activate your changes

Parental Control Setup

Parental Control allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites.



Please click on **Advance -> Parental Control** and follow the below setting.


Parental Control

Rules

Comment :

MAC Address :

Local IP : -

Destination IP : -

Protocol : Any

Local Port :

Destination Port :

Active : ○ Enable ● Disable

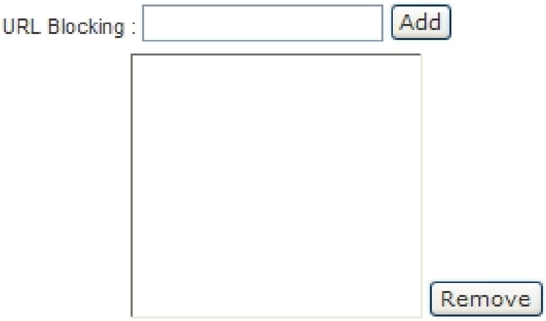
Parental Control List

#	Comment Rule	Active	Delete	Edit
No Rule in the List!				

- **Rules :** control can be managed by a rule. Use the settings on this screen to establish an access policy.
  - ➔ **Comment :** Enter a descriptive name for this rule for identifying purposes.
  - ➔ **MAC Address :** Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click "**Add**" button to add in the MAC group of each rule. Click "**Remove**" button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
  - ➔ **Local / Destination IP :** Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.

- **Protocol :** Select **Any** or specify protocol(**TCP**, **UDP**, **ICMP**, **URL Blocking** and **Application**) from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Local(LAN)/ Destination Port can not used.

  If you want to block websites with specific URL address or using specific keywords, enter each URL or keyworks in the "**URL Blocking**" field and click "**Add**" button to add in the URL Blocking list of each rule. Click "**Remove**" button can remove URL or keywords.



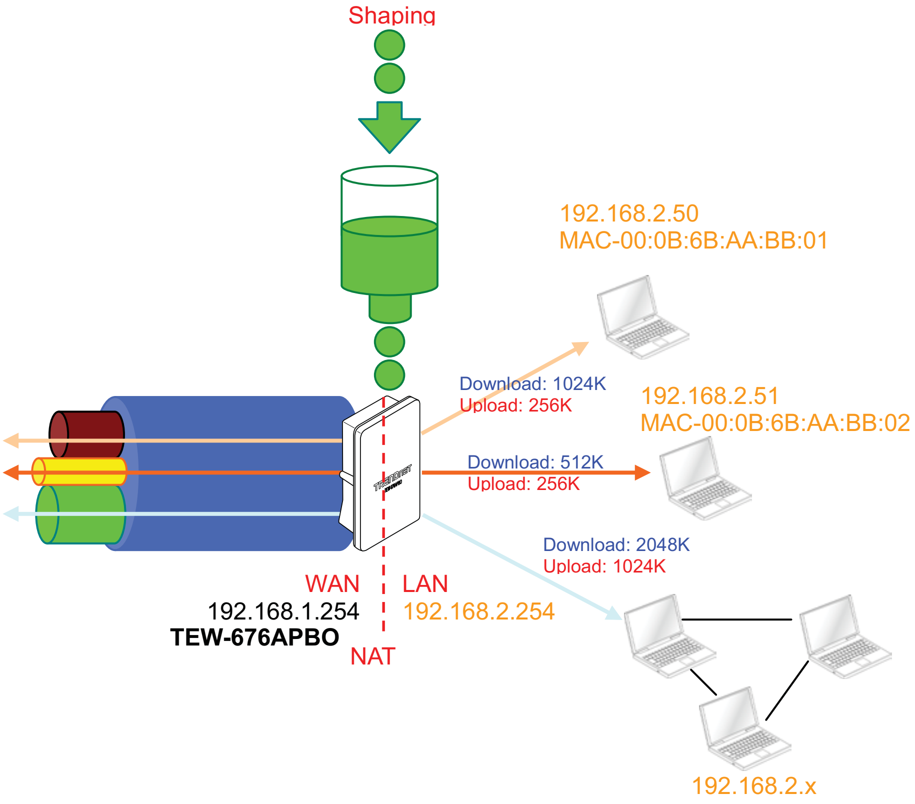
- **Local Port :** Specify local port(LAN port) range required for this rule
- **Destination Port :** Specify destination port range required for this rule
- **Active :** Check ***Enable*** button to activate this rule, and ***Disable*** to deactivate.

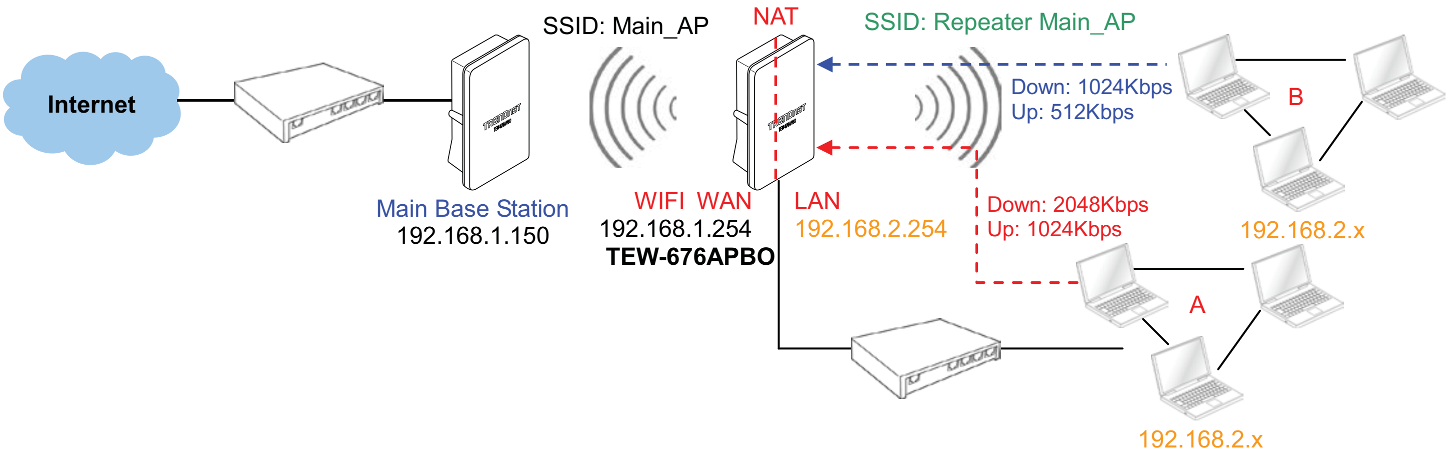
Click "**Add**" button to add control rule to List. There are **10** rules maximum allowed in this Control List. All rules can be removed or edited on the List. Click ***Reboot*** button to activate your changes.

QoS Setup

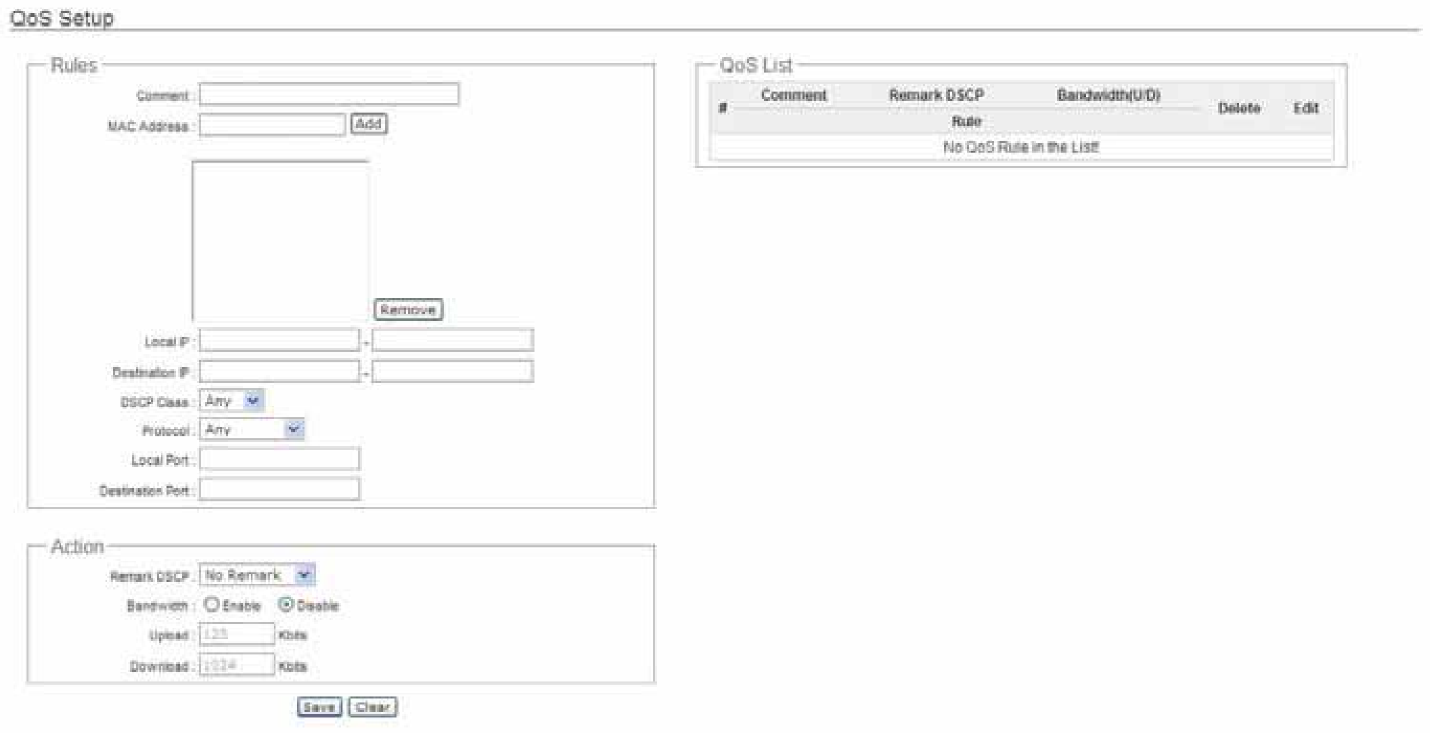
Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as FTP) to form a flow.





Please click on **Advance -> QoS** and follow the below setting.



QoS Setup

Rules

Comment :

MAC Address :

Local IP : -

Destination IP : -

DSCP Class : Any

Protocol : Any

Local Port :

Destination Port :

Action

Remark DSCP : No Remark

Bandwidth : ○ Enable ● Disable

Upload : 128 Kbits

Download : 1024 Kbits

QoS List

#	Comment	Remark DSCP	Bandwidth(U/D)	Delete	Edit
		Rule			
		No QoS Rule in the List!			

- **Rules :** Use the rules to define the classifiers. After you define the rules, you can specify action to act upon the traffic that matches the rules
  - ➔ **Comment :** Enter a descriptive name for this rule for identifying purposes.
  - ➔ **MAC Address :** Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click "**Add**" button to add in the MAC group of each rule. Click "**Remove**" button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
  - ➔ **Local / Destination IP :** Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.
  - ➔ **DSCP Class** : Differentiated services code point, DSCP. Select Any or specify classify traffic from drop-down list.

    The Per-Hop Behavior (PHB) is indicated by encoding a 6-bit value—called the Differentiated Services Code Point (DSCP)—into the 8-bit Differentiated Services (DS) field of the IP packet header. Below depicts class for DSCP.

    - ✓ **BE :** *Default* PHB, which is typically best-effort traffic
    - ✓ **EF :** *Expedited Forwarding* PHB, dedicated to low-loss, low-latency traffic
    - ✓ **AF :** *Assured Forwarding* PHB, which gives assurance of delivery under conditions. The AF behavior group defines four separate AF classes. Within each class, packets are given a drop precedence (high, medium or low). The combination of classes and drop precedence yields twelve separate DSCP encodings from **AF11** through **AF43** (see table)

DROP Precedence	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11	AF21	AF31	AF41
Medium Drop	AF12	AF22	AF32	AF42
High Drop	AF13	AF23	AF33	AF43

- ➔ **Protocol :** Select **Any** or specify protocol from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Source/ Destination Port cannot be used.
- ➔ **Local Port :** Specify local port(LAN port) range required for this rule
- ➔ **Destination Port :** Specify destination port range required for this rule

- ■ **Action :** After configuring rule, a policy rule ensures that a traffic flow gets the requested treatment in the network.
  - ➔ **Remark DSCP :** Specify a new DSCP class, if you want to replace or remark the DSCP
  - ➔ **Bandwidth :** Click "**Enable**" to activate function, and click "**Disable**" to deactivate function
  - ➔ **Upload / Download :** Specify the bandwidth in kilobit per second (Kbps). Enter a number between **8** to **8192**, default upload is **128** Kbps, download is **1024** Kbps.

Click "**Add**" button to add QoS rule to List. There are **10** rules maximum allowed in this QoS List. All rules can be removed or edited on the List. Click ***Reboot*** button to activate your changes.

When you create rules on the QoS List, the previous rules have higher priority. . Below depict the examples for explaining priority of QoS setup.

- ➢ **Example 1 :** On this setting, the FTP has **1024** Kbps upload and **8196** Kbps download on **192.168.2.10**. The remaining IP address and other remaining protocol of IP address 192.168.2.10 only can use total bandwidth **512** Kbps bandwidth. Because rule 1's priority is higher than rule 2

Rule	Source IP	Destination IP	DSCP	Protocol	Remark DSCP	Bandwidth (Up/Down)
1	192.168.2.10		ANY	FTP	NO	1024/8196
2			ANY	ANY	NO	512/512

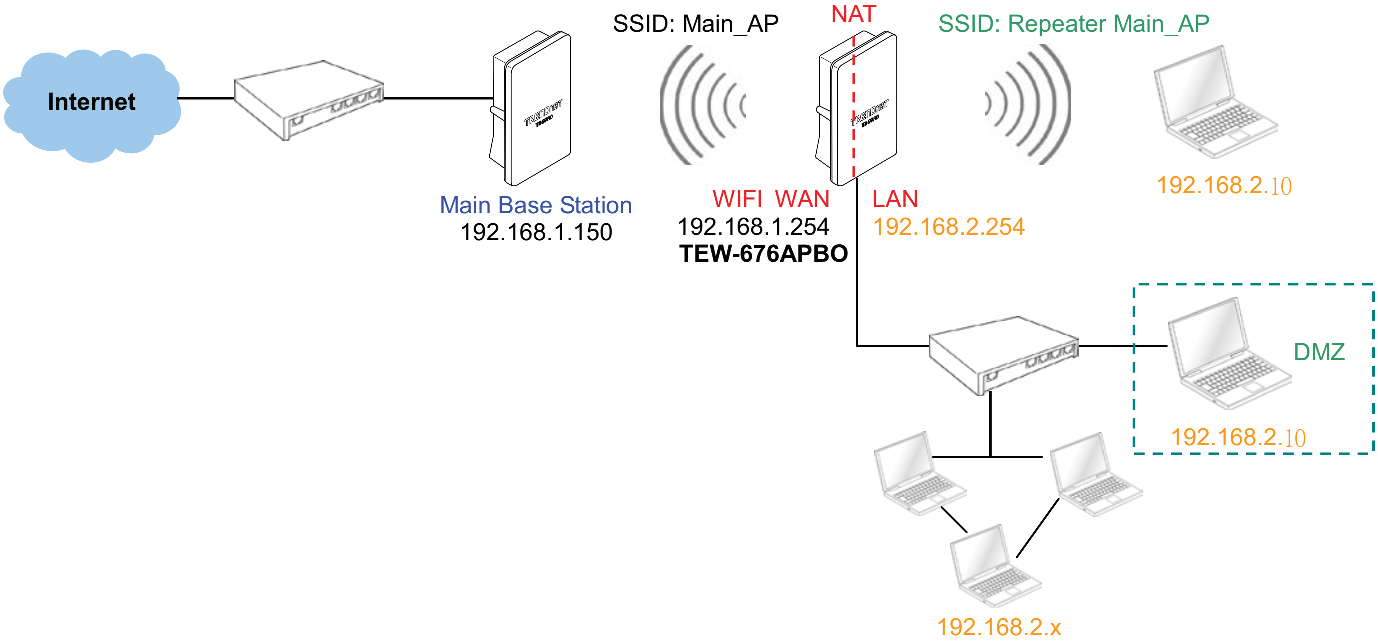
- ➢ **Example 2 :** On this setting, the FTP has **512** Kbps upload and **512** Kbps download on **192.168.2.10** Because rule 1's priority is higher than rule 2

Rule	Source IP	Destination IP	DSCP	Protocol	Remark DSCP	Bandwidth (Up/Down)
1			ANY	ANY	NO	512/512
2	192.168.2.10		ANY	FTP	NO	1024/8196

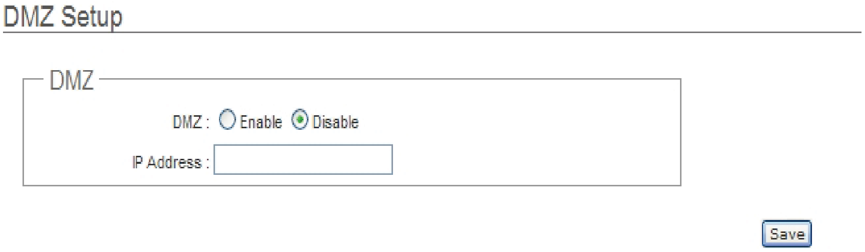
Resource Sharing

DMZ

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding*)* while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.



Please click on **Advance -> DMZ** and follow the below setting.



DMZ Setup

DMZ

DMZ : ○ Enable ● Disable

IP Address :

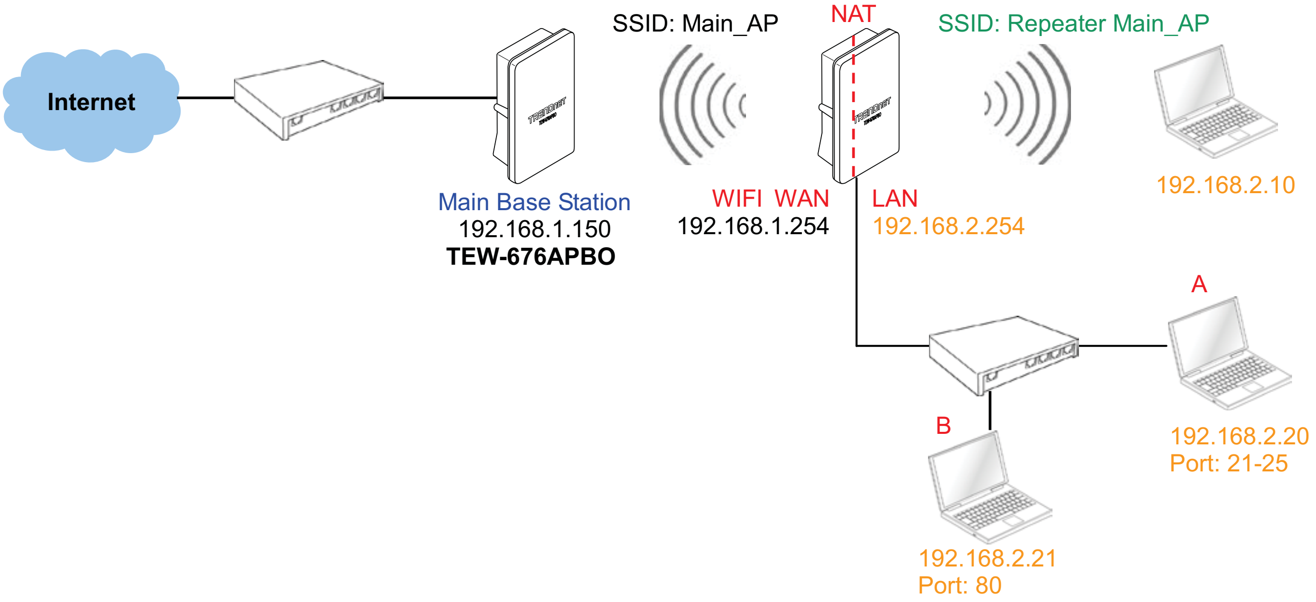
- **DMZ :** By default, it's *"**Disable**"*. Check ***Enable*** radial button to enable DMZ.
- **IP Address :** Enter IP address of DMZ host and only one DMZ host is supported.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

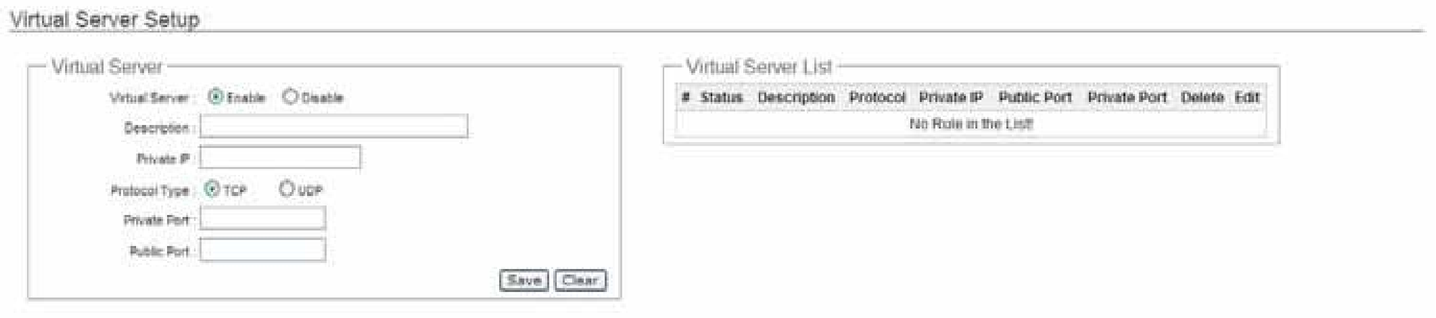
Virtual Server (Port Forwarding)

"Virtual Server" can also referred to as "Port Forward" as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don't repeat ports' usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.



Please click on **Advance -> Virtual Server** and follow the below setting.



Virtual Server Setup

Virtual Server

Virtual Server : ● Enable ○ Disable

Description :

Private IP :

Protocol Type : ● TCP ○ UDP

Private Port :

Public Port :

Virtual Server List

#	Status	Description	Protocol	Private IP	Public Port	Private Port	Delete	Edit
No Rule in the List!								

- **Virtual Server :** By Default, It's "***Disable***"**.** Check ***Enable*** radial button to enable Virtual Server.
- **Description :** Enter appropriate message for resource sharing via Virtual Server.
- **Private IP :** Enter corresponding IP address of internal resource to share.
- **Protocol Type :** Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.
- **Private Port :** A port or a range of ports may be specified as ***start:end***; i.e. port 20:80
- **Public Port :** A port or a range of ports may be specified as ***start:end***; i.e. port 20:80

.

The Private Port and Public Port can be different. However, total number of ports need to be the same.
Example : Public Port is 11 to 20 and the Private Port can be a 10 ports range.

Click “**Add**” button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List. Click ***Reboot*** button to activate your changes.

While creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ one while both rules exist. Example 1 and 2 demonstrate proper usage of DMZ and Virtual Server rules.

- **Example 1 :** All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all connections to TCP port 22 will be directed to TCP port 22 of 192.168.2.10 and remaining connections to port TCP ***20~80*** will be redirected to port TCP ***20~80*** of ***192.168.2.11***

DMZ Enabled : 192.168.2.12

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.10	22	22
2	TCP	192.168.2.11	20:80	20:80

- **Example 2 :** All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all other connections to TCP port ***20~80*** will be redirected to port ***20~80*** of ***192.168.2.11***. The rule 2 won’t take effect.

DMZ Enabled : 192.168.2.12

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.11	20:80	20:80
2	TCP	192.168.2.10	22	22

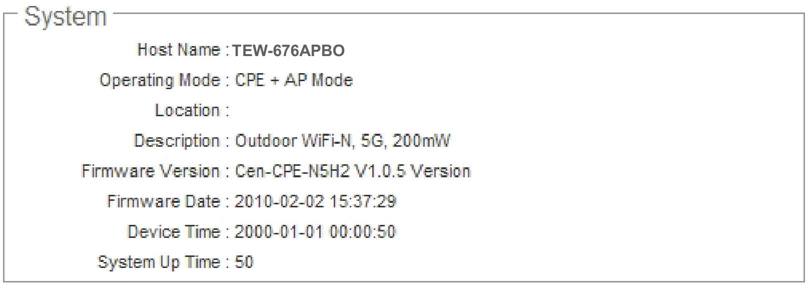
System Status

This section breaks down into subsections of ***System Overview***, ***Associated Clients Status, Remote AP***, ***Extra Information*** and ***Event Log***.

Overview

Detailed information on **System**, **WAN Information**, **LAN Information**, **Wireless Information** and **DHCP Server Status** can be reviewed via this page.

- **System :** Display the information of the system.

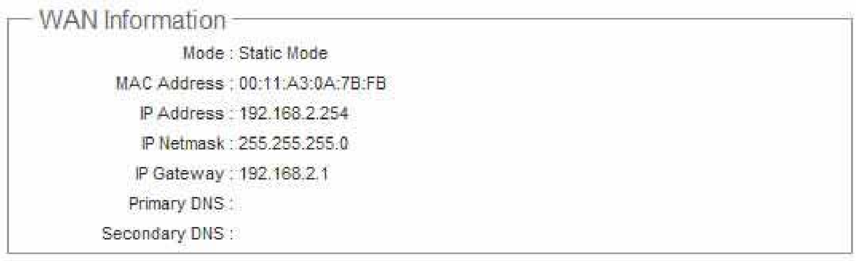


System

Host Name : TEW-676APBO
Operating Mode : CPE + AP Mode
Location :
Description : Outdoor WiFi-N, 5G, 200mW
Firmware Version : Cen-CPE-N5H2 V1.0.5 Version
Firmware Date : 2010-02-02 15:37:29
Device Time : 2000-01-01 00:00:50
System Up Time : 50

- ➔ **System Name :** The name of the system.
- ➔ **Operating Mode :** The mode currently in service.
- ➔ **Location :** The reminding note on the geographical location of the system.
- ➔ **Description :** The reminding note of the system.
- ➔ **Firmware Version :** The current firmware version installed.
- ➔ **Firmware Date :** The build time of the firmware installed.
- ➔ **Device Time :** The current time of the system.
- ➔ **System Up Time :** The time period that system has been in service since last reboot.

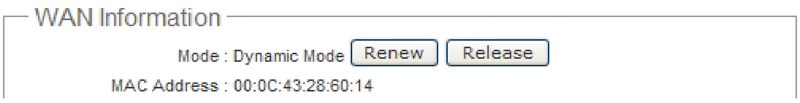
- **WAN Information :** Display the information of the WAN interface.



WAN Information

Mode : Static Mode
MAC Address : 00:11:A3:0A:7B:FB
IP Address : 192.168.2.254
IP Netmask : 255.255.255.0
IP Gateway : 192.168.2.1
Primary DNS :
Secondary DNS :

The WAN port specified **Dynamic IP**, the Release and Renew button will be show-up, click **Release** button to release IP address of WAN port, **Renew** button to renew IP address through DHCP server.

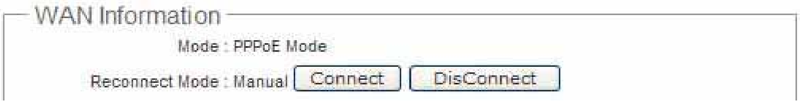


WAN Information

Mode : Dynamic Mode

MAC Address : 00:0C:43:28:60:14

The WAN port specified **PPPoE** or **PPTP**, and the **Connect** and **DisConnect** button will be show up. Click “**Connect**” button to assigned IP address from PPPoE or PPTP server, “**DisConnect**” button to release IP address of WAN port.



WAN Information

Mode : PPPoE Mode

Reconnect Mode : Manual

➔ **Mode :** Supports Static, Dynamic, PPPoE and PPTP modes.

➔ **Reconnect Mode :** The current reconnect mode of the PPPoE or PPTP.

➔ **MAC Address :** The MAC address of the WAN port.

➔ **IP Address :** The IP address of the WAN port.

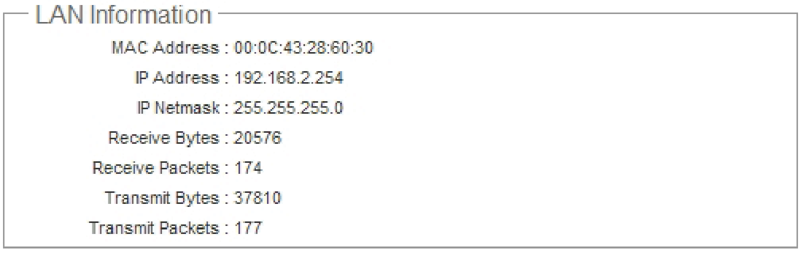
➔ **IP Netmask :** The IP netmask of the WAN port.

➔ **IP Gateway :** The gateway IP address of the WAN port.

➔ **Primary DNS :** The primary DNS server in service.

➔ **Secondary DNS :** The secondary DNS server in service.

■ **LAN Information :** Display total received and transmitted statistics on the LAN interface.



LAN Information

MAC Address : 00:0C:43:28:60:30

IP Address : 192.168.2.254

IP Netmask : 255.255.255.0

Receive Bytes : 20576

Receive Packets : 174

Transmit Bytes : 37810

Transmit Packets : 177

➔ **MAC Address :** The MAC address of the LAN port.

➔ **IP Address :** The IP address of the LAN port.

➔ **IP Netmask :** The IP netmask of the LAN port.

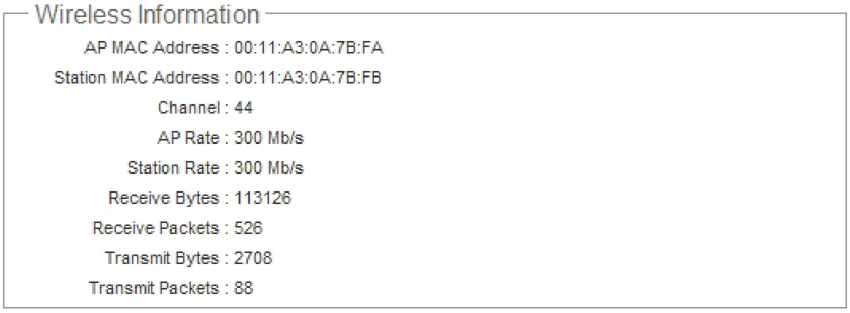
➔ **Receive bytes :** The total received packets in bytes on the LAN port.

➔ **Receive packets :** The total received packets of the LAN port.

➔ **Transmit bytes :** The total transmitted packets in bytes of the LAN port.

➔ **Transmit packets :** The total transmitted packets of the LAN port.

- **Wireless Information :** Display the detailed receive and transmit statistics of Wireless interface.



Wireless Information

AP MAC Address : 00:11:A3:0A:7B:FA
Station MAC Address : 00:11:A3:0A:7B:FB
Channel : 44
AP Rate : 300 Mb/s
Station Rate : 300 Mb/s
Receive Bytes : 113126
Receive Packets : 526
Transmit Bytes : 2708
Transmit Packets : 88

➔ **AP MAC Address :** The MAC address of the Repeater AP.

➔ **Station MAC Address :** The MAC address of the Wireless Client Station.

➔ **Channel :** The current channel on the Wireless port.

➔ **AP Rate :** The current Bit Rate on the Repeater AP.

➔ **Station Rate :** The current Bit Rate on the Wireless Client Station.

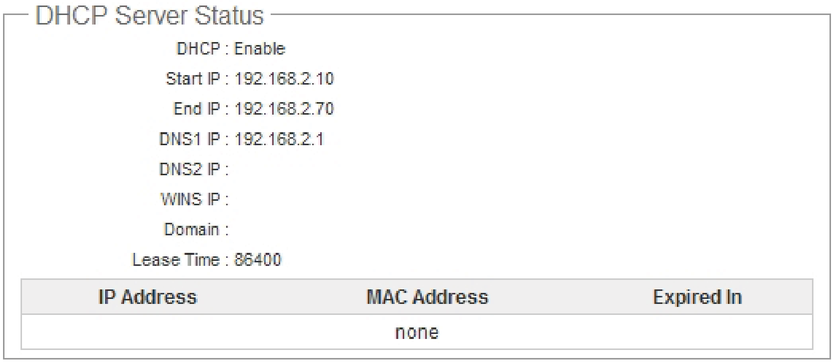
➔ **Receive bytes :**The total received packets in bytes on the Wireless port.

➔ **Receive packets :** The total received packets on the Wireless port.

➔ **Transmit bytes :** The total transmitted packets in bytes on the Wireless port.

➔ **Transmit packets :** The total transmitted packets on the Wireless port.

- **DHCP Server Status :** Users could retrieve DHCP server and DHCP clients' IP/MAC address via this field.



DHCP Server Status

DHCP : Enable
Start IP : 192.168.2.10
End IP : 192.168.2.70
DNS1 IP : 192.168.2.1
DNS2 IP :
WINS IP :
Domain :
Lease Time : 86400

IP Address	MAC Address	Expired In
	none	

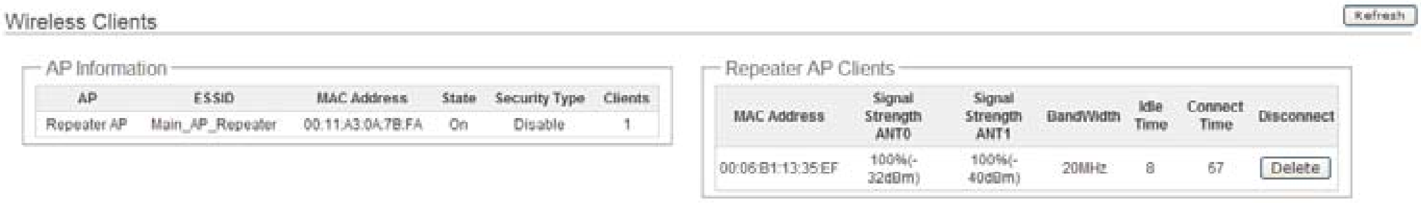
➔ **IP Address :** IP addresses to LAN devices by DHCP server.

➔ **MAC Address :** MAC addresses of LAN devices.

➔ **Expired In :** Shows how long the leased IP address will expire.

Associated Clients Status

It displays ESSID, on/off Status, Security Type, total number of wireless clients associated with Repeater AP.



AP Information

AP	ESSID	MAC Address	State	Security Type	Clients
Repeater AP	Main_AP_Repeater	00:11:A3:0A:7B:FA	On	Disable	1

Repeater AP Clients

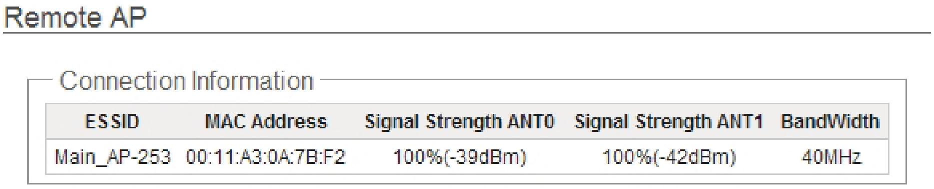
MAC Address	Signal Strength ANT0	Signal Strength ANT1	BandWidth	Idle Time	Connect Time	Disconnect
00:06:B1:13:35:EF	100%(-32dBm)	100%(-40dBm)	20MHz	8	67	Delete

- **AP Information :** Highlights key Repeater AP information.
  - ➔ **AP :** Available Repeater AP.
  - ➔ **ESSID :** Display name of ESSID for Repeater AP.
  - ➔ **MAC Address :** Display MAC address for Repeater AP.
  - ➔ **Status :** On/Off
  - ➔ **Security Type :** Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
  - ➔ **Clients :** Display total number of wireless connections on Repeater AP.

- **Repeater AP Clients :** Display all associated clients.
  - ➔ **MAC Address :** MAC address of associated clients
  - ➔ **Signal Strength ANT0/ANT1 :** Signal Strength of from associated clients.
  - ➔ **Bandwidth :** Channel bandwidth of from associated clients
  - ➔ **Idle Time :** Last inactive time period in seconds for a wireless connection.
  - ➔ **Connect Time :** Total connection time period in seconds for a wireless connection.
  - ➔ **Disconnect :** Click “**Delete**” button to manually disconnect a wireless client in a Repeater AP.

Remote AP

SSID, MAC address,   antenna 0/1 received signal strength and channel bandwidth for associated AP are available.



Remote AP

Connection Information

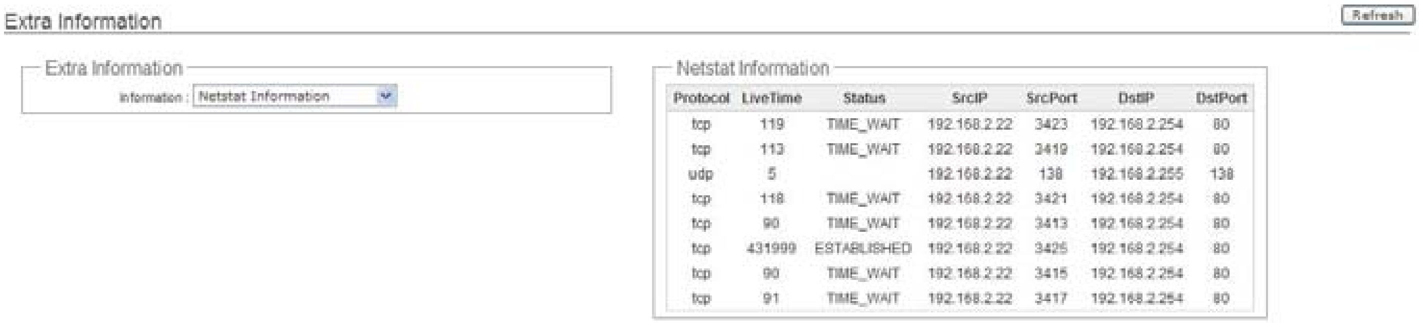
ESSID	MAC Address	Signal Strength ANT0	Signal Strength ANT1	BandWidth
Main_AP-253	00:11:A3:0A:7B:F2	100%(-39dBm)	100%(-42dBm)	40MHz

- **ESSID :** Shows the current ESSID, which must be the same on the wireless client and AP in order for communication to be established.
- **MAC Address :** Display MAC address of associated AP.
- **Signal Strength ANT0/ANT1 :** Shows the wireless signal strength of the connection between system and an access point.
- **BandWidth :** Shows the current channel bandwidth used for communication. It should be “20” or “40”

*If display “**No Connection AP!**” , you need check Wireless configuration. Things to verify are **Channel** and **Security type.** Also, adjust antenna angle and Tx Power.*

Extra Info

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.



Extra Information

Information : Netstat Information

Netstat Information

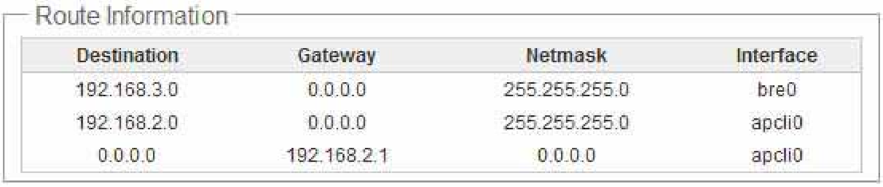
Protocol	LiveTime	Status	SrcIP	SrcPort	DstIP	DstPort
tcp	119	TIME_WAIT	192.168.2.22	3423	192.168.2.254	80
tcp	113	TIME_WAIT	192.168.2.22	3419	192.168.2.254	80
udp	5		192.168.2.22	138	192.168.2.255	138
tcp	118	TIME_WAIT	192.168.2.22	3421	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3413	192.168.2.254	80
tcp	431999	ESTABLISHED	192.168.2.22	3425	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3415	192.168.2.254	80
tcp	91	TIME_WAIT	192.168.2.22	3417	192.168.2.254	80

- **Netstat Information :** Select “**NetStatus Information**” on the drop-down list, the connection track list should show-up, the list can be updated using the Refresh button.

  NetStatus will show all connection track on the system, the information include *Protocol*, *Live Time*, *Status* , *Source/Destination IP address* and *Port*.

- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

  TEW-676APBO could be used as a L2 or L3 device. It doesn’t support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it’s capable of being a gateway to route packets inward and outward.

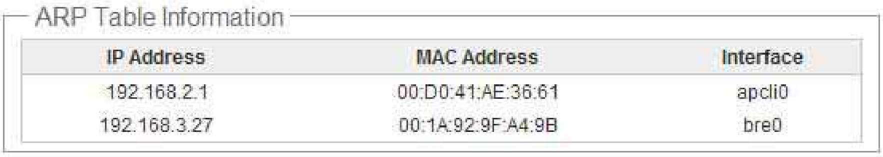


Route Information

Destination	Gateway	Netmask	Interface
192.168.3.0	0.0.0.0	255.255.255.0	bre0
192.168.2.0	0.0.0.0	255.255.255.0	apcli0
0.0.0.0	192.168.2.1	0.0.0.0	apcli0

- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

  ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

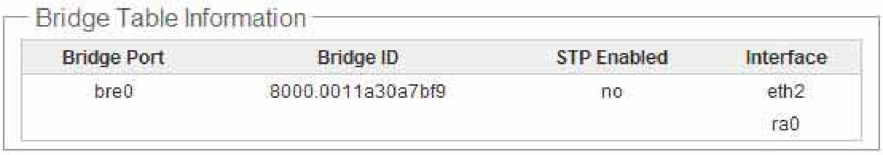


ARP Table Information

IP Address	MAC Address	Interface
192.168.2.1	00:D0:41:AE:36:61	apcli0
192.168.3.27	00:1A:92:9F:A4:9B	bre0

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

  Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces.



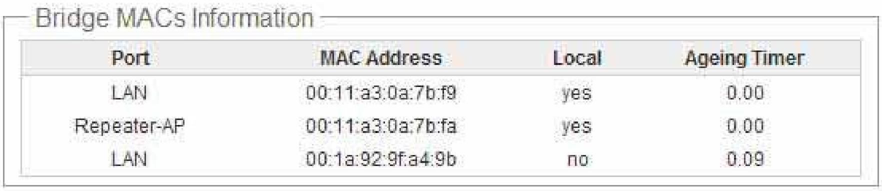
Bridge Table Information

Bridge Port	Bridge ID	STP Enabled	Interface
bre0	8000.0011a30a7bf9	no	eth2 ra0

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

  This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

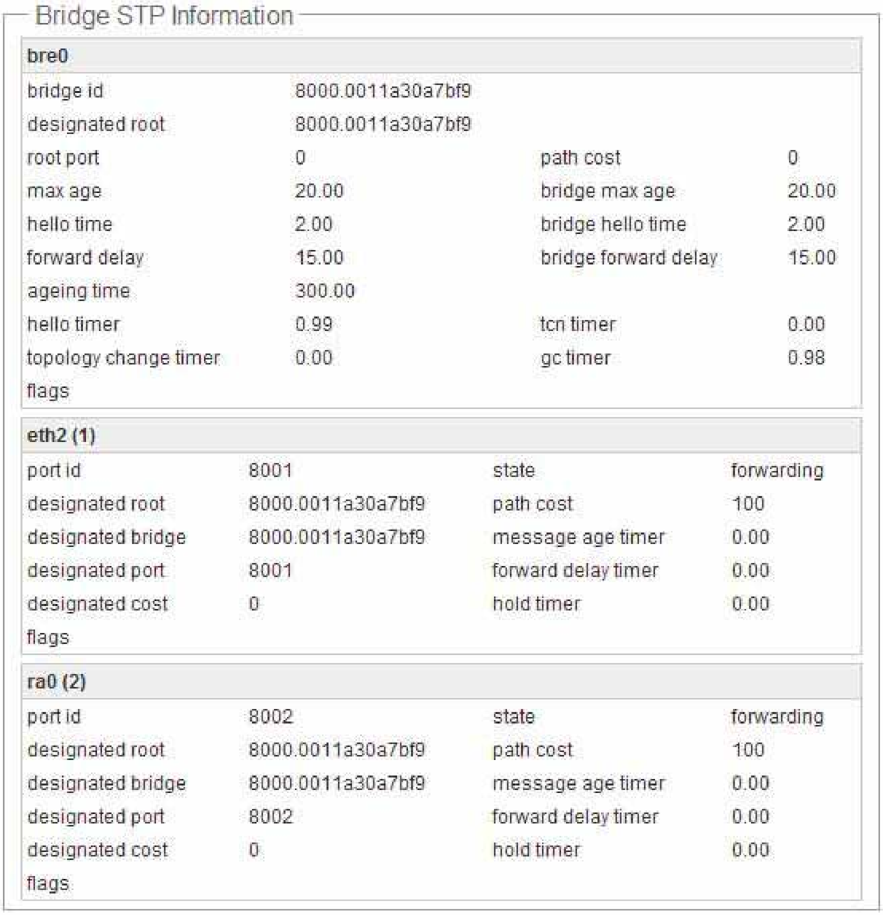
  Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.



Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
LAN	00:11:a3:0a:7b:f9	yes	0.00
Repeater-AP	00:11:a3:0a:7b:fa	yes	0.00
LAN	00:1a:92:9f:a4:9b	no	0.09

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.



Bridge STP Information

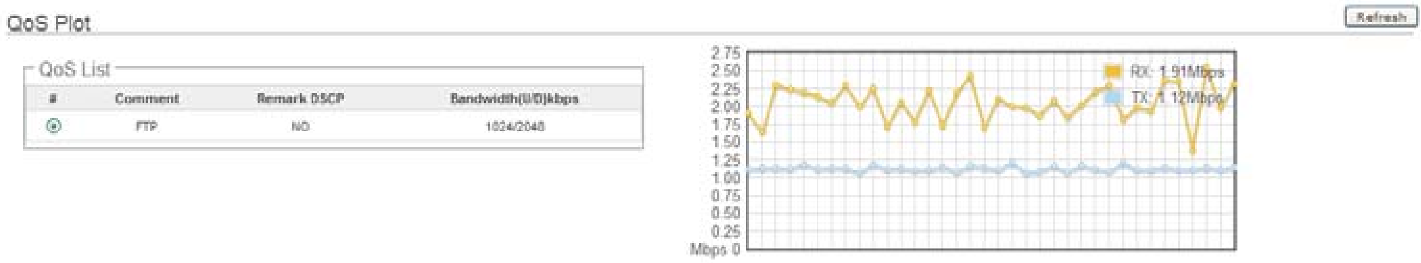
bre0			
bridge id	8000.0011a30a7bf9		
designated root	8000.0011a30a7bf9		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00		
hello timer	0.99	tcn timer	0.00
topology change timer	0.00	gc timer	0.98
flags			

eth2 (1)			
port id	8001	state	forwarding
designated root	8000.0011a30a7bf9	path cost	100
designated bridge	8000.0011a30a7bf9	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

ra0 (2)			
port id	8002	state	forwarding
designated root	8000.0011a30a7bf9	path cost	100
designated bridge	8000.0011a30a7bf9	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

QoS Plot

The QoS Plot show graphs which continuously represents the current data traffic on each QoS rule. The chart scale and throughput dimension (bps, Kbps, Mbps) changes dynamically according to the mean throughput value. The statistics is updated automatically every **5** seconds. The throughput statistics of QoS can be updated manually using the ***Refresh*** button.

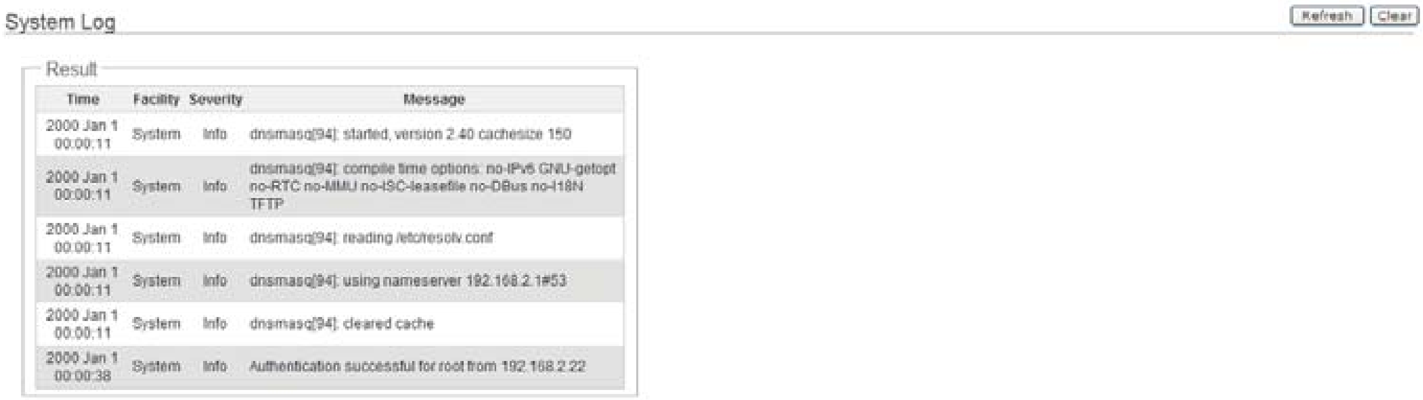


QoS List

#	Comment	Remark DSCP	Bandwidth(U/D)kbps
◉	FTP	NO	1024/2048

Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.



Time	Facility	Severity	Message
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: started, version 2.40 cachesize 150
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-I18N TFTP
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: reading /etc/resolv.conf
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: using nameserver 192.168.2.1#53
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: cleared cache
2000 Jan 1 00:00:38	System	Info	Authentication successful for root from 192.168.2.22

- **Time :** The date and time when the event occurred.
- **Facility :** It helps users to identify source of events such “System” or “User”
- **Severity :** Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message :** Description of the event.

Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

Client Bridge + Universal Repeater Configuration

When Client Bridge+Universal Repeater mode is activated, the system can be configured as an **Access Point** and **Client Station** simultaneously. This section provides information in configuring the Client Bridge+Universal Repeater mode with graphical illustrations. TEW-676APBO provides functions as stated below where they can be configured via a user-friendly web based interface.

Option	System	Wireless	Utilities	Status
Functions	Operating Mode	General Setup	Profiles Settings	System Overview
	LAN	Advanced Setup	Firmware Upgrade	Clients
	Management	Repeater AP Setup	Network Utility	Remote AP
	Time Server	Wireless Profile	Reboot	Extra Info
	SNMP	Site Survey		Event Log

Table 7-1: Client Bridge+Universal Repeater Mode Functions

External Network Connection

Network Requirement

It can be used as an Client Bridge or Universal Repeater to receive and repeat wireless signal over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers. In this mode, TEW-676APBO is enabled with DHCP Server functions. The wired clients of WCB1200H2PX are in **the same** subnet from Main Base Station and it **accepts** wireless connections from wireless client devices.

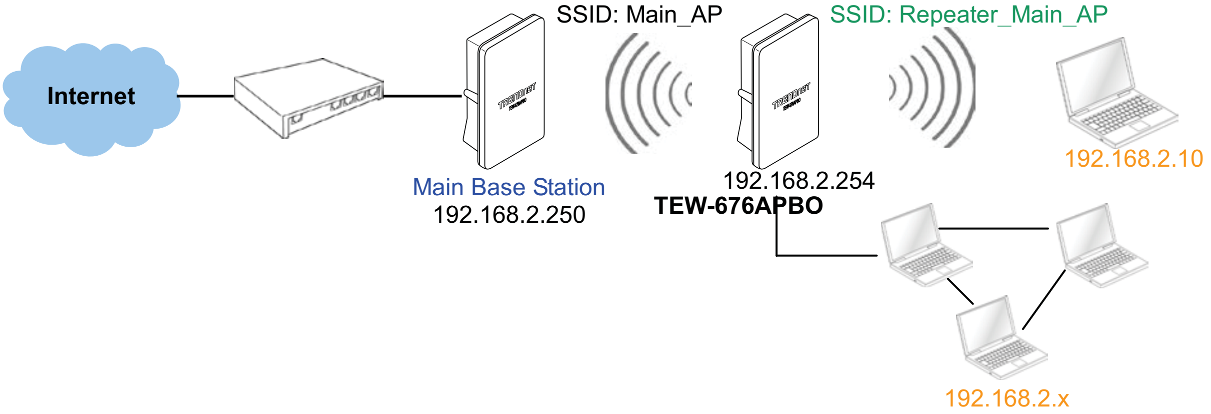


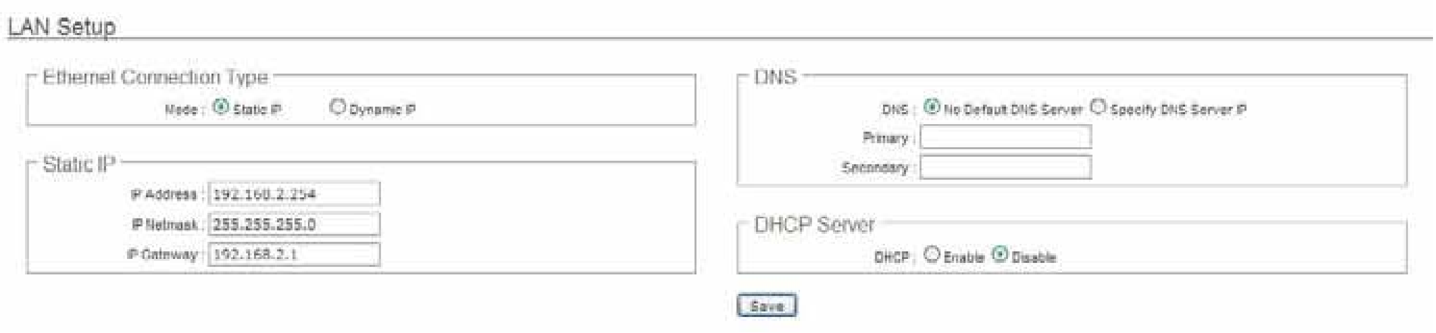
Figure 7-1 Client Bridge + Universal Repeater mode network Configuration

When the TEW-676APBO *configured as an Access Point and Client Station simultaneously, the Wireless General and Advanced Setup also used simultaneously. But the Security Type can be different. In the other word, the channel or other settings will be the same between* TEW-676APBO *to Main Base Station and wireless client to* TEW-676APBO*, but security type can be different.*

Configure LAN IP

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.



LAN Setup

Ethernet Connection Type

Mode : ● Static IP ○ Dynamic IP

Static IP

IP Address : 192.160.2.254

IP Netmask : 255.255.255.0

IP Gateway : 192.168.2.1

DNS

DNS : ● No Default DNS Server ○ Specify DNS Server IP

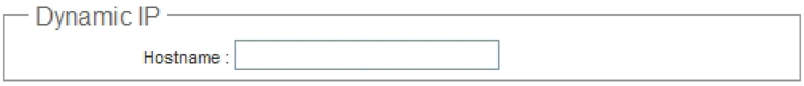
Primary :

Secondary :

DHCP Server

DHCP : ○ Enable ● Disable

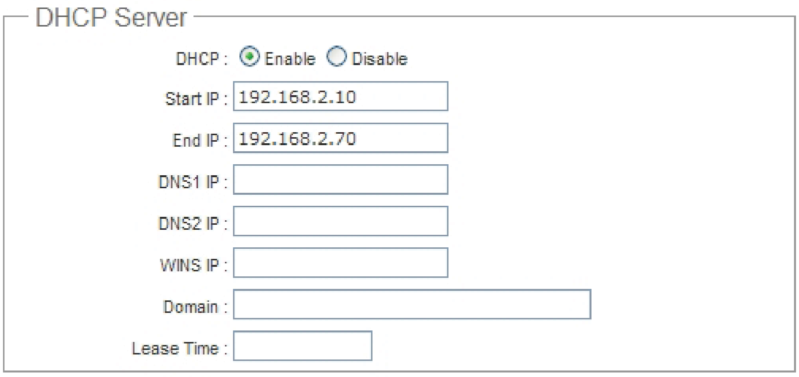
- **Mode :** Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
  - ➔ **Static IP :** The administrator can manually setup the LAN IP address when static IP is available/ preferred.
    - ✓ **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
    - ✓ **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0
    - ✓ **IP Gateway :** The default gateway of the LAN port; default Gateway is 192.168.2.1
  - ➔ **Dynamic IP :** This configuration type is applicable when the WCB1200H2PX is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.



Dynamic IP

Hostname :

- **Hostname :** The Hostname of the LAN port
- **DNS :** Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.
  - ➔ **Primary :** The IP address of the primary DNS server.
  - ➔ **Secondary :** The IP address of the secondary DNS server.
- **DHCP Setup :** Devices connected to the system can obtain an IP address automatically when this service is enabled.



DHCP Server

DHCP : ● Enable ○ Disable

Start IP : 192.168.2.10

End IP : 192.168.2.70

DNS1 IP :

DNS2 IP :

WINS IP :

Domain :

Lease Time :

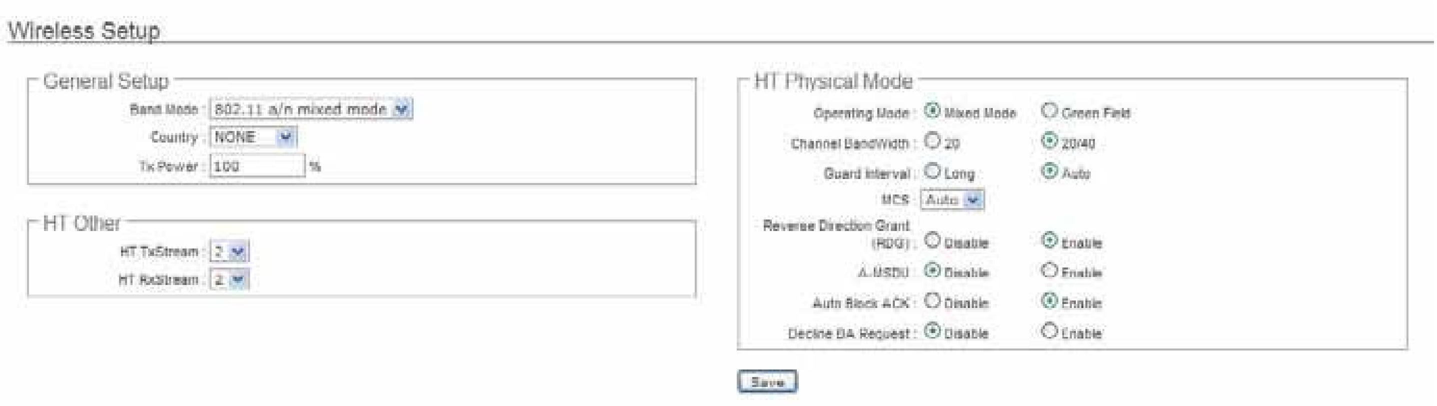
- **DHCP :** Check ***Enable*** button to activate this function or ***Disable*** to deactivate this service.
- **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- **DNS1 IP :** Enter IP address of the first DNS server; this field is required.
- **DNS2 IP :** Enter IP address of the second DNS server; this is optional.
- **WINS IP :** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- **Domain :** Enter the domain name for this network.
- **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 interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Access Point Association

Configure Wireless General Setting

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.



Wireless Setup

General Setup

Band Mode : 802.11 a/n mixed mode

Country : NONE

Tx Power : 100 %

HT Other

HT TxStream : 2

HT RxStream : 2

HT Physical Mode

Operating Mode : ● Mixed Mode ○ Green Field

Channel BandWidth : ○ 20 ● 20/40

Guard Interval : ○ Long ● Auto

MCS : Auto

Reverse Direction Grant (RDG) : ○ Disable ● Enable

A-MSDU : ● Disable ○ Enable

Auto Block ACK : ○ Disable ● Enable

Decline BA Request : ● Disable ○ Enable

- **Band Mode :** Select an appropriate wireless band; bands available are **801.11a** or ***802.11a/n mixed*** mode.
- **Transmit Rate Control :** Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54** Mbps for **802.11a**
- **Country :** Select the desired country code from the drop-down list; the options are ***US***, ***ETSI***, ***JP*** and ***NONE***.
- **Tx Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit number between ***1*** to ***100*** (the unit is %) for your environment. If you are not sure of which setting to choose, then keep the default setting, **100**%.

When **Band Mode** select in **802.11a only mode**, the **HT(High Throughput) Physical Mode and 11n Configuration** settings should be hidden immediately.

- **Operating Mode :** By default, it's Mixed Mode
  - ➔ **Mixed Mode :** In this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
  - ➔ **Green Field :** In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth :** The "**Auto**" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval :** Using "**Auto**" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

- **MCS :** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to ***Appendix C. MCS Data Rate***)
- **MPDU Enable :** Check ***Enable*** button to activate this function, and ***Disable*** to deactivate.
- **A-MPDU :** A-MPDU (Aggregated Mac Protocol Data Unit) allows the transmissions of multiple Ethernet frames to a single location as burst of up to 64kbytes This is performed on the hardware itself. Select “Manual” to set “MPDU Density”
- **MPDU Density :** Minimum separation of MPDUs in an A-MPDU.

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
No Restriction	¼ μs	½ μs	1 μs	2 μs	4 μs	8 μs	16 μs

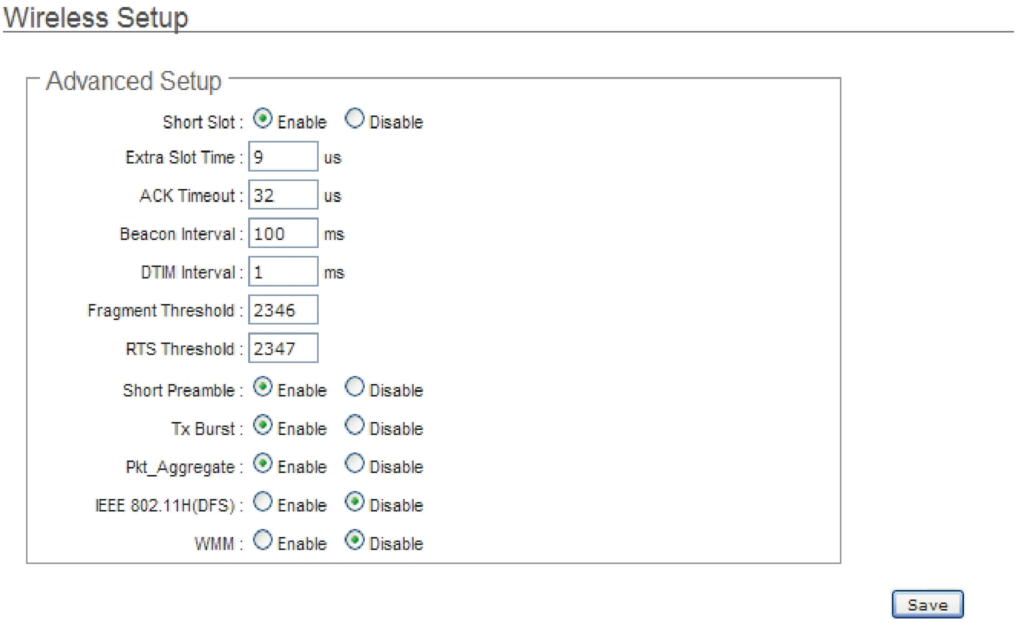
- **A-MSDU :** Aggregated Mac Service Data Unit, A-MSDU. Select **Enable** to allow aggregation for multiple MSDUs in one MPDU. Default is disabled.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to **Repeater AP**

Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



Wireless Setup

Advanced Setup

Short Slot : ● Enable ○ Disable
Extra Slot Time : 9 us
ACK Timeout : 32 us
Beacon Interval : 100 ms
DTIM Interval : 1 ms
Fragment Threshold : 2346
RTS Threshold : 2347
Short Preamble : ● Enable ○ Disable
Tx Burst : ● Enable ○ Disable
Pkt_Aggregate : ● Enable ○ Disable
IEEE 802.11H(DFS) : ○ Enable ● Disable
WMM : ○ Enable ● Disable

- **Short Slot :** By default, it's "***Enable***" for educing the slot time from the standard **20** *microseconds* to the **9** *microsecond* short slot time

  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **Extra Slot Time :** Slot time is in the range of **1~255** and set in unit of ***microsecond***. The default value is **9** microsecond.

When you enable Short Slot and set Extra Slot time to "10", the actual Slot Time=9+10 us.
When you disable Short Slot and set Extra Slot time to "10", the actual Slot Time=20+10 us.

- **ACK Timeout :** ACK timeout is in the range of **1~255** and set in unit of ***microsecond***. The default value is **32** microsecond.

  All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughputs become low due to excessively high re-transmission.

  ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval :** Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1~255**. The default is **1**.

  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256~2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

  With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

- **Pkt_Aggregate :** By default, it's "***Enable***"

  Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.

- **IEEE802.11H (DFS) :** By default, it's "***Disable***". To ***Enable*** is to use IEEE802.11H(DFS)

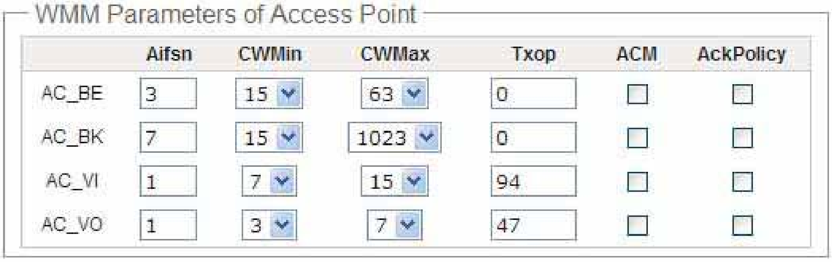
  With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

DFS Channels	52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

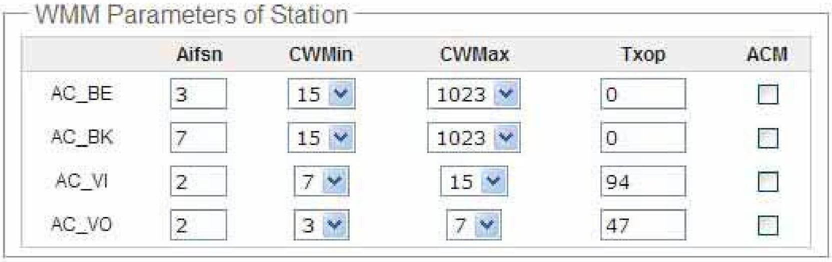
*The Channel **52-140** is DFS channel. If tuen on IEEE802.11H, AP Will have **60** sec to do channel available check, and will not send beacon and cannot be connected. When WCB1200H2PX detect radar(5GHz) signal, the AP will switch channel and stop beacon trasmit between **15** sec.*

- **WMM :** By default, it's "***Disable***". To ***Enable*** is to use WMM and the WMM parameters should appears.



WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐



WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

➔ **WMM Parameters of Access Point :** *This affects traffic flowing from the access point to the client station*

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM :** Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy :** Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"

  When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

  When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ ***WMM Parameters of Station :*** *This affects traffic flowing from the client station to the access point.*

Queue	Data Transmitted Clients to AP	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.

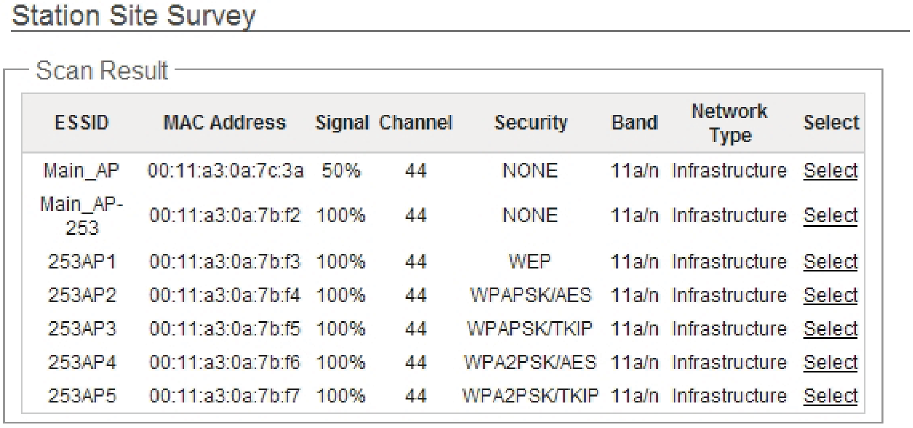
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM :** Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **Repeater AP**.

Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with.

Please click on **Wireless -> Site Survey**. Below depicts an example for site survey.



Station Site Survey

Scan Result

ESSID	MAC Address	Signal	Channel	Security	Band	Network Type	Select
Main_AP	00:11:a3:0a:7c:3a	50%	44	NONE	11a/n	Infrastructure	Select
Main_AP-253	00:11:a3:0a:7b:f2	100%	44	NONE	11a/n	Infrastructure	Select
253AP1	00:11:a3:0a:7b:f3	100%	44	WEP	11a/n	Infrastructure	Select
253AP2	00:11:a3:0a:7b:f4	100%	44	WPAPSK/AES	11a/n	Infrastructure	Select
253AP3	00:11:a3:0a:7b:f5	100%	44	WPAPSK/TKIP	11a/n	Infrastructure	Select
253AP4	00:11:a3:0a:7b:f6	100%	44	WPA2PSK/AES	11a/n	Infrastructure	Select
253AP5	00:11:a3:0a:7b:f7	100%	44	WPA2PSK/TKIP	11a/n	Infrastructure	Select

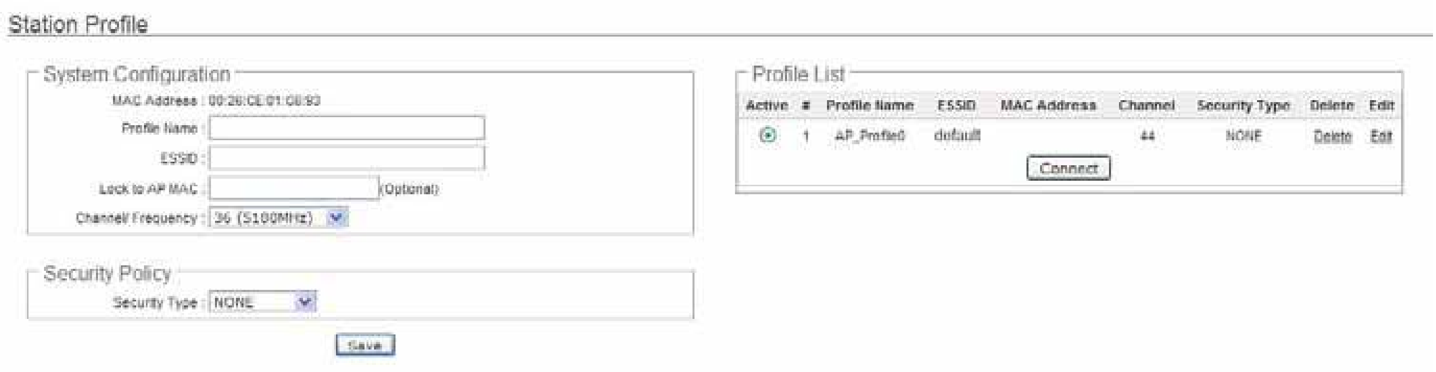
- **ESSID : Available** Extend Service Set ID of surrounding Access Points.
- **MAC Address :** MAC addresses of surrounding Access Points.
- **Signal :** Received signal strength of all found Access Points.
- **Channel :** Channel numbers used by all found Access Points.
- **Security :** Security type by all found Access Points.
- **Band :** Wireless band used by all found Access Points.
- **Network Type :** Network type used by all found Access Points.
- **Select :** Click “**Select**” to configure settings and associate with chosen AP.

*While clicking “Select” button in the Site Survey Table, the “**ESSID**” and “**Security Type**” will apply in the **Wireless Profile** Setup. However, more settings are needed including Security Key.*

Create Wireless Profile

The administrator can configure station profiles via this page.

Please click on **Wireless -> Wireless Profile** and follow the below setting.



Station Profile

System Configuration

MAC Address : 00:26:CE:01:08:93

Profile Name :

ESSID :

Lock to AP MAC : (Optional)

Channel/ Frequency : 36 (5180MHz)

Security Policy

Security Type : NONE

Profile List

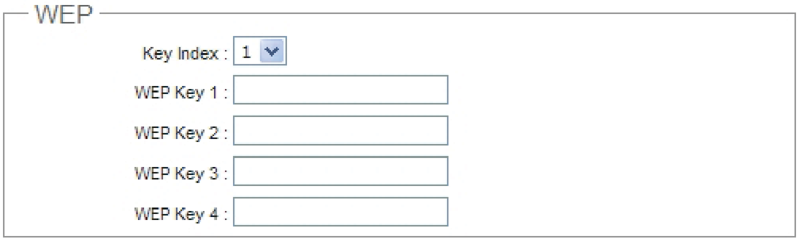
Active	#	Profile Name	ESSID	MAC Address	Channel	Security Type	Delete	Edit
◉	1	AP_Profile0	default		44	NONE	Delete	Edit

- **MAC Address :** The MAC address of the Wireless Station is displayed here.
- **Profile Name :** Set different profiles for quick connection uses.
- **ESSID :** Assign Service Set ID for the wireless system.
- **Lock to AP MAC :** This allows the station to always maintain connection to a particular AP with a specific MAC address. This is useful as sometimes there can be few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to MAC address and not roam between several Access Points with the same ESSID.
- **Channel/Frequency :** Select the desired channel range.

If tuen on IEEE802.11H and TEW-676APBO *connect AP with DFS channel* ***52-140***, TEW-676APBO *Will have* ***60*** *sec to do channel available check, and will not send beacon and can not be connect.*

- **Security Type :** Select the desired security type from the drop-down list; the options are "**NONE**" "**OPEN**", "**SHARED**", "**WPA-PSK**" and "**WPA2-PSK**".

  ➔ **OPEN / SHARED :** OPEN and SHARED require the user to set a WEP key to exchange data.



WEP

Key Index : 1

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

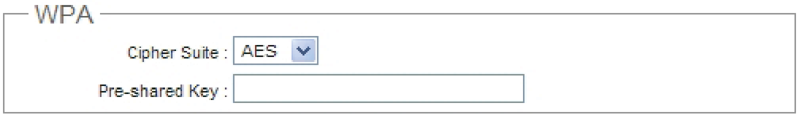
WEP Key 4 :

✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.

✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

➔ **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.



WPA

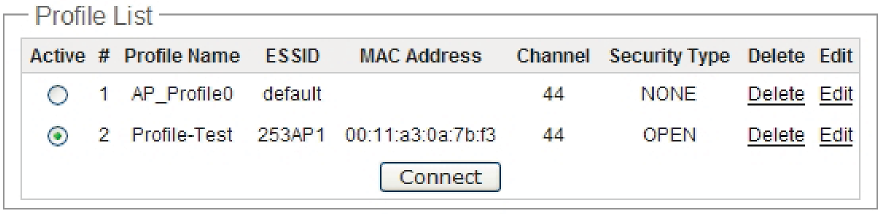
Cipher Suite : AES

Pre-shared Key :

✓ **Cipher Suite :** Select the desired cipher suite from the drop-down list; the options are **AES** and **TKIP**

✓ **Pre-shared Key :** Enter the information for pre-shared key; the key can be either entered as a 256-bit secret in **64 HEX** digits format, or **8 to 63 ASCII** characters.

■ **Profile List :** The user can manage the created profiles for home, work or public areas. Below depict an example for Profile List



Profile List

Active	#	Profile Name	ESSID	MAC Address	Channel	Security Type	Delete	Edit
○	1	AP_Profile0	default		44	NONE	Delete	Edit
●	2	Profile-Test	253AP1	00:11:a3:0a:7b:f3	44	OPEN	Delete	Edit

➔ Click “”**Edit**” an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click “**Save**” button to save the profile.

➔ Click “**Delete**” to remove profile.

➔ Click and Select a profile from list, then click the “**Connect**” button to connecting to the wireless network with the profile setting. After clicking “**Connect**” button, the system should be jump to **Remote AP Page**, you can verify connecting status on **Remote AP Page**.

*When you click “**Save**” button on this page, the system will connect to specify AP and jump to **Remote AP Page***

If tuen on IEEE802.11H and TEW-676APBO *connect AP with DFS channel **52-140**,* TEW-676APBO *Will have **60** sec to do channel available check, and will not send beacon and can not be connect.*

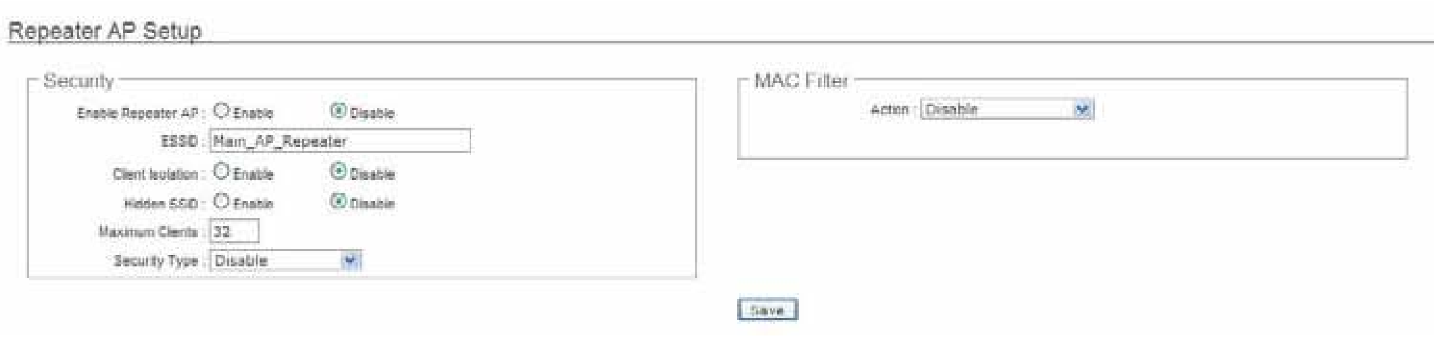
Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Wireless LAN Network Creation

The network manager can configure related wireless settings, **Repeater AP Setup, Security Settings,** and **MAC Filter Settings**.

Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and MAC Filter settings.



Repeater AP Setup

Security

Enable Repeater AP : ○ Enable ● Disable

ESSID : Main_AP_Repeater

Client Isolation : ○ Enable ● Disable

Hidden SSID : ○ Enable ● Disable

Maximum Clients : 32

Security Type : Disable

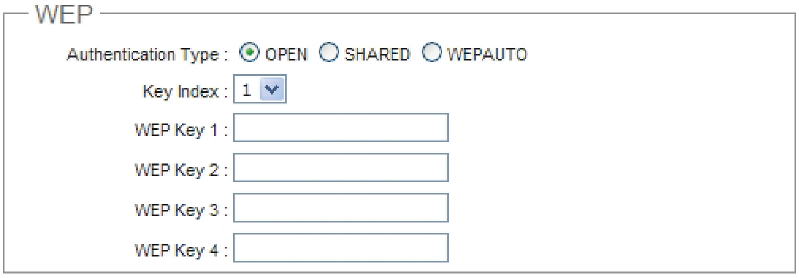
MAC Filter

Action : Disable

- **Enable Repeater AP :** By default, it's "**En*able***" for repeater AP. Select "***Enable***" to activate Repeater AP or click "***Disable***" to deactivate this function
- **ESSID :** Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP's clients associated with the specified AP.
- **Client Isolation :** By default, it's "***Disable***".

  Select "**Enable"**, all clients will be isolated from each other, which means they can't reach each other.
- **Hidden SSID :** By default, it's "***Disable***".

  Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP's clients could make to associate to it.
- **Maximum Clients :** The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this Repeater AP.
- **Security Type :** Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
  - ➔ **Disable :** Data are unencrypted during transmission when this option is selected.
  - ➔ **WEP :** Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.



WEP

Authentication Type : ● OPEN ○ SHARED ○ WEPAUTO

Key Index : 1

WEP Key 1 :

WEP Key 2 :

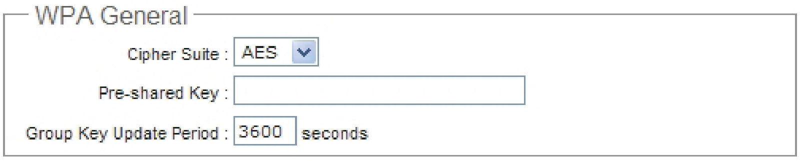
WEP Key 3 :

WEP Key 4 :

- ✓ **Authentication Method :** Enable the desire option among ***OPEN***, ***SHARED*** or ***WEPAUTO***.
- ✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	**Hex**	**ASCII**
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

➔ **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.



WPA General

Cipher Suite : AES

Pre-shared Key :

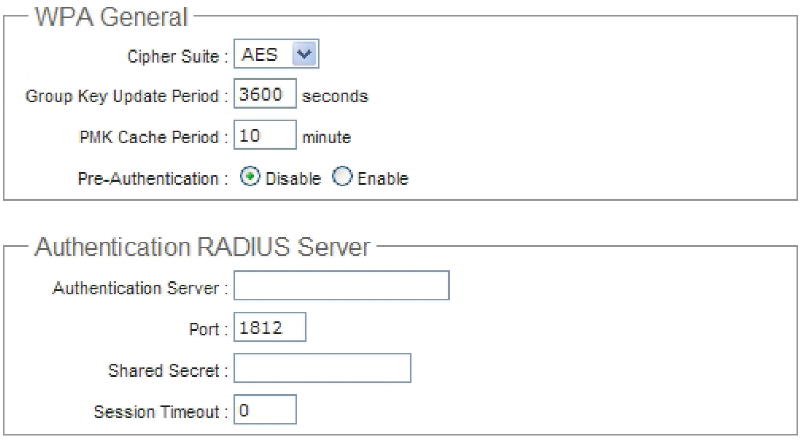
Group Key Update Period : 3600 seconds

- ✓ **Cipher Suite :** By default, it is **AES**. Select either AES or TKIP cipher suites
- ✓ **Pre-shared Key :** Enter the pre-shared key; the format shall go with the selected key type.

Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

- ✓ **Group Key Update Period :** By default, it is **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

➔ **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this is selected.



WPA General

Cipher Suite : AES

Group Key Update Period : 3600 seconds

PMK Cache Period : 10 minute

Pre-Authentication : ● Disable ○ Enable

Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

Session Timeout : 0

✓ **WPA General Settings :**

- **Cipher Suite :** By default, it is AES. Select either AES or TKIP cipher suites
- **Group Key Update Period :** By default, it’s **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- **PMK Cache Period :** By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- **Pre-Authentication :** By default, it's “Disable”. To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.

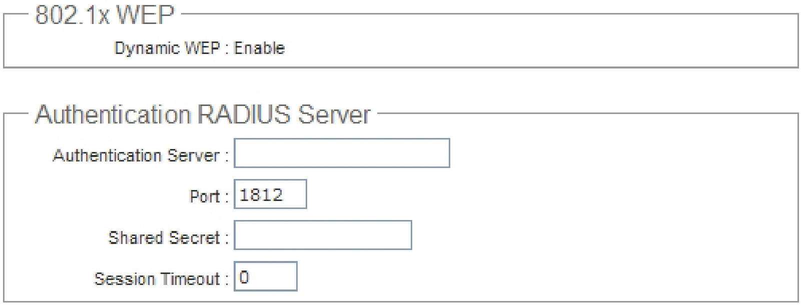
PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise

✓ **Radius Server Settings :**

- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it’s **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60** *seconds*. The default is **0** to disable re-authenticate service.

  Amount of time before a client will be required to re-authenticate.

➔ **WEP 802.1X :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.



802.1x WEP

Dynamic WEP : Enable

Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

Session Timeout : 0

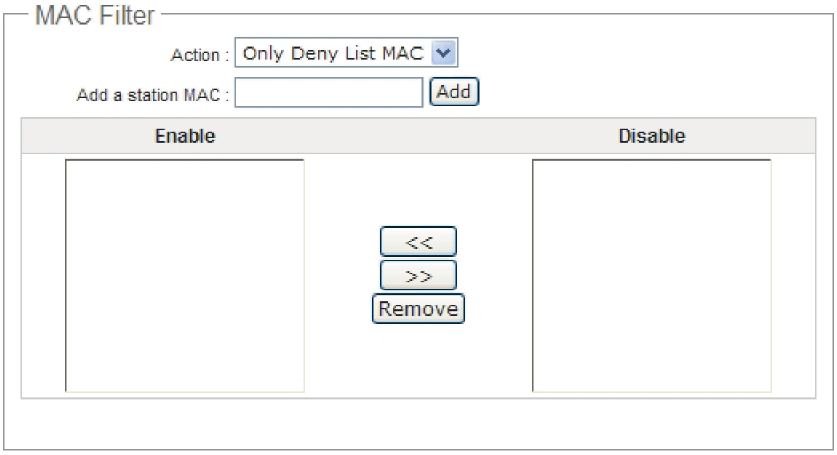
✓ **Radius Server Settings :**

- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60** *seconds*. The default is **0** to disable re-authenticate service.

  Amount of time before a client will be required to re-authenticate.

Wireless MAC Filter Setup

Continue **7.3.1 Repeater AP Setup** section, the administrator can allow or reject clients to access Repeater AP.



- **MAC Filter Setup :** By default, it's "***Disable***". Options are **Disable, Only Deny List MAC or Only Allow List MAC**.

  Two ways to set MAC filter rules :

  ➔ **Only Allow List MAC**.

  The wireless clients in the "**Enable**" list will be **allowed** to access the Access Point; All others or clients in the "**Disable**" list will be **denied**.

  ➔ **Only Deny List MAC**.

  The wireless clients in the "**Enable**" list will be **denied** to access the Access Point; All others or clients in the "**Disable**" list will be **allowed**.

- **Add a station MAC :** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the "**Enable**" List.

There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons**.**

Click ***Reboot*** button to activate your changes

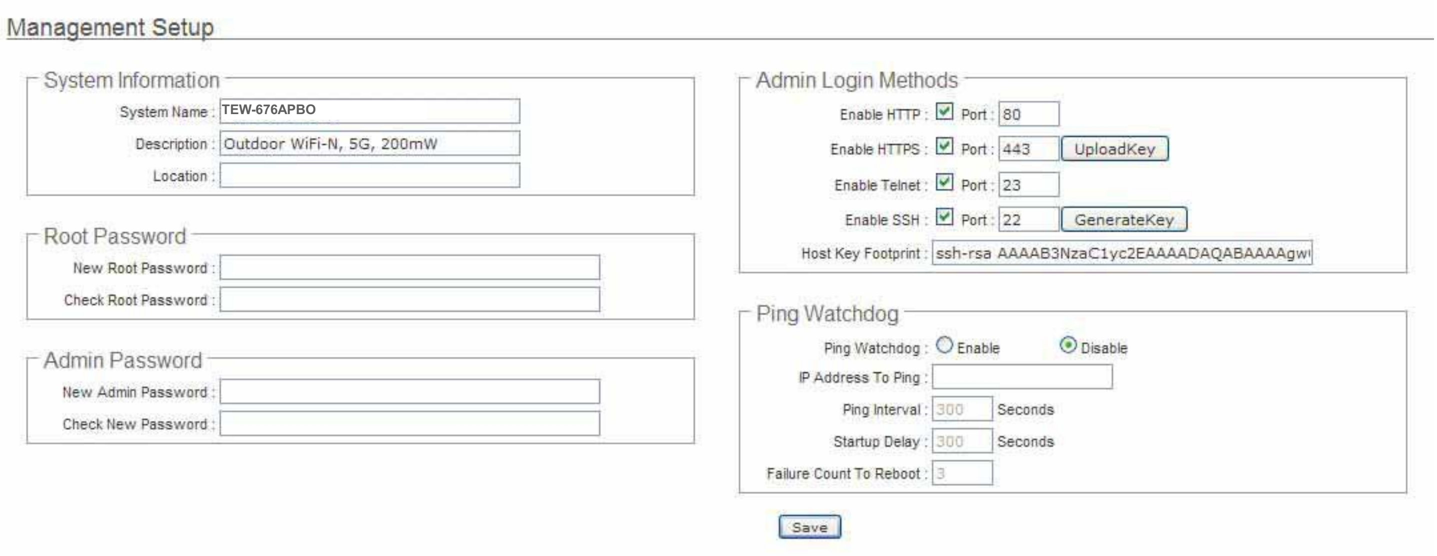
MAC Access Control is the weakest security approach.WPA or WPA2 security method is highly recommended.

System Management

Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.



Management Setup

System Information

System Name : TEW-676APBO

Description : Outdoor WiFi-N, 5G, 200mW

Location :

Root Password

New Root Password :

Check Root Password :

Admin Password

New Admin Password :

Check New Password :

Admin Login Methods

Enable HTTP : ☑ Port : 80

Enable HTTPS : ☑ Port : 443 UploadKey

Enable Telnet : ☑ Port : 23

Enable SSH : ☑ Port : 22 GenerateKey

Host Key Footprint : ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgw

Ping Watchdog

Ping Watchdog : ○ Enable ● Disable

IP Address To Ping :

Ping Interval : 300 Seconds

Startup Delay : 300 Seconds

Failure Count To Reboot : 3

Save

- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default one.
  - ➔ **Description :** Provide description of the system.
  - ➔ **Location :** Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to ***Appendix D. Network manager Privileges***.

- **Root Password :** Log in as a root user and is allowed to change its own, plus admin user's password.
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Password :** Log in as a admin user and is allowed to change its own,
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Login Methods :** Only **root** user can enable or disable system login methods and change services port.
  - ➔ **Enable HTTP :** Check to select HTTP Service.

- ➔ **HTTP Port :** The default is **80** and the range is between 1 ~ 65535.
- ➔ **Enable HTTPS :** Check to select HTTPS Service
- ➔ **HTTPS Port :** The default is **443** and the range is between 1 ~ 65535.

> *If you already have an SSL Certificate, please click “**UploadKey**” button to select the file and upload it.*

- ➔ **Enable Telnet :** Check to select Telnet Service
- ➔ **Telnet Port :** The default is **23** and the range is between 1 ~ 65535.
- ➔ **Enable SSH :** Check to select SSH Service
- ➔ **SSH Port :** Please The default is **22** and the range is between 1 ~ 65535.

> *Click “**GenerateKey**” button to generate RSA private key. The “host key footprint” gray blank will display content of RSA key.*

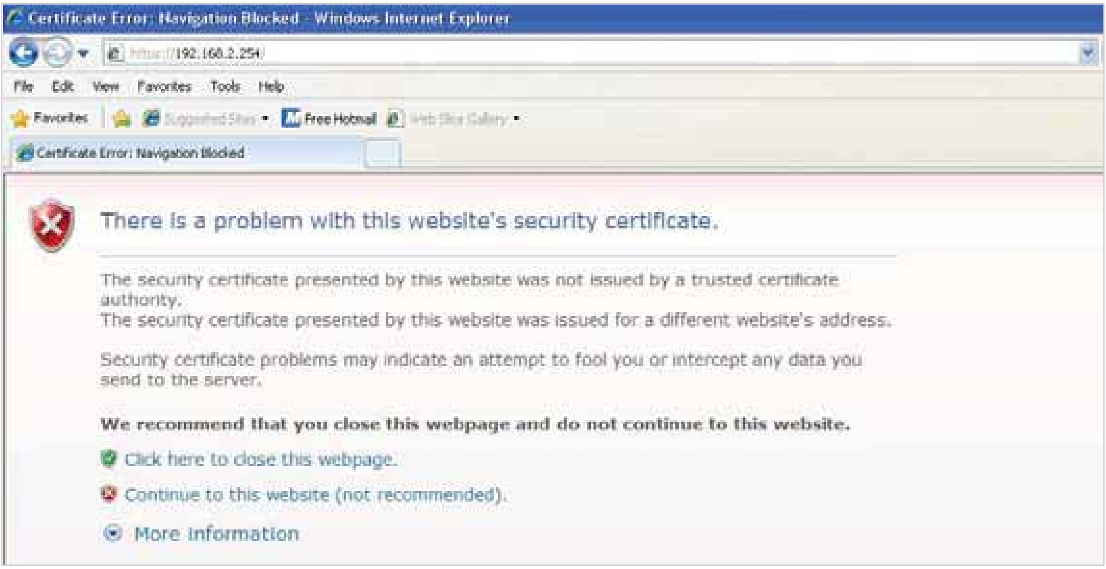
- ■ **Ping Watchdog :** The ping watchdog sets the TEW-676APBO Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the TEW-676APBO device will automatically reboot. This option creates a kind of "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 :** specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
  - ➔ **Ping Interval :** specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool. Default is **300** seconds.
  - ➔ **Startup Delay :** specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** 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.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (https://192.168.2.254). There will be a "Certificate Error", because the browser treats system as an illegal website.



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.2.254/
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

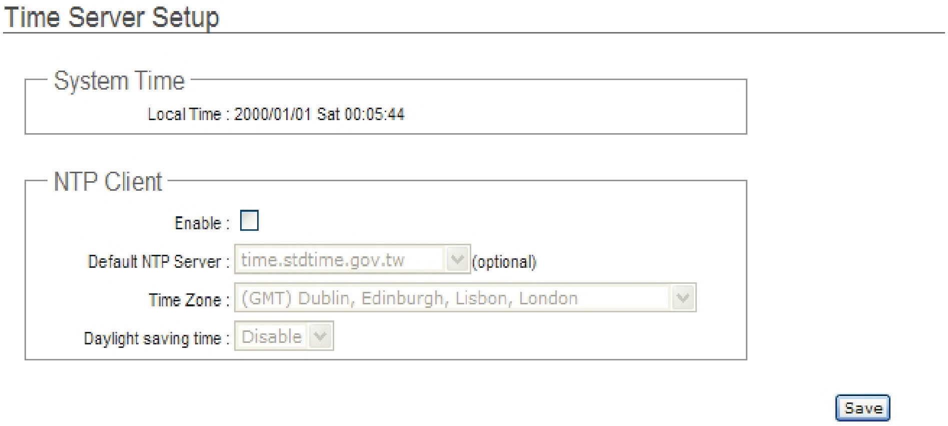
More information

Click "***Continue to this website***" to access the system's WMI. The system's Overview page will appear.

Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.



Time Server Setup

System Time

Local Time : 2000/01/01 Sat 00:05:44

NTP Client

Enable : □

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight saving time : Disable

- **Local Time :** Display the current system time.

- **NTP Client :** To synchronize the system time with NTP server.
  - ➔ **Enable :** Check to select NTP client.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Select a desired time zone from the drop-down list.
  - ➔ **Daylight saving time :** Enable or disable Daylight saving.

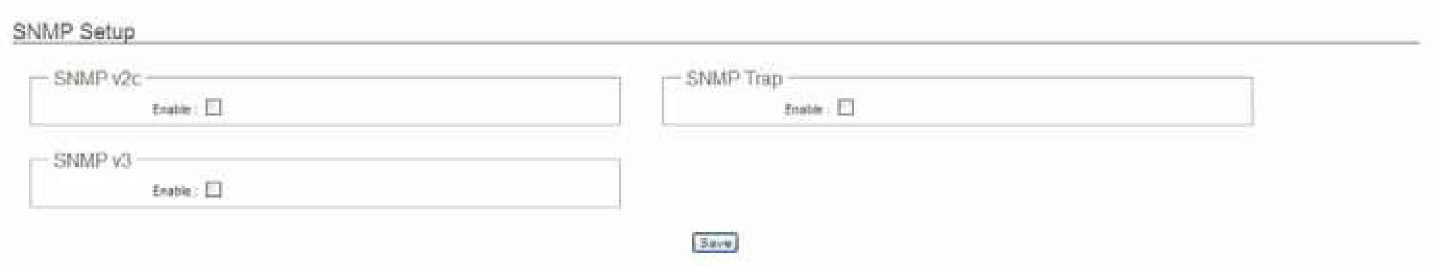
If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP manager and agent. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.



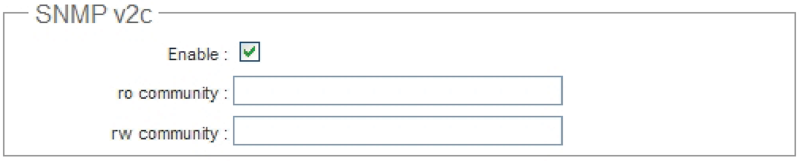
SNMP Setup

SNMP v2c
Enable : □

SNMP Trap
Enable : □

SNMP v3
Enable : □

- **SNMP v2c Enable:** Check to enable SNMP v2c.



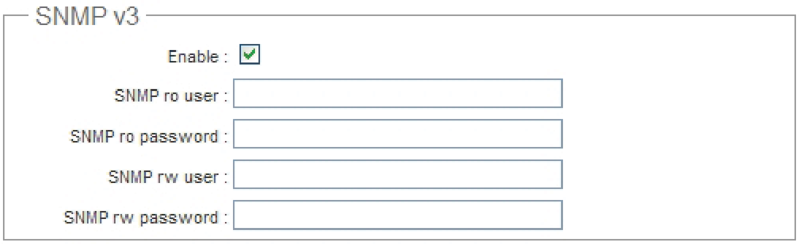
SNMP v2c
Enable : ☑
ro community :
rw community :

➔ **ro community :** Set a community string to authorize read-only access.

➔ **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

SNMPv3 supports the highest level SNMP security.



SNMP v3
Enable : ☑
SNMP ro user :
SNMP ro password :
SNMP rw user :
SNMP rw password :

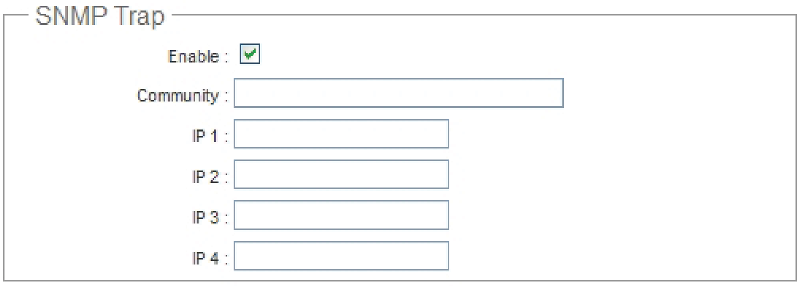
➔ **SNMP ro user :** Set a community string to authorize read-only access.

➔ **SNMP ro password :** Set a password to authorize read-only access.

➔ **SNMP rw user :** Set a community string to authorize read/write access.

➔ **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.



SNMP Trap

Enable : ☑

Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

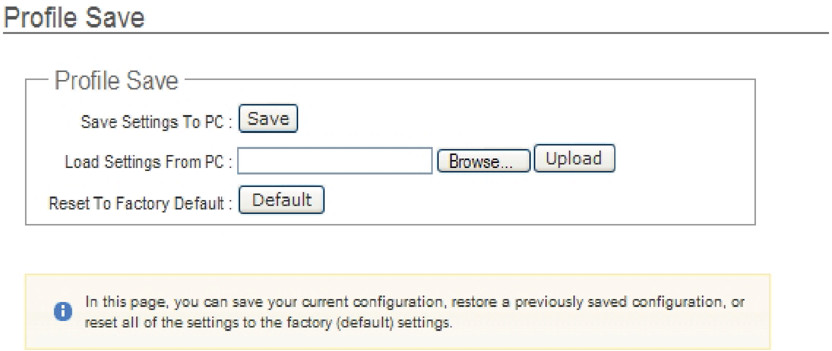
- ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

Click ***Save*** button to save changes and click ***Reboot*** button to activate.

Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.



Profile Save

Profile Save

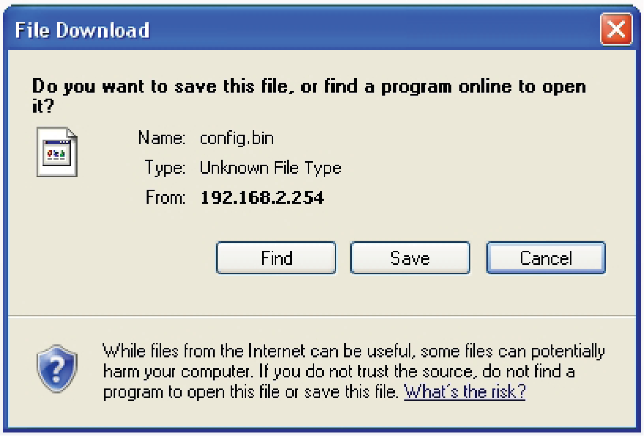
Save Settings To PC : Save

Load Settings From PC : Browse... Upload

Reset To Factory Default : Default

In this page, you can save your current configuration, restore a previously saved configuration, or reset all of the settings to the factory (default) settings.

- **Save Settings To PC :** Click ***Save*** button to save the current configuration to a local disk.



File Download

Do you want to save this file, or find a program online to open it?

Name: config.bin

Type: Unknown File Type

From: 192.168.2.254

Find Save Cancel

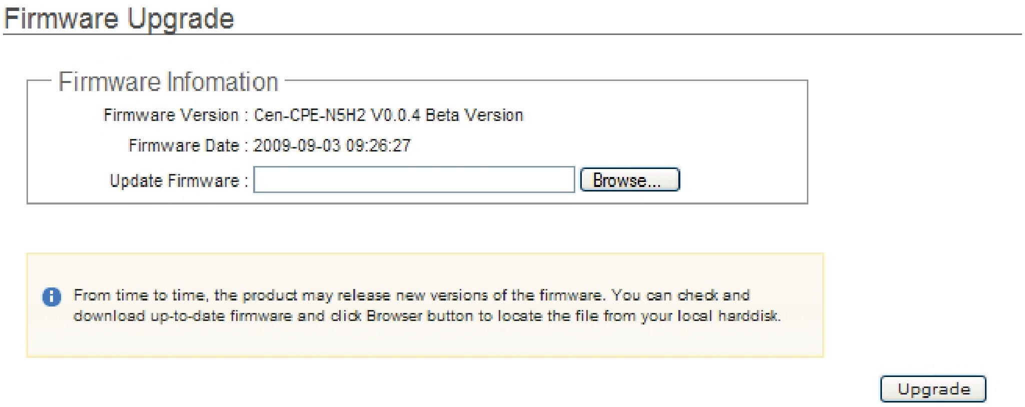
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click ***Browse*** button to locate the new firmware, and then click ***Upgrade*** button to upgrade.



Firmware Upgrade

Firmware Infomation

Firmware Version : Cen-CPE-N5H2 V0.0.4 Beta Version

Firmware Date : 2009-09-03 09:26:27

Update Firmware :

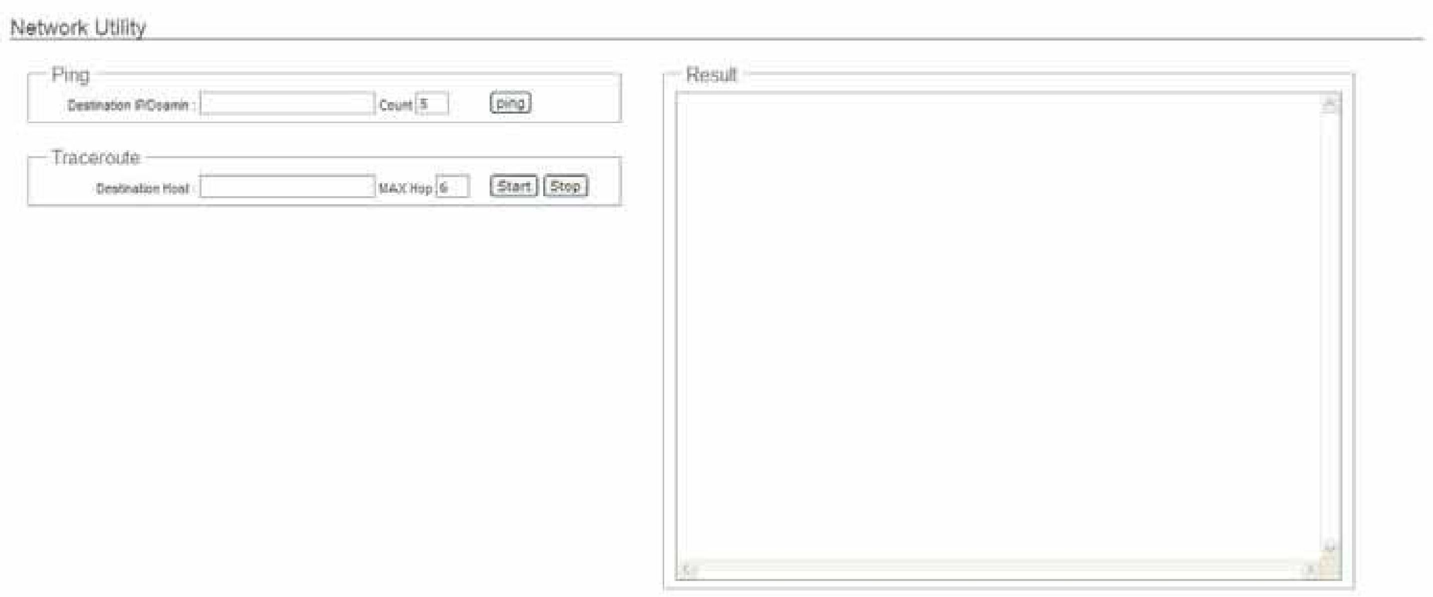
From time to time, the product may release new versions of the firmware. You can check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.

1. *To prevent data loss during firmware upgrade, please back up current settings before proceeding*
2. *Do not interrupt during firmware upgrade including power on/off as this may damage system.*
3. *Never perform firmware upgrade over wireless connection or via remote access connection.*

Network Utility

The administrator can diagnose network connectivity via the PING utility.

Please click on **Utilities -> Network Utility** and follow the below setting.



Network Utility

Ping

Destination IP/Doamin :

Count 5

Traceroute

Destination Host :

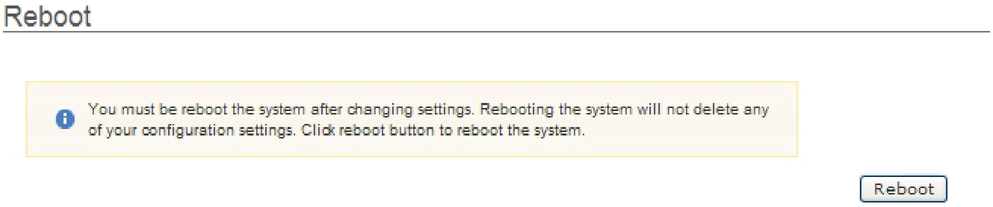
MAX Hop 6

- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - ➔ **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - ➔ **Count :** By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

- **Traceroute :** Allows tracing the hops from the TEW-676APBO device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click Stop button to stopped test
  - ➔ **Destination Host :** Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
  - ➔ **MAX Hop :** Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

Reboot

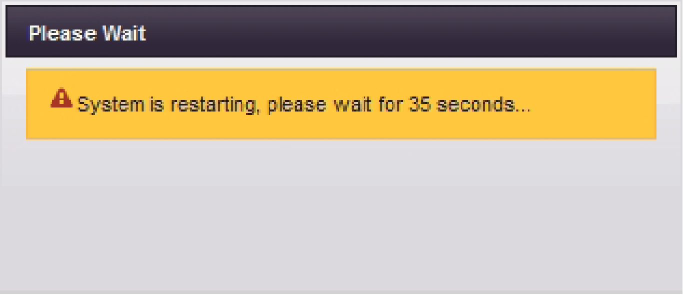
This function allows user to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.



Reboot

You must be reboot the system after changing settings. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



Please Wait

System is restarting, please wait for 35 seconds...

The **System Overview** page appears upon the completion of reboot.

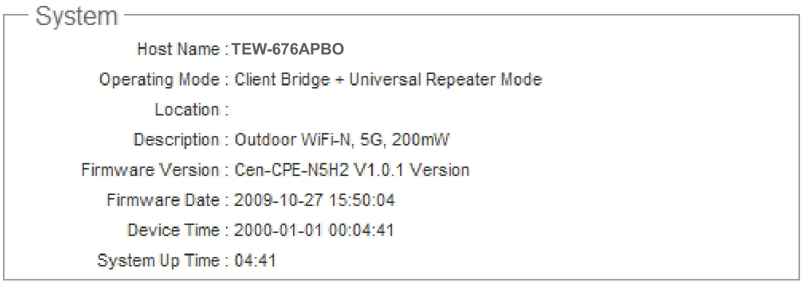
System Status

This section breaks down into subsections of ***System Overview***, ***Associated Clients Status***, ***Remote AP***, ***Extra Information*** and ***Event Log***.

System Overview

Display detailed information of ***System, Network, LAN and Wireless*** in the System Overview page.

- **System :** Display the information of the system.



System

Host Name : TEW-676APBO
Operating Mode : Client Bridge + Universal Repeater Mode
Location :
Description : Outdoor WiFi-N, 5G, 200mW
Firmware Version : Cen-CPE-N5H2 V1.0.1 Version
Firmware Date : 2009-10-27 15:50:04
Device Time : 2000-01-01 00:04:41
System Up Time : 04:41

➔ **System Name :** The name of the system.

➔ **Operating Mode :** The mode currently in service.

➔ **Location :** The reminding note on the geographical location of the system.

➔ **Description :** The reminding note of the system.

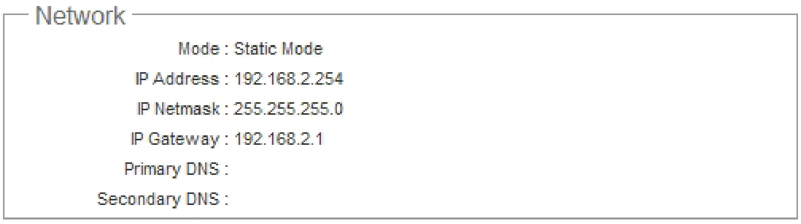
➔ **Firmware Version :** The current firmware version installed.

➔ **Firmware Date :** The build time of the firmware installed.

➔ **Device Time :** The current time of the system.

➔ **System Up Time :** The time period that system has been in service since last reboot.

- **Network Information :** Display the information of the Network.



Network

Mode : Static Mode
IP Address : 192.168.2.254
IP Netmask : 255.255.255.0
IP Gateway : 192.168.2.1
Primary DNS :
Secondary DNS :

➔ **Mode :** Supports Static or Dynamic modes on the LAN interface.

➔ **IP Address :** The management IP of system. By default, it's 192.168.2.254.

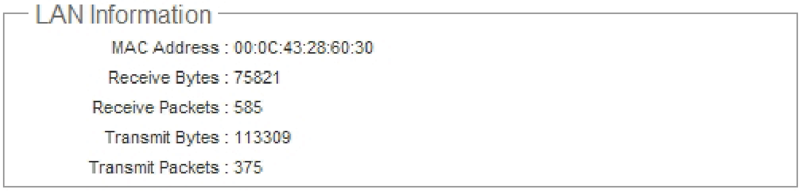
➔ **IP Netmask :** The network mask. By default, it's 255.255.255.0.

➔ **IP Gateway :** The gateway IP address and by default, it's 192.168.2.1.

➔ **Primary DNS :** The primary DNS server in service.

➔ **Secondary DNS :** The secondary DNS server in service.

- **LAN Information :** Display the detailed receive and transmit statistics of LAN interface.



LAN Information

MAC Address : 00:0C:43:28:60:30
Receive Bytes : 75821
Receive Packets : 585
Transmit Bytes : 113309
Transmit Packets : 375

➔ **MAC Address :** The MAC address of the LAN port.

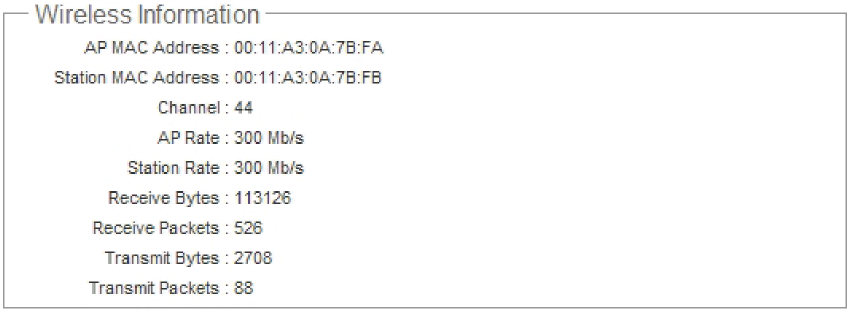
➔ **Receive bytes :** The total received packets in bytes on the LAN port.

➔ **Receive packets :** The total received packets of the LAN port.

➔ **Transmit bytes :** The total transmitted packets in bytes of the LAN port.

➔ **Transmit packets :** The total transmitted packets of the LAN port.

- **Wireless Information :** Display the detailed receive and transmit statistics of Wireless interface.



Wireless Information

AP MAC Address : 00:11:A3:0A:7B:FA
Station MAC Address : 00:11:A3:0A:7B:FB
Channel : 44
AP Rate : 300 Mb/s
Station Rate : 300 Mb/s
Receive Bytes : 113126
Receive Packets : 526
Transmit Bytes : 2708
Transmit Packets : 88

➔ **AP MAC Address :** The MAC address of the repeater AP.

➔ **Station MAC Address :** The MAC address of the Wireless Client Station.

➔ **Channel :** The current channel on the Wireless port.

➔ **AP Rate :** The current Bit Rate on the Repeater AP.

➔ **Station Rate :** The current Bit Rate on the Wireless Client Station.

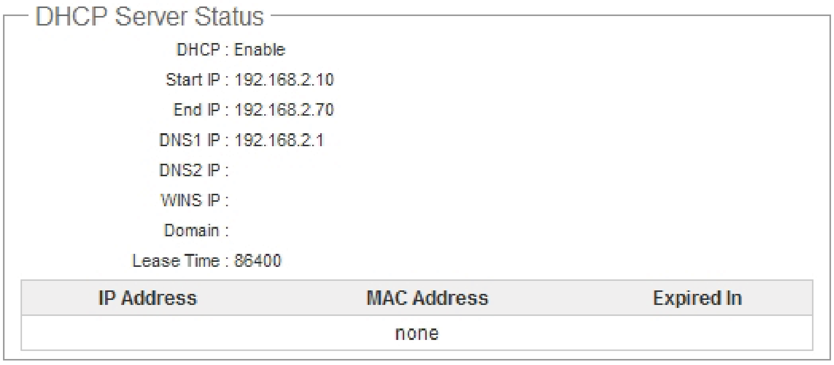
➔ **Receive bytes :**The total received packets in bytes on the Wireless port.

➔ **Receive packets :** The total received packets on the Wireless port.

➔ **Transmit bytes :** The total transmitted packets in bytes on the Wireless port.

➔ **Transmit packets :** The total transmitted packets on the Wireless port.

- **DHCP Server Status :** Users could retrieve DHCP server and DHCP clients' IP/MAC address via this field.



DHCP Server Status

DHCP : Enable
Start IP : 192.168.2.10
End IP : 192.168.2.70
DNS1 IP : 192.168.2.1
DNS2 IP :
WINS IP :
Domain :
Lease Time : 86400

IP Address	MAC Address	Expired In
	none	

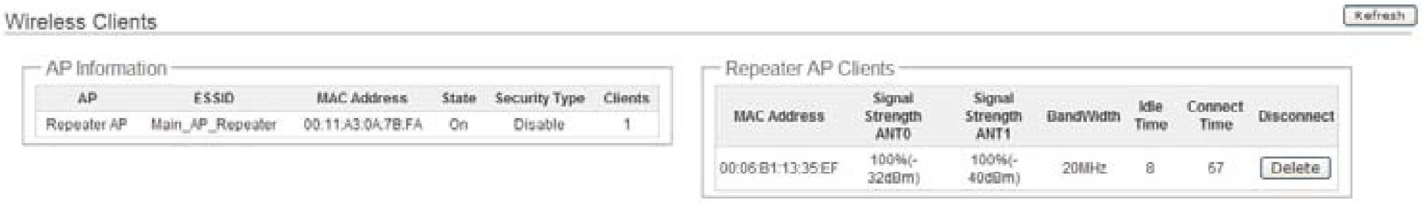
➔ **IP Address :** IP addresses to LAN devices by DHCP server.

➔ **MAC Address :** MAC addresses of LAN devices.

➔ **Expired In :** Shows how long the leased IP address will expire.

Associated Clients Status

It displays ESSID, on/off Status, Security Type, total number of wireless clients associated with Repeater AP.



AP Information

AP	ESSID	MAC Address	State	Security Type	Clients
Repeater AP	Main_AP_Repeater	00:11:A3:0A:7B:FA	On	Disable	1

Repeater AP Clients

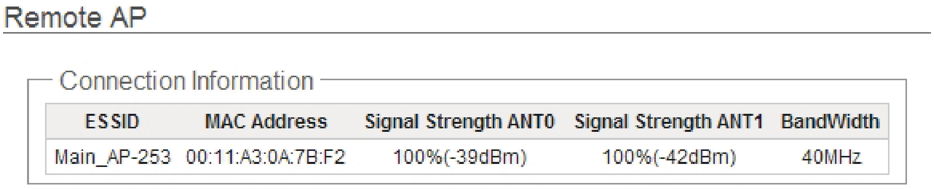
MAC Address	Signal Strength ANT0	Signal Strength ANT1	BandWidth	Idle Time	Connect Time	Disconnect
00:06:B1:13:35:EF	100%(-32dBm)	100%(-40dBm)	20MHz	8	67	Delete

- **AP Information :** Highlights key Repeater AP information.
  - ➔ **AP :** Available Repeater AP.
  - ➔ **ESSID :** Display name of ESSID for Repeater AP.
  - ➔ **MAC Address :** Display MAC address for Repeater AP.
  - ➔ **Status :** On/Off
  - ➔ **Security Type :** Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
  - ➔ **Clients :** Display total number of wireless connections on Repeater AP.

- **Repeater AP Clients :** Display all associated clients.
  - ➔ **MAC Address :** MAC address of associated clients
  - ➔ **Signal Strength ANT0/ANT1 :** Signal Strength of from associated clients.
  - ➔ **Bandwidth :** Channel bandwidth of from associated clients
  - ➔ **Idle Time :** Last inactive time period in seconds for a wireless connection.
  - ➔ **Connect Time :** Total connection time period in seconds for a wireless connection.
  - ➔ **Disconnect :** Click “**Delete**” button to manually disconnect a wireless client in a Repeater AP.

Remote AP

SSID, MAC address, antenna 0/1 received signal strength and channel bandwidth for associated AP are available.



Remote AP

Connection Information

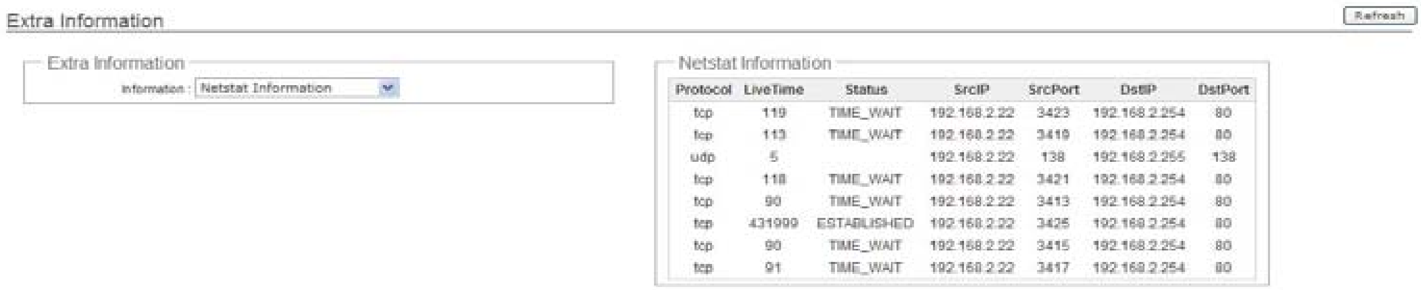
ESSID	MAC Address	Signal Strength ANT0	Signal Strength ANT1	BandWidth
Main_AP-253	00:11:A3:0A:7B:F2	100%(-39dBm)	100%(-42dBm)	40MHz

- **ESSID :** Shows the current ESSID, which must be the same on the wireless client and AP in order for communication to be established.
- **MAC Address :** Display MAC address of associated AP.
- **Signal Strength ANT0/ANT1 :** Shows the wireless signal strength of the connection between system and an access point.
- **BandWidth :** Shows the current channel bandwidth used for communication. It should be “20” or “40”

*If display “**No Connection AP!**” , you need check Wireless configuration. Things to verify are **Channel** and **Security type.** Also, adjust antenna angle and Tx Power.*

Extra Information

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

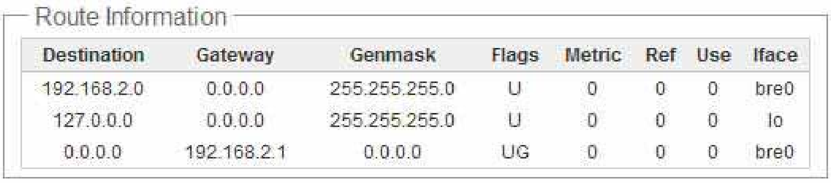


Netstat Information

Protocol	LiveTime	Status	SrcIP	SrcPort	DstIP	DstPort
tcp	119	TIME_WAIT	192.168.2.22	3423	192.168.2.254	80
tcp	113	TIME_WAIT	192.168.2.22	3419	192.168.2.254	80
udp	5		192.168.2.22	138	192.168.2.255	138
tcp	118	TIME_WAIT	192.168.2.22	3421	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3413	192.168.2.254	80
tcp	431999	ESTABLISHED	192.168.2.22	3425	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3415	192.168.2.254	80
tcp	91	TIME_WAIT	192.168.2.22	3417	192.168.2.254	80

- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

TEW-676APBO could be used as a L2 or L3 device. It doesn’t support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it’s capable of being a gateway to route packets inward and outward.

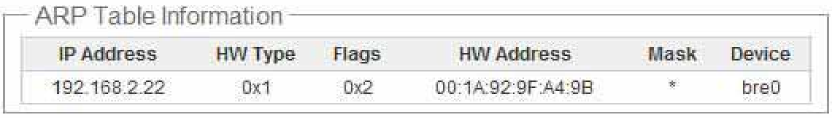


Route Information

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	bre0
127.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	lo
0.0.0.0	192.168.2.1	0.0.0.0	UG	0	0	0	bre0

- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

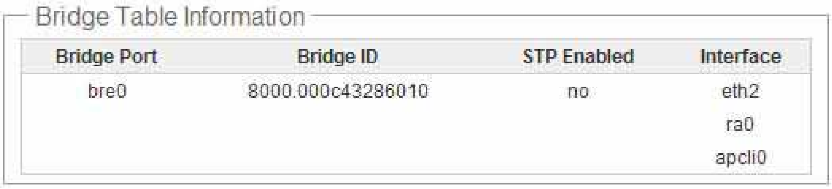


ARP Table Information

IP Address	HW Type	Flags	HW Address	Mask	Device
192.168.2.22	0x1	0x2	00:1A:92:9F:A4:9B	*	bre0

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces. (e.g. eth2, ra0 and apcli0).



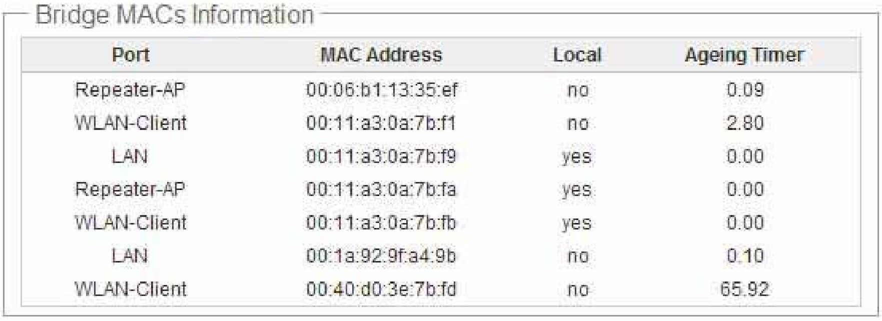
Bridge Table Information

Bridge Port	Bridge ID	STP Enabled	Interface
bre0	8000.000c43286010	no	eth2 ra0 apcli0

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

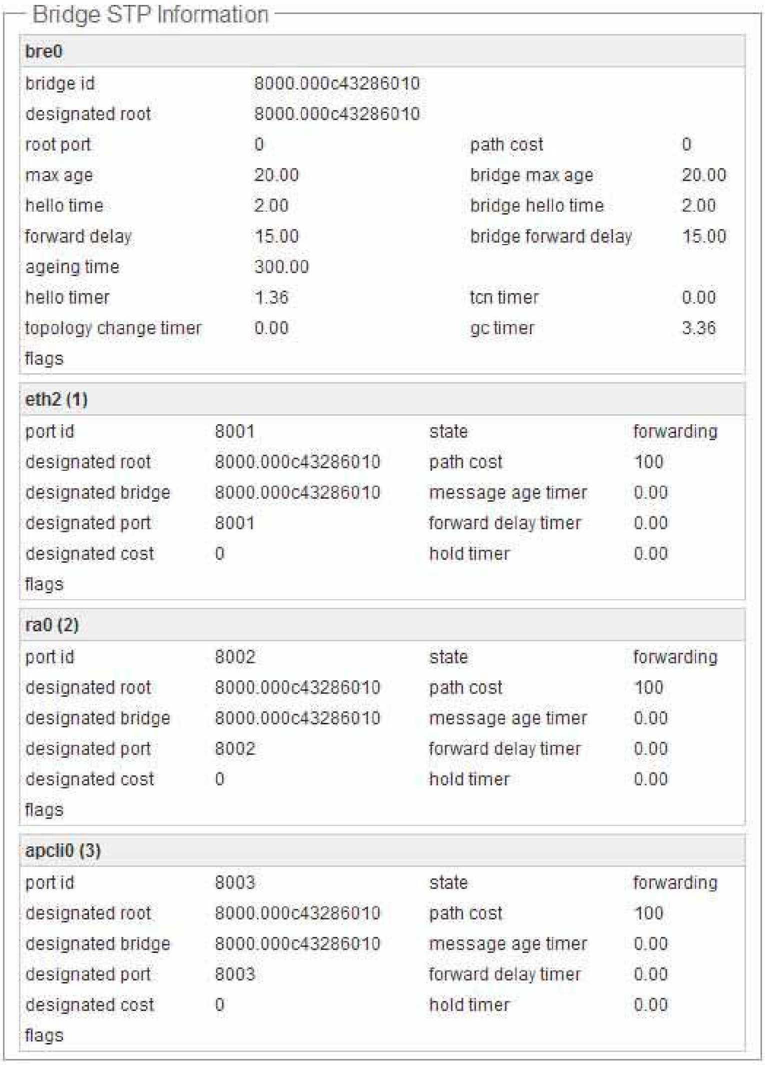
Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.



Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
Repeater-AP	00:06:b1:13:35:ef	no	0.09
WLAN-Client	00:11:a3:0a:7b:f1	no	2.80
LAN	00:11:a3:0a:7b:f9	yes	0.00
Repeater-AP	00:11:a3:0a:7b:fa	yes	0.00
WLAN-Client	00:11:a3:0a:7b:fb	yes	0.00
LAN	00:1a:92:9f:a4:9b	no	0.10
WLAN-Client	00:40:d0:3e:7b:fd	no	65.92

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.



Bridge STP Information

bre0			
bridge id	8000.000c43286010		
designated root	8000.000c43286010		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00		
hello timer	1.36	tcn timer	0.00
topology change timer	0.00	gc timer	3.36
flags			

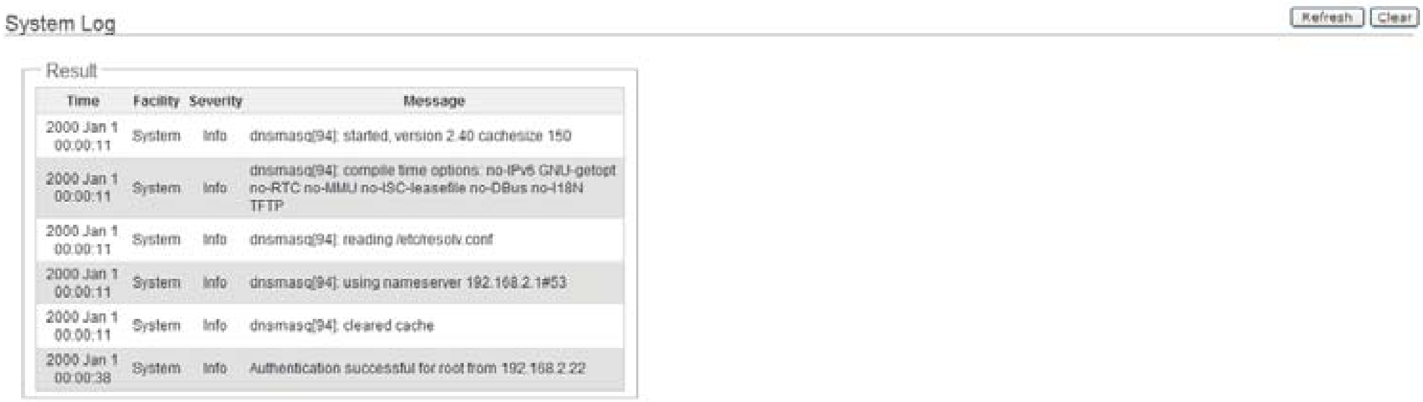
eth2 (1)			
port id	8001	state	forwarding
designated root	8000.000c43286010	path cost	100
designated bridge	8000.000c43286010	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

ra0 (2)			
port id	8002	state	forwarding
designated root	8000.000c43286010	path cost	100
designated bridge	8000.000c43286010	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

apcli0 (3)			
port id	8003	state	forwarding
designated root	8000.000c43286010	path cost	100
designated bridge	8000.000c43286010	message age timer	0.00
designated port	8003	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.



Time	Facility	Severity	Message
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: started, version 2.40 cachesize 150
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-I18N TFTP
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: reading /etc/resolv.conf
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: using nameserver 192.168.2.1#53
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: cleared cache
2000 Jan 1 00:00:38	System	Info	Authentication successful for root from 192.168.2.22

- **Time :** The date and time when the event occurred.
- **Facility :** It helps users to identify source of events such "System" or "User"
- **Severity :** Severity level that a specific event is associated such as "info", "error", "warning", etc.
- **Message :** Description of the event.

Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

Router AP Mode Configuration

When Router AP mode is chosen, the system can be configured as a Router with Access Point and WDS function. This section provides detailed explanation for users to configure in the Router AP mode with help of illustrations. In the Router AP mode, functions listed in the table below are also available from the Web-based GUI interface.

OPTION	System	Wireless	Advance	Utilities	Status
Functions	Operating Mode	General Setup	DMZ	Profiles Settings	System Overview
	WAN	Advanced Setup	IP Filter	Firmware Upgrade	Station Statistics
	LAN	Virtual AP Setup	MAC Filter	Network Utility	Extra Info
	DDNS	WDS Setup	Virtual Server	Reboot	QoS Plot
	Management		Parental Control		Event Log
	Time Server		QoS		
	UPNP				
	SNMP				

Table 8-1: Router AP Mode Functions

External Network Connection

Network Requirement

It can be used as an Router AP with WDS function. In this mode, TEW-676APBO is a gateway enabled with NAT and DHCP Server functions. The wireless clients connected to TEW-676APBO are in **different** subnet from those connected to Internet.

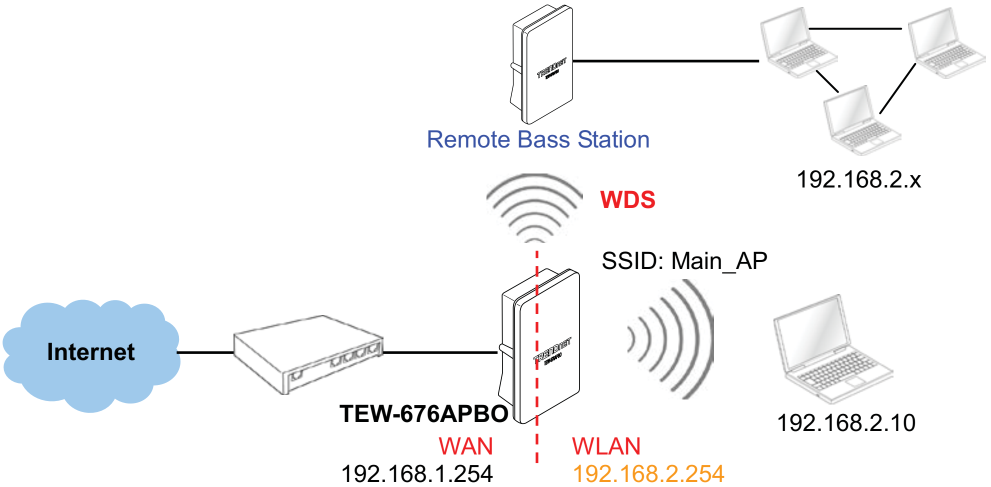
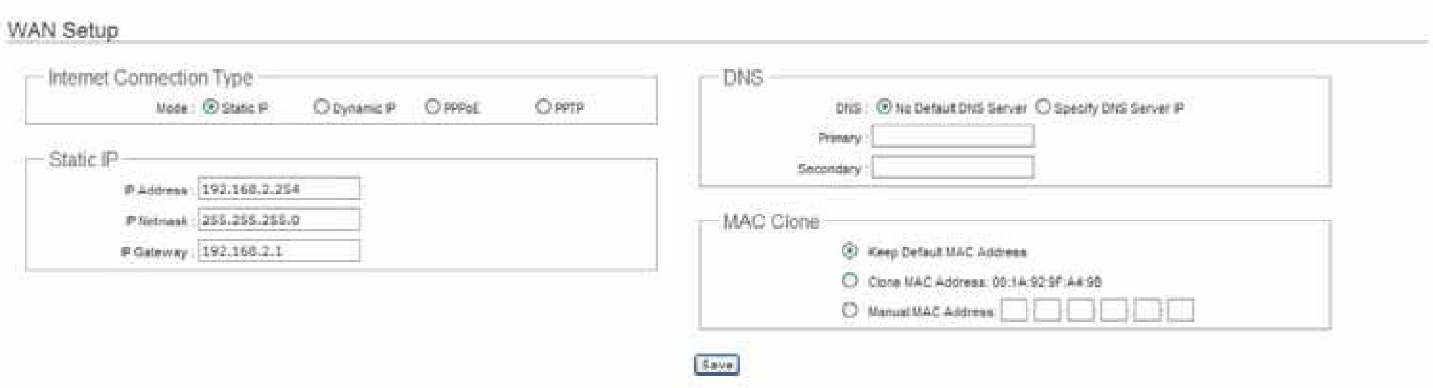


Figure 8-1 Router AP mode network configuration

Configure WAN Setup

There are three connection types for the WAN port : **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**.

Please click on **System -> WAN** and follow the below setting.



WAN Setup

Internet Connection Type

Mode : ● Static IP ○ Dynamic IP ○ PPPoE ○ PPTP

Static IP

IP Address : 192.168.2.254

IP Netmask : 255.255.255.0

IP Gateway : 192.168.2.1

DNS

DNS : ● No Default DNS Server ○ Specify DNS Server IP

Primary :

Secondary :

MAC Clone

● Keep Default MAC Address

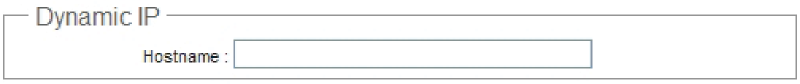
○ Clone MAC Address: 00:1A:92:9F:A4:9B

○ Manual MAC Address: □ □ □ □ □ □

Save

In Router AP mode, the WAN Port is the wired interface.

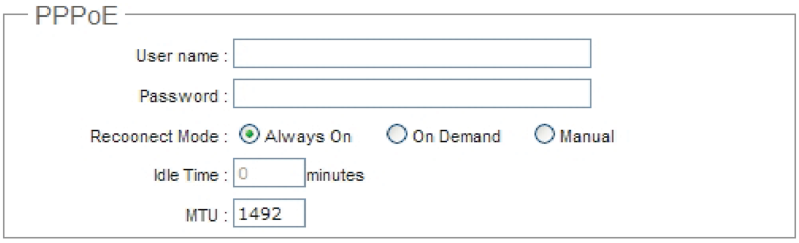
- **Mode :** By default, it's "***Static IP***". Check "Static IP", "Dynamic IP", "PPPoE" or "PPTP"to set up system WAN IP.
  - ➔ **Static IP :** Users can manually setup the WAN IP address with a static IP provided by WISP.
    - ✓ **IP Address :** The IP address of the WAN port; default IP address is 192.168.1.254
    - ✓ **IP Netmask :** The Subnet mask of the WAN port; default Netmask is 255.255.255.0
    - ✓ **IP Gateway :** The default gateway of the WAN port; default Gateway is 192.168.1.1
  - ➔ **Dynamic IP :** Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings including DNS can be available from DHCP server. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to "**WAN Information**" in the Overview page to click ***Release*** button to release IP address and click ***Renew*** button to renew IP address again.



Dynamic IP

Hostname :

    - ✓ **Hostname :** The Hostname of the WAN port



PPPoE

User name :

Password :

Recoonect Mode : ● Always On ○ On Demand ○ Manual

Idle Time : 0 minutes

MTU : 1492

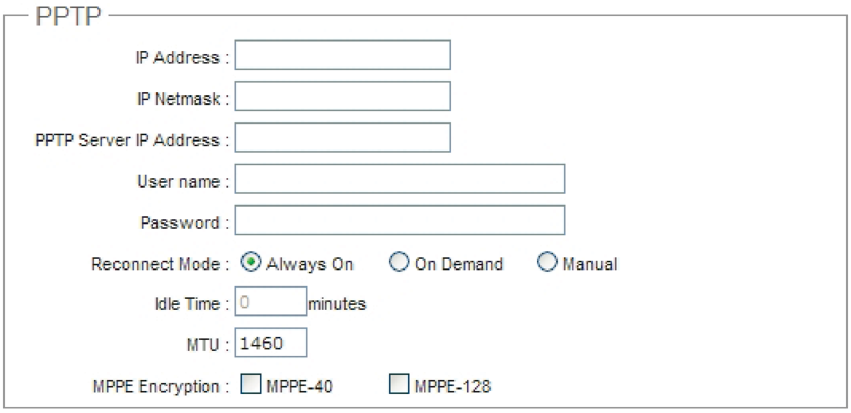
  - ➔ **PPPoE :** To create wireless PPPoE WAN connection to a PPPoE server in network.

- ✓ **User Name :** Enter User Name for PPPoE connection
- ✓ **Password :** Enter Password for PPPoE connection
- ✓ **Reconnect Mode :**
  - **Always on** – A connection to Internet is always maintained.
  - **On Demand** – A connection to Internet is made as needed.

*When **Time Server** is enabled at the "On Demand" mode, the "Reconnect Mode" will turn out "Always on".*

  - **Manual** – Click the "**Connect**" button on "**WAN Information**" in the Overview page to connect to the Internet.
- ✓ **Idle Time :** Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is "**0**", indicates disabled. When Idle time is disabled, the "**Reconnect Mode**" will turn out "**Always on**"
- ✓ **MTU :** By default, it's **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.

➔ **PPTP :** The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.



PPTP

IP Address :

IP Netmask :

PPTP Server IP Address :

User name :

Password :

Reconnect Mode : ● Always On ○ On Demand ○ Manual

Idle Time : 0 minutes

MTU : 1460

MPPE Encryption : □ MPPE-40 □ MPPE-128

- ✓ **IP Address :** The IP address of the WAN port
- ✓ **IP Netmask :** The Subnet mask of the WAN port
- ✓ **PPTP Server IP Address :** The IP address of the PPTP server
- ✓ **User Name :** Enter User Name for PPTP connection
- ✓ **Password :** Enter Password for PPTP connection
- ✓ **Reconnect Mode :**
  - **Always on** – A connection to Internet is always maintained.
  - **On Demand** – A connection to Internet is made as needed.

*When **Time Server** is enabled at the "On Demand" mode, the "Reconnect Mode" will turn out "Always on".*

- **Manual** – Click the "**Connect**" button on "**WAN Information**" in the Overview page to connect to the Internet.

✓ **Idle Time :** Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is "**0**", indicates disabled. When Idle time is disabled, the "**Reconnect Mode**" will turn out "**Always on**"

✓ **MTU :** By default, it's **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.

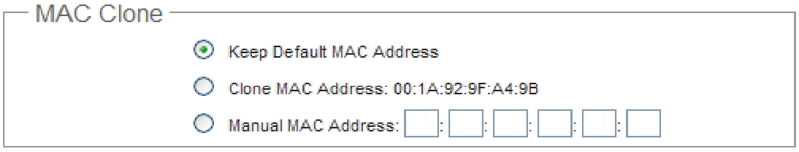
✓ **MPPE Encryption :** Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. **128-bit** key (strong) and **40-bit** key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.

■ **DNS :** Check "No Default DNS Server" or "Specify DNS Server IP" radial button as desired to set up system DNS.

➔ **Primary :** The IP address of the primary DNS server.

➔ **Secondary :** The IP address of the secondary DNS server.

■ **MAC Clone :** The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



MAC Clone

● Keep Default MAC Address

○ Clone MAC Address: 00:1A:92:9F:A4:9B

○ Manual MAC Address: □:□:□:□:□:□

➔ **Keep Default MAC Address :** Keep the default MAC address of WAN port on the system.

➔ **Clone MAC Address :** If you want to clone the MAC address of the PC, then click the **Clone MAC Address** button. The system will automatically detect your PC's MAC address.

The Clone MAC Address field will display MAC address of the PC connected to system. Click "Save" button can make clone MAC effective.

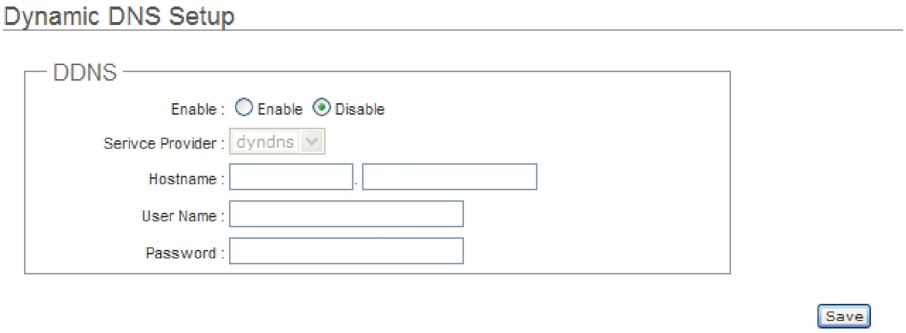
➔ **Manual MAC Address :** Enter the MAC address registered with your ISP.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Configure DDNS Setup

Dynamic DNS allows you to map domain name to dynamic IP address.

Please click on **System -> DDNS Setup** and follow the below setting.



Dynamic DNS Setup

DDNS

Enable : ○ Enable ● Disable

Serivce Provider : dyndns

Hostname : .

User Name :

Password :

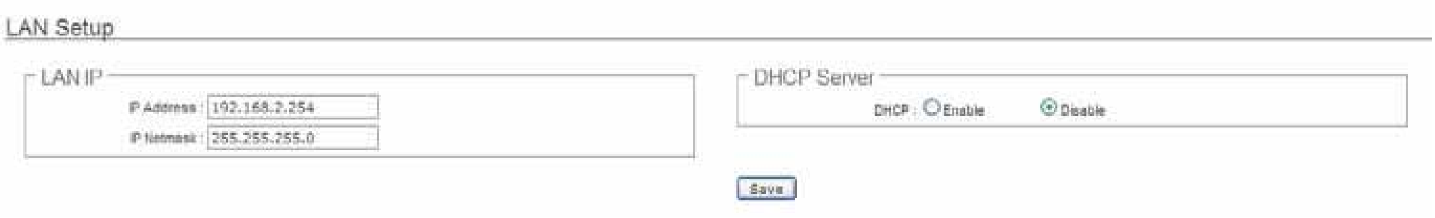
- **Enabled:** By default, it's "***Disable***"*.* The mapping domain name won't change when dynamic IP changes. The beauty of it is no need to remember the dynamic WAP IP while accessing to it.
- **Service Provider:** Select the preferred Service Provider from the drop-down list including *dyndns*, *dhs*, *ods* and *tzo*
- **Hostname:** Host Name that you register to Dynamic-DNS service and export.
- **User Name & Password:** User Name and Password are used to login DDNS service.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Configure LAN Setup

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.



LAN Setup

LAN IP

IP Address : 192.168.2.254

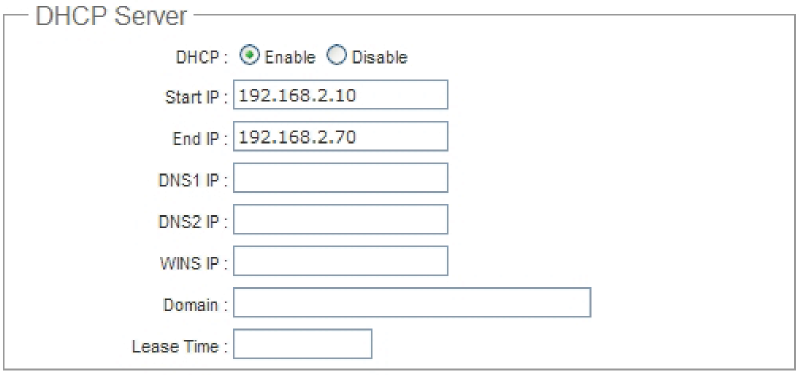
IP Netmask : 255.255.255.0

DHCP Server

DHCP : ○ Enable ● Disable

- **LAN IP :** The administrator can manually setup the LAN IP address.
  - ➔ **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
  - ➔ **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0

- **DHCP Setup :** Devices connected to the system can obtain an IP address automatically when this service is enabled.



DHCP Server

DHCP : ● Enable ○ Disable

Start IP : 192.168.2.10

End IP : 192.168.2.70

DNS1 IP :

DNS2 IP :

WINS IP :

Domain :

Lease Time :

- ➔ **DHCP :** Check ***Enable*** button to activate this function or ***Disable*** to deactivate this service.
- ➔ **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- ➔ **DNS1 IP :** Enter IP address of the first DNS server; this field is required.
- ➔ **DNS2 IP :** Enter IP address of the second DNS server; this is optional.
- ➔ **WINS IP :** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- ➔ **Domain :** Enter the domain name for this network.
- ➔ **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 interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

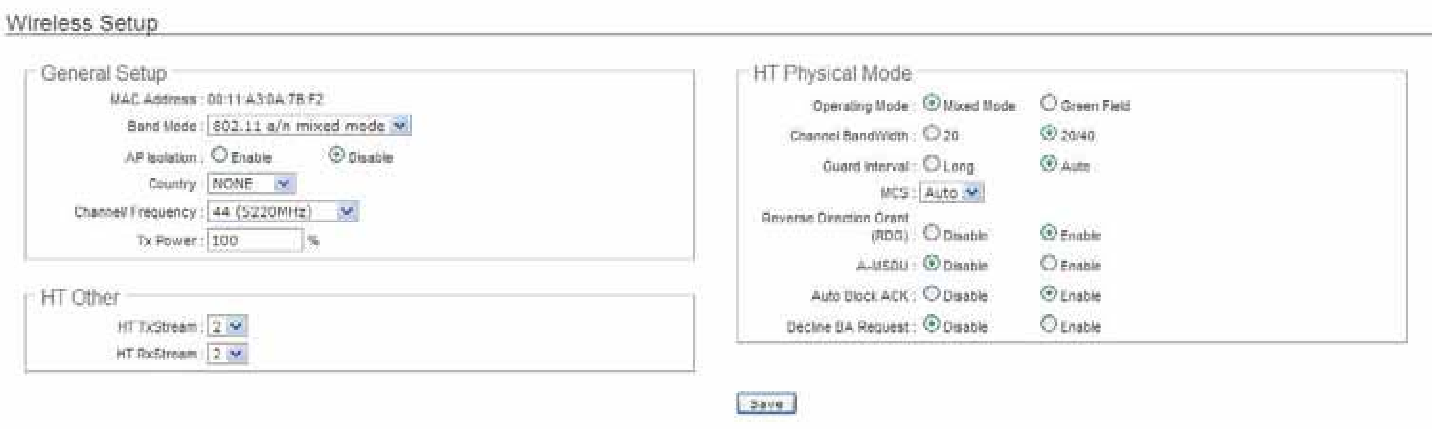
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Wireless LAN Network Creation

The network manager can configure related wireless settings, **General Settings, Advanced Settings, Virtual AP(VAP) Setting, Security Settings,** and **MAC Filter Settings**.

Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.



Wireless Setup

General Setup

MAC Address : 00:11:A3:0A:7B:F2

Band Mode : 802.11 a/n mixed mode

AP Isolation : ○ Enable ● Disable

Country : NONE

Channel/ Frequency : 44 (5220MHz)

Tx Power : 100 %

HT Other

HT TxStream : 2

HT RxStream : 2

HT Physical Mode

Operating Mode : ● Mixed Mode ○ Green Field

Channel BandWidth : ○ 20 ● 20/40

Guard Interval : ○ Long ● Auto

MCS : Auto

Reverse Direction Grant (RDG) : ○ Disable ● Enable

A-MSDU : ● Disable ○ Enable

Auto Block ACK : ○ Disable ● Enable

Decline BA Request : ● Disable ○ Enable

- **MAC Address :** The MAC address of the Wireless interface is displayed here.
- **Band Mode :** Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed** mode.
- **AP Isolation :** Select **Enable**, all clients will be isolated from each VAP, that means different VAP's clients can not reach to each other.
- **Transmit Rate Control :** Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54Mbps** only for **802.11a** mode.
- **Country :** Select the desired country code from the drop-down list; the options are ***US***, ***ETSI***, ***JP*** and ***NONE***.
- **Channel/Frequency :** The channel range will be changed by selecting different country code. Below depicts the channel range for different ***Country***. When "**Band Mode**" selected in "**802.11a**", the Channel **140** and **165** does not shown-up on list.

Country	**Channel**
US	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
JP	36, 40, 44, 48
NONE	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161.165

- **Tx Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between ***1*** to ***100*** (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting, **100**%.

When **Band Mode** select in **802.11a only mode**, the **HT(High Throughput)** settings should be hidden immediately.

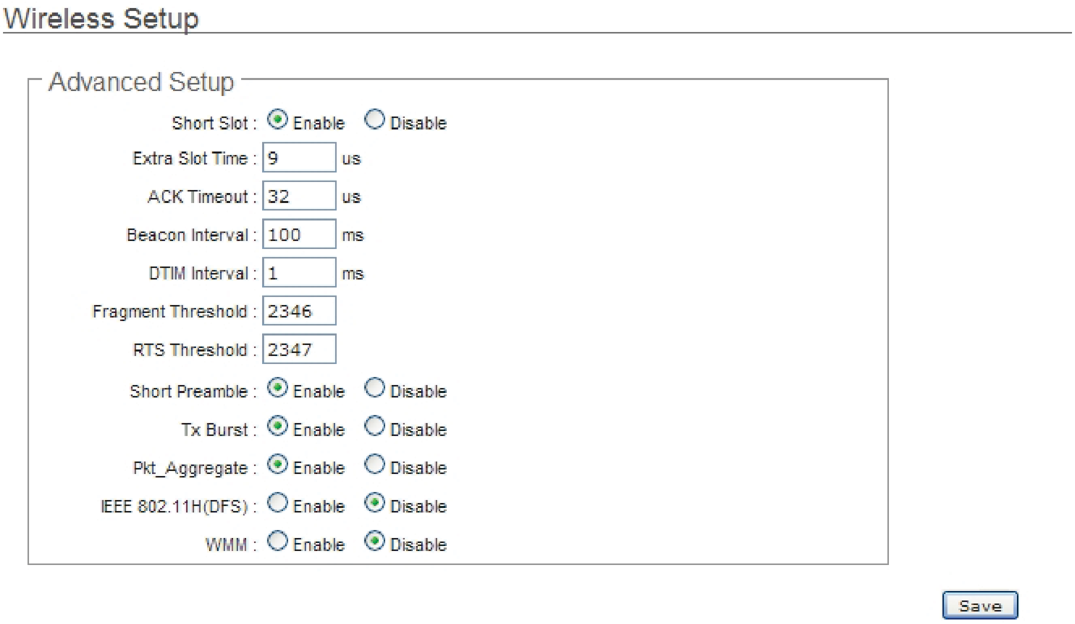
- **HT TxStream**/**RxStream :** By default, it's **2**.
- **Operating Mode :** By default, it's Mixed Mode.
  - ➔ **Mixed Mode : I**n this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
  - ➔ **Green Field :** In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth :** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval :** Using "**Auto**" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **MCS :** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to **Appendix C. MCS Data Rate**)
- **Reverse Direction Grant(RDG) :** Disable or enable reserve direction grant. Default is enabled.
- **A-MSDU :** Aggregated Mac Service Data Unit. Select **Enable** to allow aggregation for multiple MSDUs in one MPDU Default is disabled.
- **Auto Block ACK :** Disable or enable auto block ACK. Default is enabled.
- **Decline BA Request :** Disable or enable decline BA request. Default is disabled.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to **all VAPs** and **WDS Links**.

Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



Wireless Setup

Advanced Setup

Short Slot : ● Enable ○ Disable

Extra Slot Time : 9 us

ACK Timeout : 32 us

Beacon Interval : 100 ms

DTIM Interval : 1 ms

Fragment Threshold : 2346

RTS Threshold : 2347

Short Preamble : ● Enable ○ Disable

Tx Burst : ● Enable ○ Disable

Pkt_Aggregate : ● Enable ○ Disable

IEEE 802.11H(DFS) : ○ Enable ● Disable

WMM : ○ Enable ● Disable

- **Short Slot :** By default, it's "***Enable***" for educing the slot time from the standard **20** *microseconds* to the **9** *microsecond* short slot time

  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **Extra Slot Time :** Slot time is in the range of **1~255** and set in unit of ***microsecond***. The default value is **9** microsecond.

When you enable Short Slot and set Extra Slot time to "10", the actual Slot Time=9+10 us.
When you disable Short Slot and set Extra Slot time to "10", the actual Slot Time=20+10 us.

- **ACK Timeout :** ACK timeout is in the range of **1~255** and set in unit of ***microsecond***. The default value is **32** microsecond.

All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughputs become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval :** Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1~255**. The default is **1**.

DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256~2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

  With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

- **Pkt_Aggregate :** By default, it's "***Enable***"

  Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.

- **IEEE802.11H (DFS) :** By default, it's "***Disable***". To ***Enable*** is to use IEEE802.11H(DFS)

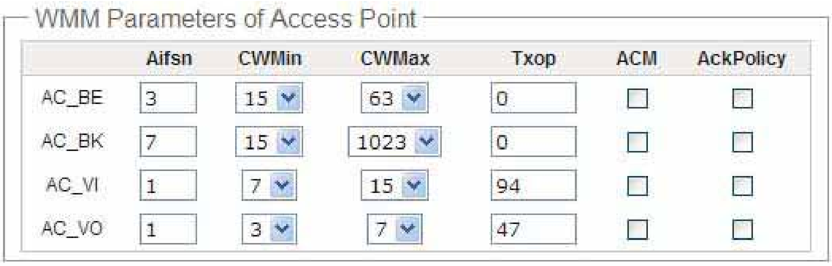
  With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

DFS Channels	52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.

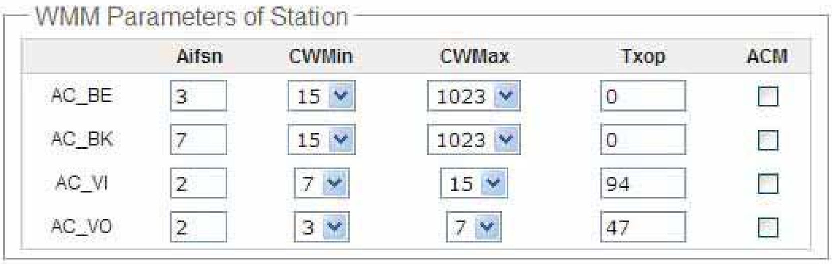
*The Channel **52-140** is DFS channel. If tuen on IEEE802.11H, AP Will have **60** sec to do channel available check, and will not send beacon and can not be connect. When* TEW-676APBO *detect radar(5GHz) signal, the AP will switch channel and stop beacon trasmit between **15** sec.*

- **WMM :** By default, it's "***Disable***". To ***Enable*** is to use WMM and the WMM parameters should appears.



WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐



WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

➔ **WMM Parameters of Access Point :** *This affects traffic flowing from the access point to the client station*

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM :** Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy :** Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "**Checkbox**" indicates "**No ACK**"

  When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

  When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ **WMM Parameters of Station :** *This affects traffic flowing from the client station to the access point.*

Queue	Data Transmitted Clients to AP	Priority	Description
AC_BK	Background.	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.

- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM :** Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **all VAPs** and **WDS Links**.

Create Virtual AP (VAP)

The TEW-676APBO support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into **7** logical access points, each of which can have a different set of security and network settings. **Figure 8-2** shows multiple SSIDs with security type settings.

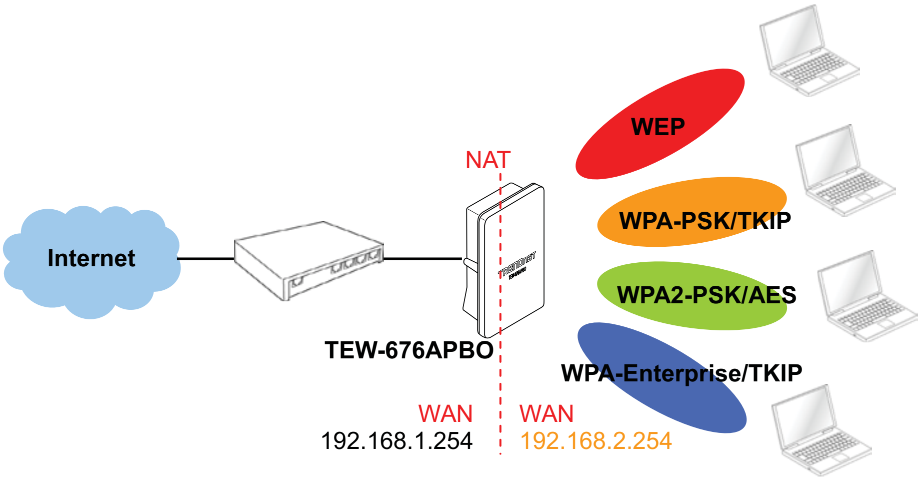
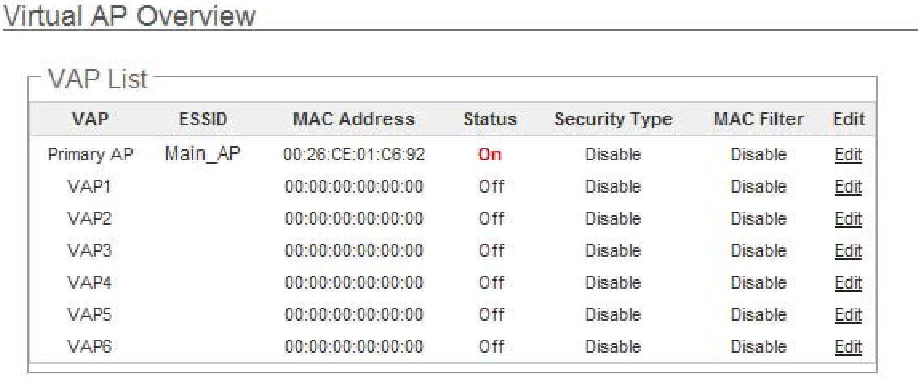


Figure 8-2 Multiple SSIDs with different Security Type

Virtual AP Overview

The administrator can view all of the Virtual AP's settings via this page.

Please click on **Wireless -> Virtual AP Setup** and the Virtual AP Overview Page appears.



Virtual AP Overview

VAP List

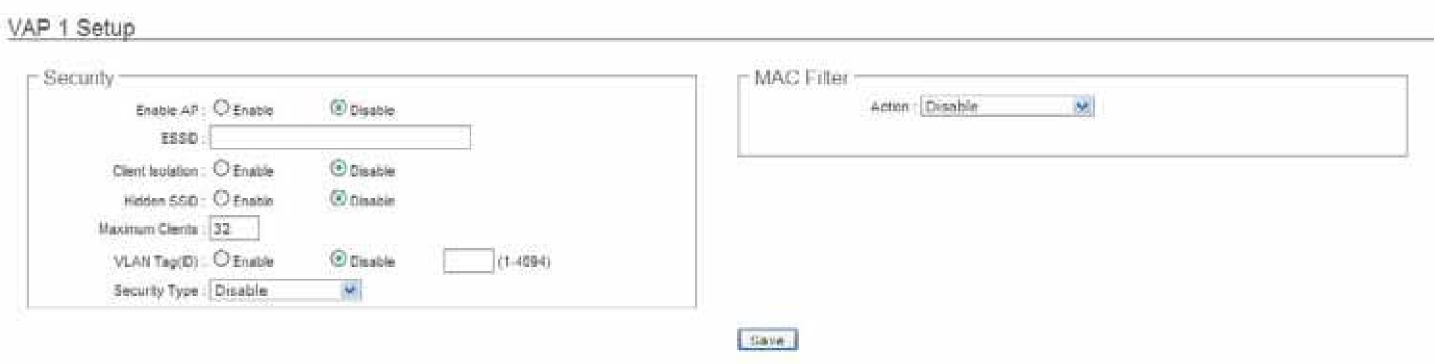
VAP	ESSID	MAC Address	Status	Security Type	MAC Filter	Edit
Primary AP	Main_AP	00:26:CE:01:C6:92	On	Disable	Disable	Edit
VAP1		00:00:00:00:00:00	Off	Disable	Disable	Edit
VAP2		00:00:00:00:00:00	Off	Disable	Disable	Edit
VAP3		00:00:00:00:00:00	Off	Disable	Disable	Edit
VAP4		00:00:00:00:00:00	Off	Disable	Disable	Edit
VAP5		00:00:00:00:00:00	Off	Disable	Disable	Edit
VAP6		00:00:00:00:00:00	Off	Disable	Disable	Edit

- **VAP :** Indicate the system's Virtual AP.
- **ESSID :** Indicate the ESSID of the respective Virtual AP
- **MAC Address :** The MAC address of the VAP Interface is displayed here. When you enable AP and reboot system, the MAC address will display here.
- **Status :** Indicate the Status of the respective Virtual AP. The **Primary AP** always on.
- **Security Type :** Indicate an used security type of the respective Virtual AP.
- **MAC Filter :** Indicate an used MAC filter of the respective Virtual AP.
- **Edit :** Click **Edit** button to configure Virtual AP's settings, including security type and MAC Filter.

Virtual AP Setup

For each Virtual AP, administrators can configure SSID, SSID broadcasting, Maximum number of client associations, security type settings.

Click **Edit** button on the Edit column, and then a Virtual AP setup page appears.



VAP 1 Setup

Security

Enable AP : ○ Enable ● Disable

ESSID :

Client Isolation : ○ Enable ● Disable

Hidden SSID : ○ Enable ● Disable

Maximum Clients : 32

VLAN Tag(ID) : ○ Enable ● Disable (1-4094)

Security Type : Disable

MAC Filter

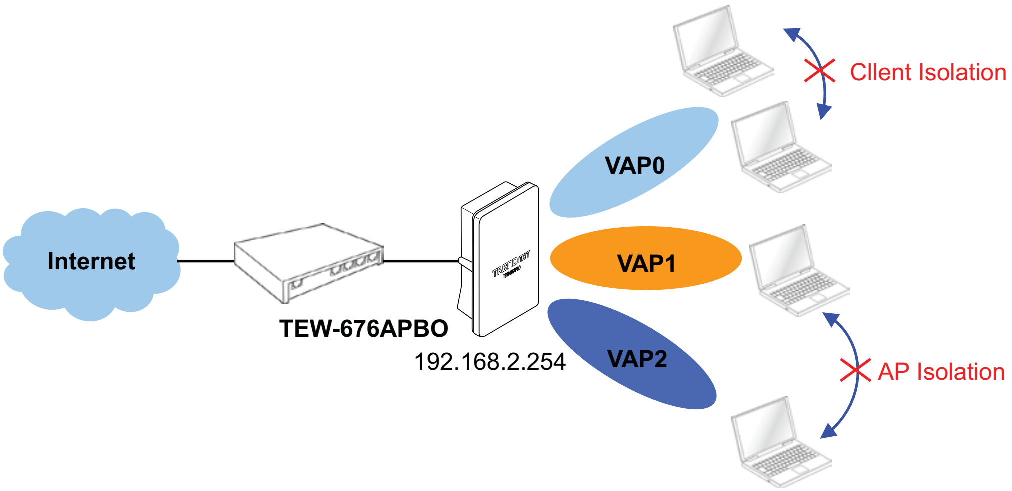
Action : Disable

- **Enable AP :** By default, it's "***Disable***" for VAP1 ~ VAP6. **The Primary AP always enabled**.

  Select "***Enable***" to activate VAP or click "***Disable***" to deactivate this function

- **ESSID :** Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP's clients associated with the specified VAP.

- **Client Isolation :** Select **Enable**, all clients will be isolated from each other, that means all clients can not reach to other clients. Below Figures depict Client Isolation and AP Isolation



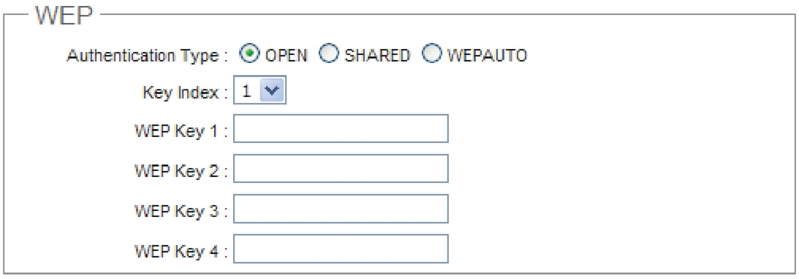
- **Hidden SSID :** By default, it's "***Disable***".

  Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP clients could make to associate to it.

- **Maximum Clients :** The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.

In this mode, the system does not support VLAN Tag(ID) function.

- **Security Type :** Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
  - ➔ **Disable :** Data are unencrypted during transmission when this option is selected.
  - ➔ **WEP :** Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.



WEP

Authentication Type : ● OPEN ○ SHARED ○ WEPAUTO

Key Index : 1

WEP Key 1 :

WEP Key 2 :

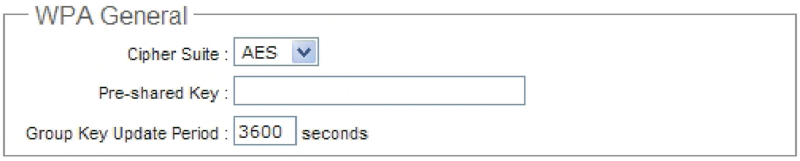
WEP Key 3 :

WEP Key 4 :

- **Authentication Method :** Enable the desire option among ***OPEN***, ***SHARED*** or ***WEPAUTO***.
  - ➔ Key Index : Key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
  - ➔ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	**Hex**	**ASCII**
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

- ➔ **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.



WPA General

Cipher Suite : AES

Pre-shared Key :

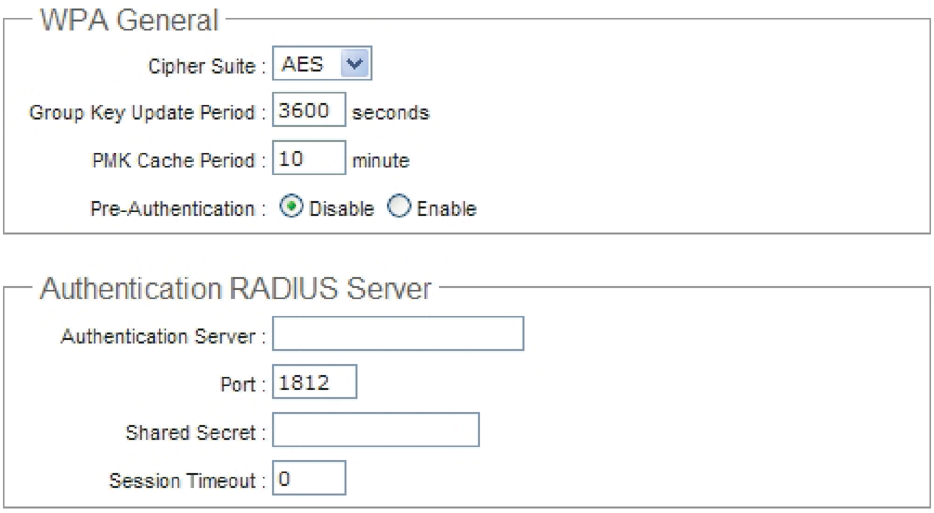
Group Key Update Period : 3600 seconds

- ✓ **Cipher Suite :** By default, it is **AES**. Select either AES or TKIP cipher suites
- ✓ **Pre-shared Key :** Enter the pre-shared key; the format shall go with the selected key type.

Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

- ✓ **Group Key Update Period :** By default, it is **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

➔ **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this is selected.



WPA General

Cipher Suite : AES

Group Key Update Period : 3600 seconds

PMK Cache Period : 10 minute

Pre-Authentication : ● Disable ○ Enable

Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

Session Timeout : 0

✓ **WPA General Settings :**

- **Cipher Suite :** By default, it is AES. Select either AES or TKIP cipher suites
- **Group Key Update Period :** By default, it's **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- **PMK Cache Period :** By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- **Pre-Authentication :** By default, it's "Disable". To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.

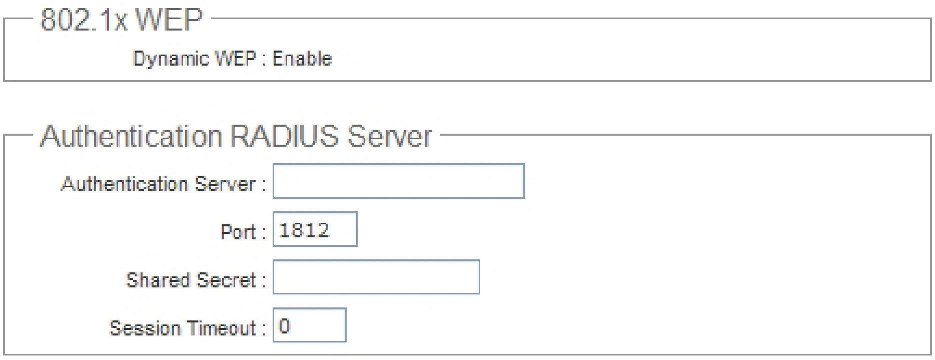
PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise

✓ **Radius Server Settings :**

- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60** *seconds*. The default is **0** to disable re-authenticate service.

  Amount of time before a client will be required to re-authenticate.

➔ **WEP 802.1X :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.



802.1x WEP

Dynamic WEP : Enable

Authentication RADIUS Server

Authentication Server :

Port : 1812

Shared Secret :

Session Timeout : 0

✓ **Radius Server Settings :**

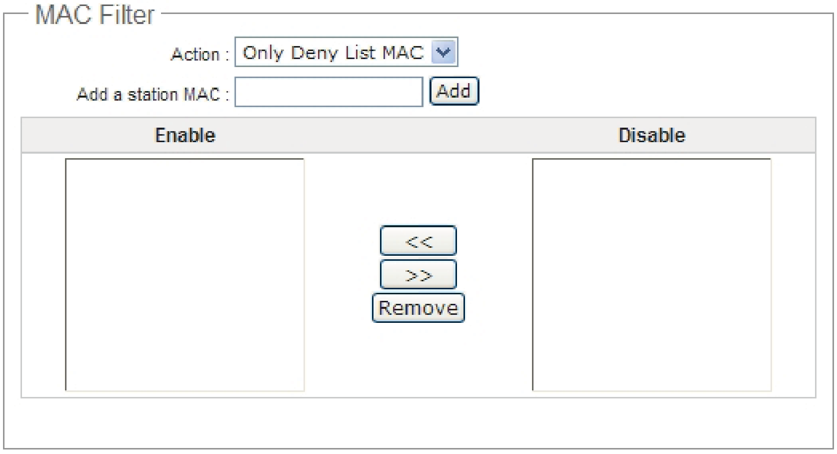
- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60** *seconds*. The default is **0** to disable re-authenticate service.

  Amount of time before a client will be required to re-authenticate.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Wireless MAC Filter Setup

Continue **Virtual AP Setup** section. For each Virtual AP setting, the administrator can allow or reject clients to access each Virtual AP.



MAC Filter

Action : Only Deny List MAC

Add a station MAC :

- **MAC Filter Setup :** By default, it's "***Disable***". Options are **Disable, Only Deny List MAC or Only Allow List MAC**.

  Two ways to set MAC filter rules :

  ➔ **Only Allow List MAC**.

  The wireless clients in the "**Enable**" list will be **allowed** to access the Access Point; All others or clients in the "**Disable**" list will be **denied**.

  ➔ **Only Deny List MAC**.

  The wireless clients in the "**Enable**" list will be **denied** to access the Access Point; All others or clients in the "**Disable**" list will be **allowed**.

- **Add a station MAC :** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the "**Enable**" List.

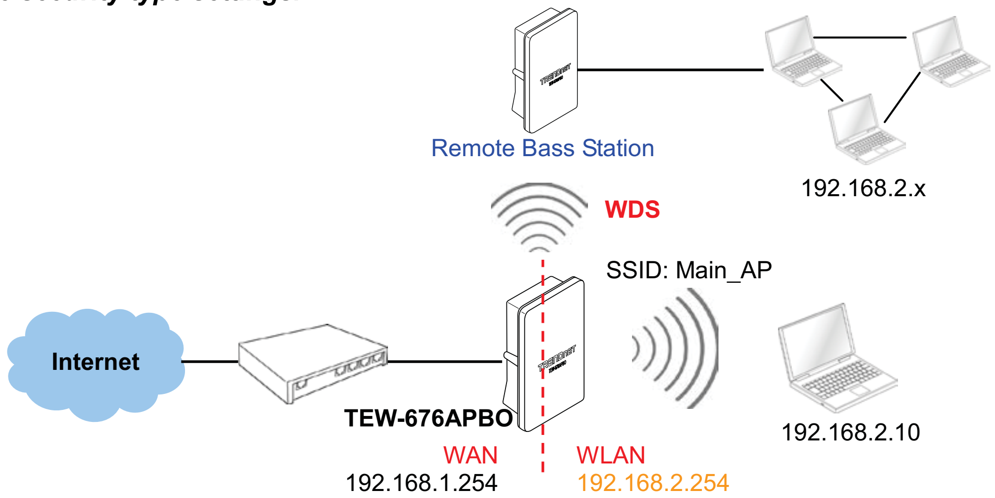
There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons**.**

Click ***Reboot*** button to activate your changes

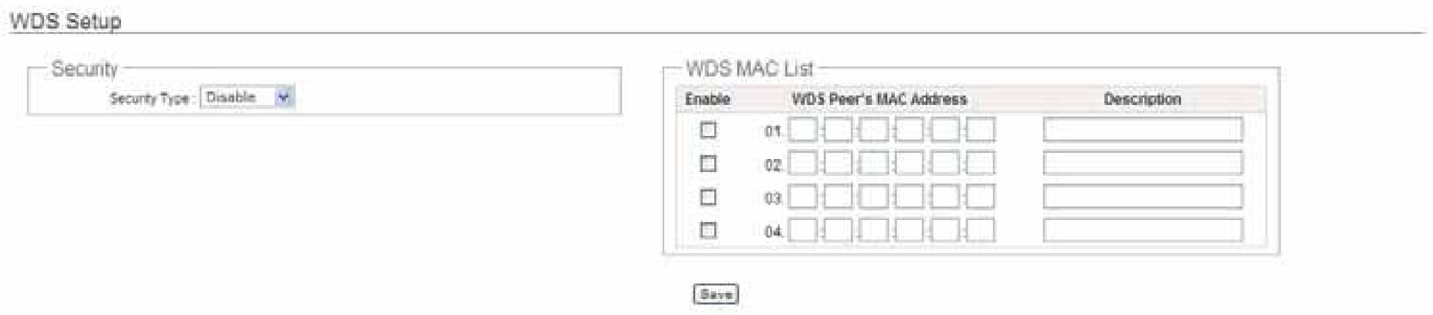
MAC Access Control is the weakest security approach. WPA and WPA2 security method is highly recommended.

Wireless Network Expansion

The administrator could create WDS Links to expand wireless network. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. ***A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.***



Please click on **Wireless -> WDS Setup** and follow the below setting.



WDS Setup

Security

Security Type : Disable

WDS MAC List

Enable		WDS Peer's MAC Address	Description
□	01		
□	02		
□	03		
□	04		

- **Security Type :** Option is "**Disable**", "**WEP**", "**TKIP**"or "**AES**" from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.
  - ➔ **WEP Key :** Enter **5 / 13 ASCII** or **10 / 26 HEX** format WEP key.
  - ➔ **TKIP Key :** Enter **8** to **63 ASCII** or **64 HEX** format TKIP key.
  - ➔ **AES Key :** Enter **8** to **63 ASCII** or **64 HEX** format AES key.
- **WDS MAC List**
  - ➔ **Enable :** Click ***Enable*** to create WDS link.
  - ➔ **WDS Peer's MAC Address :** Enter the MAC address of WDS peer.
  - ➔ **Description :** Description of WDS link.

> *The WDS link needs to be set at same **Channel** and with same **Security Type**.*

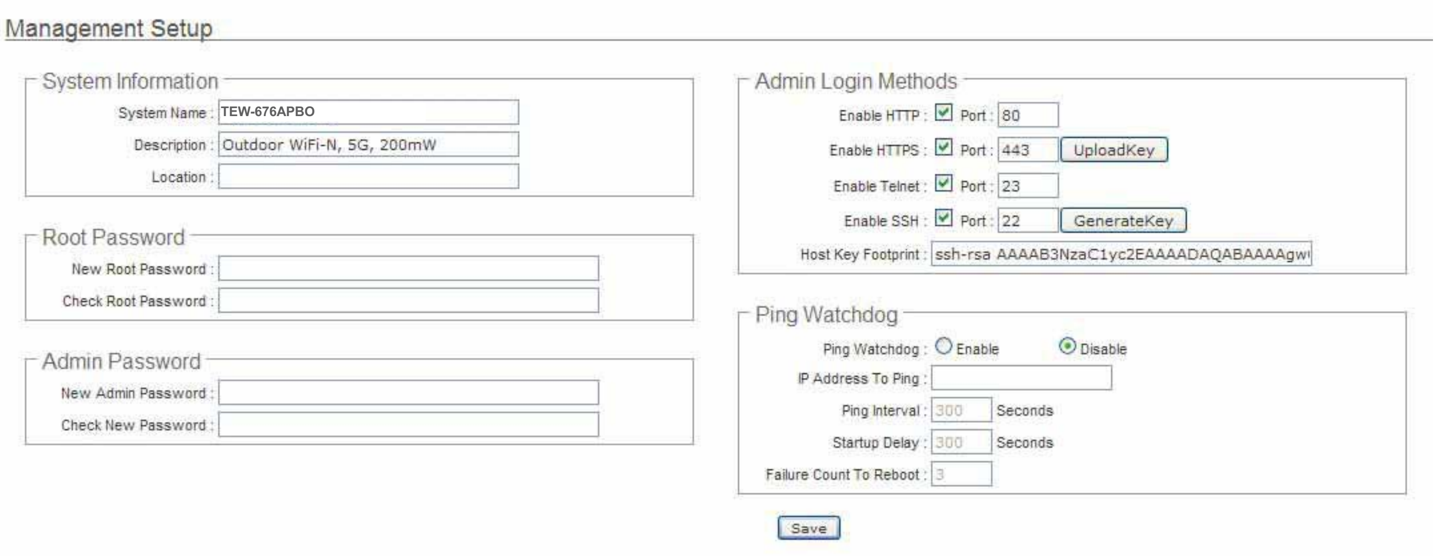
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

System Management

Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.



Management Setup

System Information
System Name : TEW-676APBO
Description : Outdoor WiFi-N, 5G, 200mW
Location :

Root Password
New Root Password :
Check Root Password :

Admin Password
New Admin Password :
Check New Password :

Admin Login Methods
Enable HTTP : ☑ Port : 80
Enable HTTPS : ☑ Port : 443 UploadKey
Enable Telnet : ☑ Port : 23
Enable SSH : ☑ Port : 22 GenerateKey
Host Key Footprint : ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgw

Ping Watchdog
Ping Watchdog : ○ Enable ● Disable
IP Address To Ping :
Ping Interval : 300 Seconds
Startup Delay : 300 Seconds
Failure Count To Reboot : 3

Save

- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default one.
  - ➔ **Description :** Provide description of the system.
  - ➔ **Location :** Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to ***Appendix D. Network manager Privileges***.

- **Root Password :** Log in as a root user and is allowed to change its own, plus admin user's password.
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Password :** Log in as a admin user and is allowed to change its own,
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Login Methods :** Only **root** user can enable or disable system login methods and change services port.

➔ **Enable HTTP :** Check to select HTTP Service.

➔ **HTTP Port :** The default is 80 and the range is between 1 ~ 65535.

➔ **Enable HTTPS :** Check to select HTTPS Service

➔ **HTTPS Port :** The default is 443 and the range is between 1 ~ 65535.

*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

➔ **Enable Telnet :** Check to select Telnet Service

➔ **Telnet Port :** The default is 23 and the range is between 1 ~ 65535.

➔ **Enable SSH :** Check to select SSH Service

➔ **SSH Port :** Please The default is 22 and the range is between 1 ~ 65535.

*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

■ **Ping Watchdog :** The ping watchdog sets the WCB1200H2PX 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 WCB1200H2PX 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 :** specify an IP address of the target host which will be monitored by Ping Watchdog Tool.

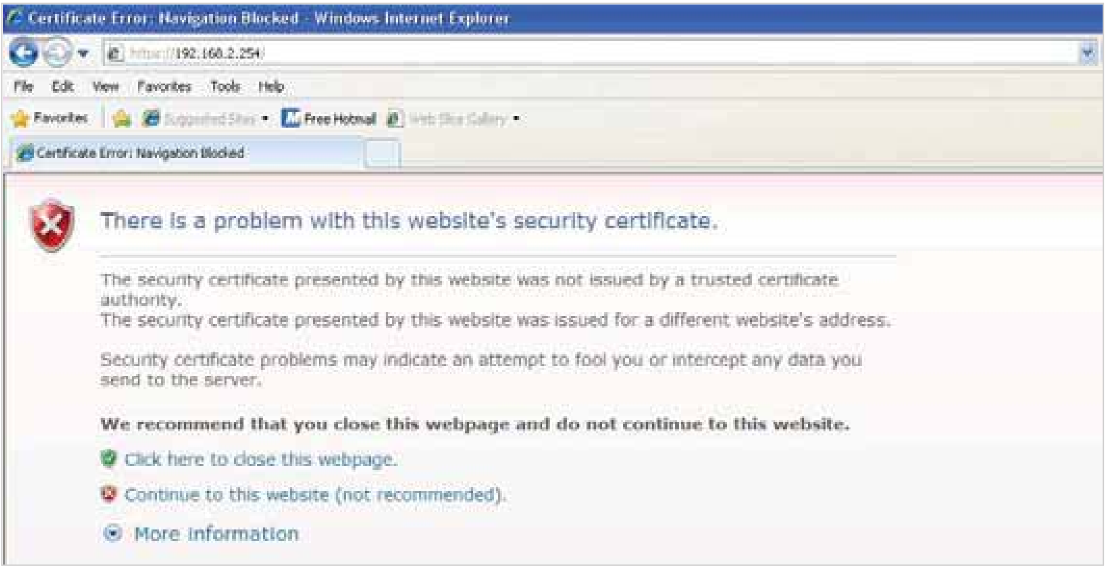
➔ **Ping Interval :** specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. Default is **300** seconds.

➔ **Startup Delay :** specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** 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.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (https://192.168.2.254). There will be a “Certificate Error”, because the browser treats system as an illegal website.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

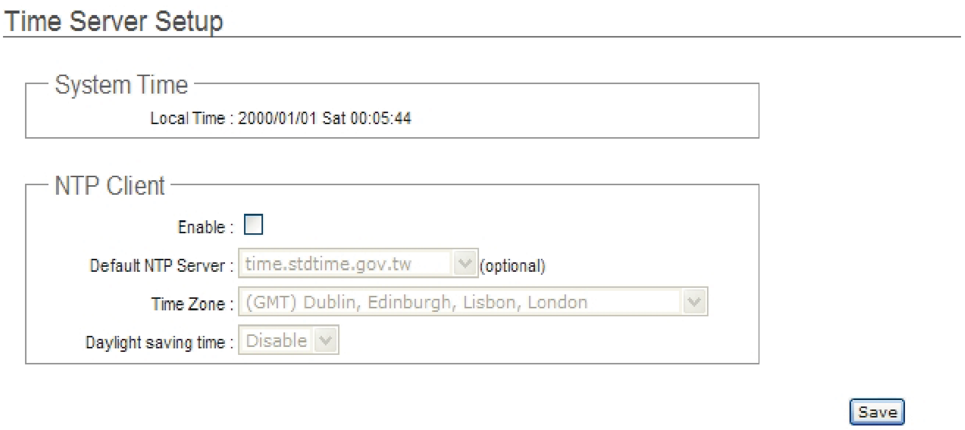
More information

Click “***Continue to this website***” to access the system's WMI. The system's Overview page will appear.

Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.



Time Server Setup

System Time

Local Time : 2000/01/01 Sat 00:05:44

NTP Client

Enable : □

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight saving time : Disable

- **Local Time :** Display the current system time.

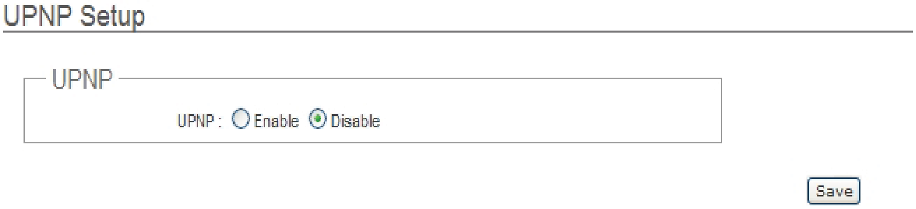
- **NTP Client :** To synchronize the system time with NTP server.
  - ➔ **Enable :** Check to select NTP client.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Select a desired time zone from the drop-down list.
  - ➔ **Daylight saving time :** Enable or disable Daylight saving.

If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.



UPNP Setup

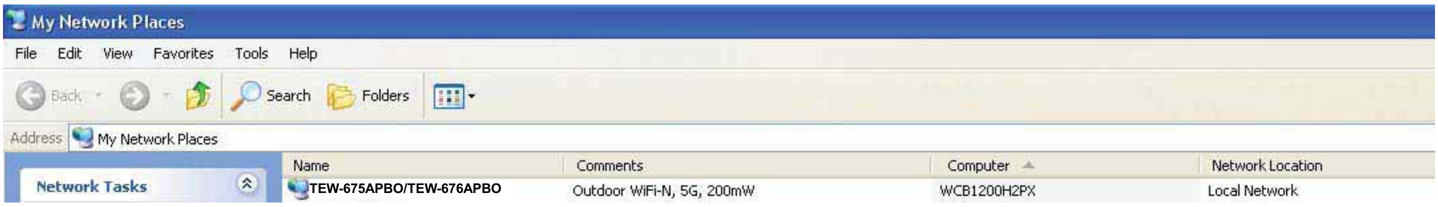
UPNP

UPNP : ○ Enable ● Disable

- **UPnP :** By default, it's "***Disable***". Select "**Enable**" or "***Disable"*** of UPnP Service.

Click ***Save*** button to save changes and click ***Reboot*** button to activate changes

For UPnP to work in Windows XP, the "TEW-676APBO" must be available in "***My Network Places***", as shown here: (your specific model may vary)



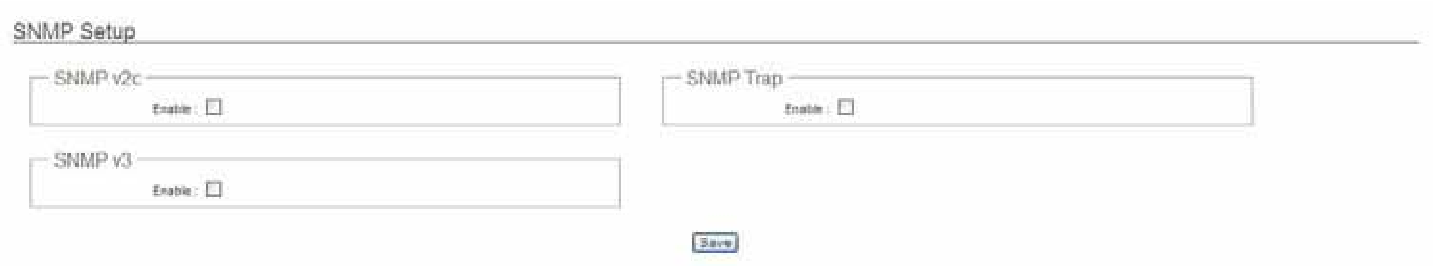
Name	Comments	Computer	Network Location
TEW-675APBO/TEW-676APBO	Outdoor WiFi-N, 5G, 200mW	WCB1200H2PX	Local Network

If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to ***Appendix E. Using UPnP on Windows XP***

Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.



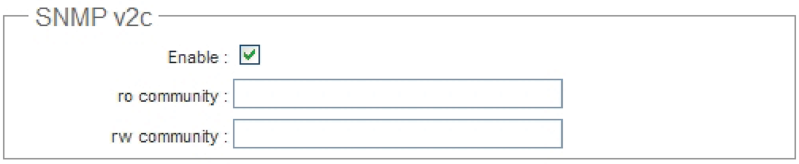
SNMP Setup

SNMP v2c
Enable : □

SNMP Trap
Enable : □

SNMP v3
Enable : □

- **SNMP v2c Enable:** Check to enable SNMP v2c.



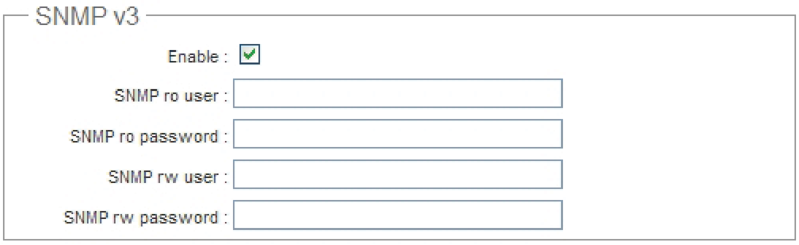
SNMP v2c
Enable : ☑
ro community :
rw community :

➔ **ro community :** Set a community string to authorize read-only access.

➔ **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

SNMPv3 supports the highest level SNMP security.



SNMP v3
Enable : ☑
SNMP ro user :
SNMP ro password :
SNMP rw user :
SNMP rw password :

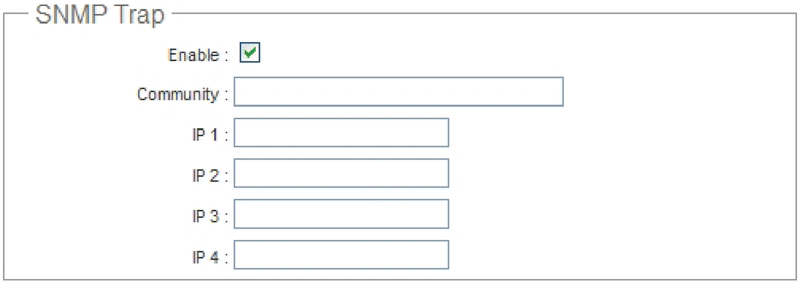
➔ **SNMP ro user :** Set a community string to authorize read-only access.

➔ **SNMP ro password :** Set a password to authorize read-only access.

➔ **SNMP rw user :** Set a community string to authorize read/write access.

➔ **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.



SNMP Trap

Enable : ☑

Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

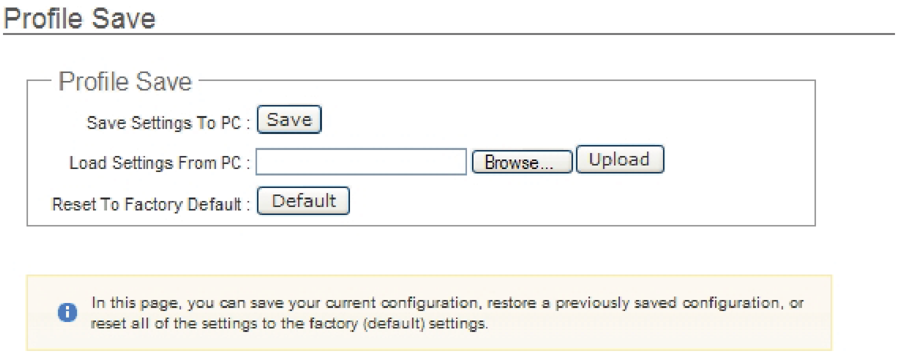
- ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

Click ***Save*** button to save changes and click ***Reboot*** button to activate.

Backup / Restore and Reset to Factory

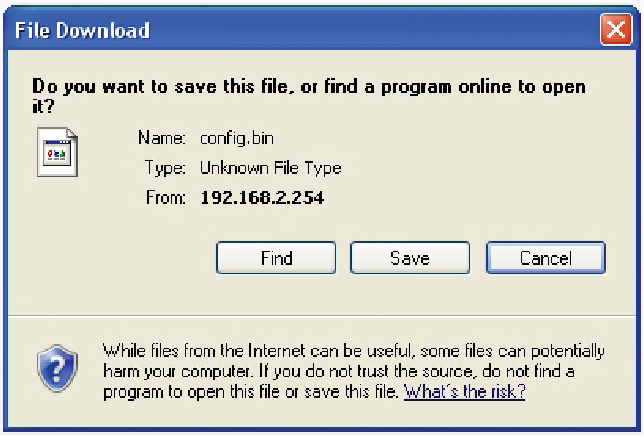
Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.



In this page, you can save your current configuration, restore a previously saved configuration, or reset all of the settings to the factory (default) settings.

- **Save Settings to PC :** Click ***Save*** button to save the current configuration to a local disk.



Do you want to save this file, or find a program online to open it?

Name: config.bin
Type: Unknown File Type
From: 192.168.2.254

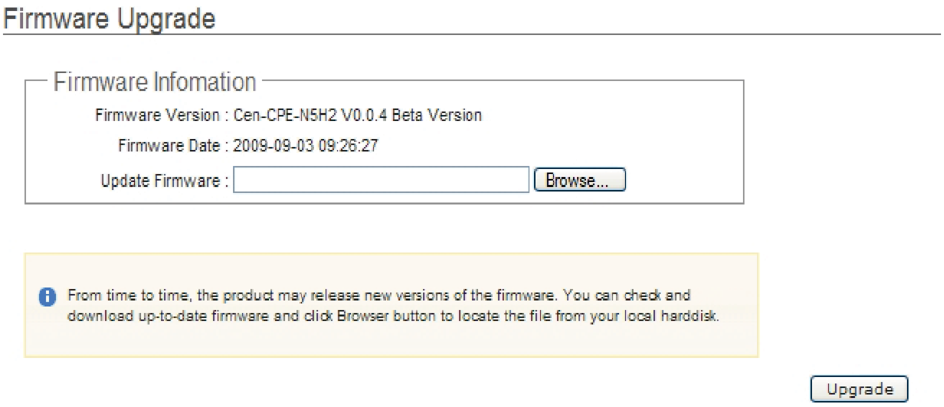
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click ***Browse*** button to locate the new firmware, and then click ***Upgrade*** button to upgrade.



Firmware Upgrade

Firmware Infomation

Firmware Version : Cen-CPE-N5H2 V0.0.4 Beta Version

Firmware Date : 2009-09-03 09:26:27

Update Firmware :

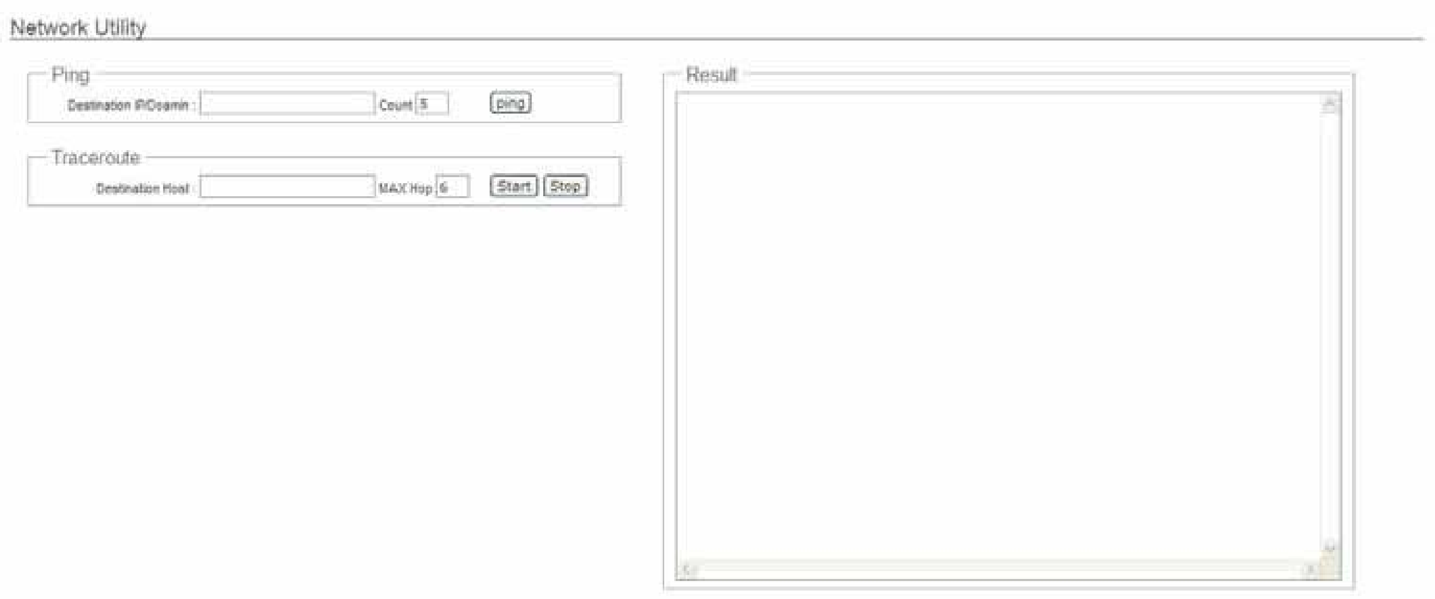
From time to time, the product may release new versions of the firmware. You can check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.

1. *To prevent data loss during firmware upgrade, please back up current settings before proceeding.*
2. *Do not interrupt during firmware upgrade including power on/off as this may damage system.*
3. *Never perform firmware upgrade over wireless connection or via remote access connection.*

Network Utility

The administrator can diagnose network connectivity via the PING and TRACEROUTE utility.

Please click on **Utilities -> Network Utility** and follow the below setting



Destination IP/Domain :

Count 5

Destination Host :

MAX Hop 6

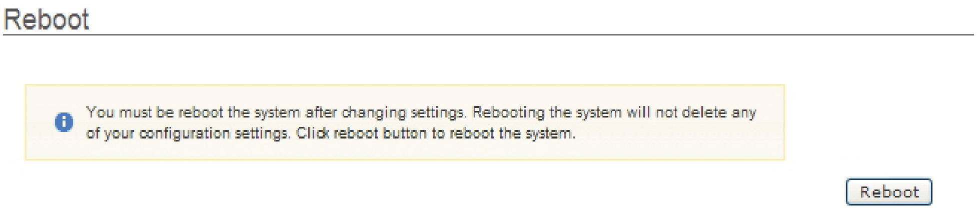
- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - ➔ **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - ➔ **Count :** By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

- **Traceroute :** Allows tracing the hops from the TEW-676APBO device to a selected outgoing IP

  address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click Stop button to stopped test
  - ➔ **Destination Host :** Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
  - ➔ **MAX Hop :** Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

Reboot

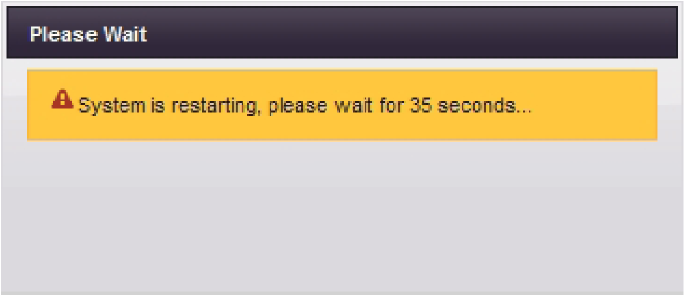
This function allows user to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.



Reboot

You must be reboot the system after changing settings. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



Please Wait

System is restarting, please wait for 35 seconds...

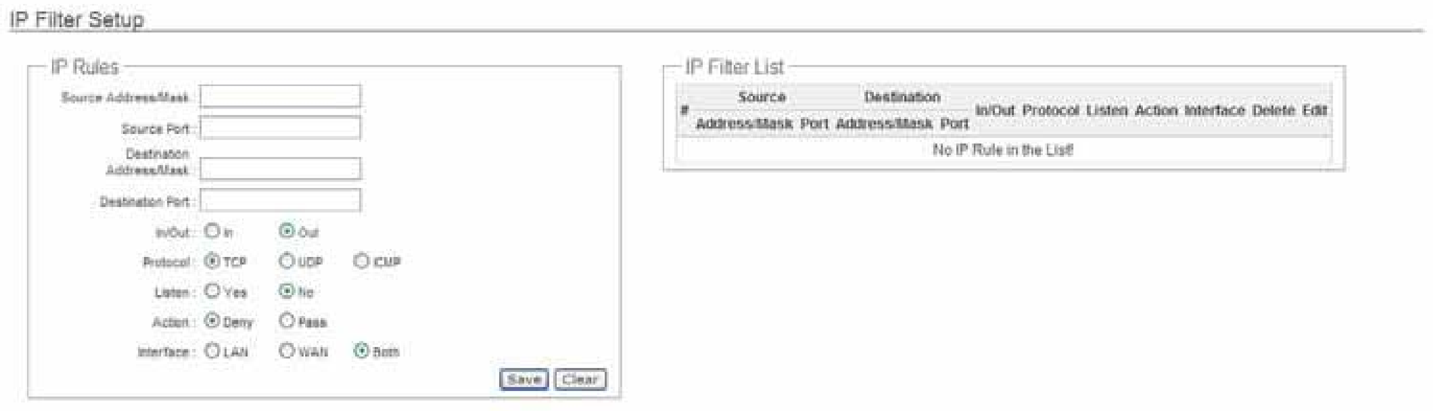
The **System Overview** page appears upon the completion of reboot.

Access Control List

IP Filter Setup

Allows to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules.

Please click on **Advance -> IP Filter Setup** and follow the below setting.



IP Filter Setup

IP Rules

Source Address/Mask :

Source Port :

Destination Address/Mask :

Destination Port :

In/Out : ○ In ● Out

Protocol : ● TCP ○ UDP ○ CMP

Listen : ○ Yes ● No

Action : ● Deny ○ Pass

Interface : ○ LAN ○ WAN ● Both

IP Filter List

#	Source Address/Mask	Source Port	Destination Address/Mask	Destination Port	In/Out	Protocol	Listen	Action	Interface	Delete	Edit
No IP Rule in the List!											

- **Source Address/Mask :** Enter desired source IP address and netmask; i.e. 192.168.2.10/32.

- **Source Port :** Enter a port or a range of ports as ***start:end***; i.e. port 20:80
- **Destination Address/Mask :** Enter desired destination IP address and netmask; i.e. 192.168.1.10/32
- **Destination Port :** Enter a port or a range of ports as ***start:end***; i.e. port 20:80
- **In/Out :** Applies to Ingress or egress packets
- **Protocol :** Supports ***TCP***, ***UDP*** or ***ICMP***.
- **Listen :** Click ***Yes*** radial button to match TCP packets only with the SYN flag.
- **Active :** ***Deny*** to drop and ***Pass*** to allow per filter rules
- **Interface :** The interface that a filter rule applies

> All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

Click "**Save**" button to add IP filter rule. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. Click ***Reboot*** button to activate your changes.

When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

➔ **Example 1 :** Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN

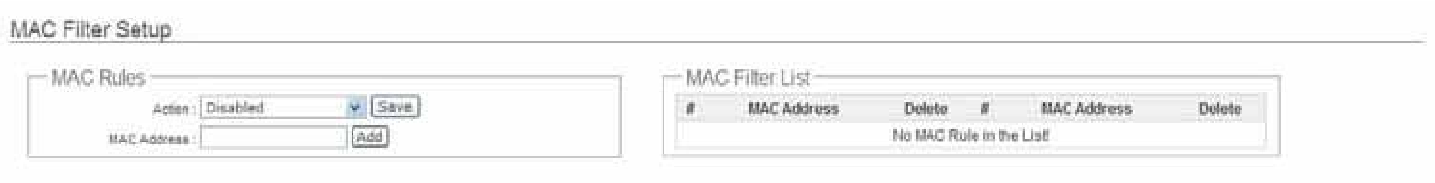
➔ **Example 2 :** All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN
2	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	pass	LAN

MAC Filter Setup

Allows to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important to note that MAC filter rules have precedence over IP Filter rules.

Please click on **Advance -> MAC Filter Setup** and follow the below setting.



Action : Disabled

MAC Address :

#	MAC Address	Delete	#	MAC Address	Delete
No MAC Rule in the List!					

- **MAC Filter Rule :** By default, it's "***Disable***". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**. Click ***Save*** button to save your change.

  Two ways to set the MAC Filter List:

  ➔ **Only Allow List MAC**.

  The wireless clients in the MAC Filter List will be **allowed** to access to Access Point; All others will be denied.

  ➔ **Only Deny List MAC**.

  The wireless clients in the MAC Filter List will be **denied** to access to Access Point; All others will be allowed.

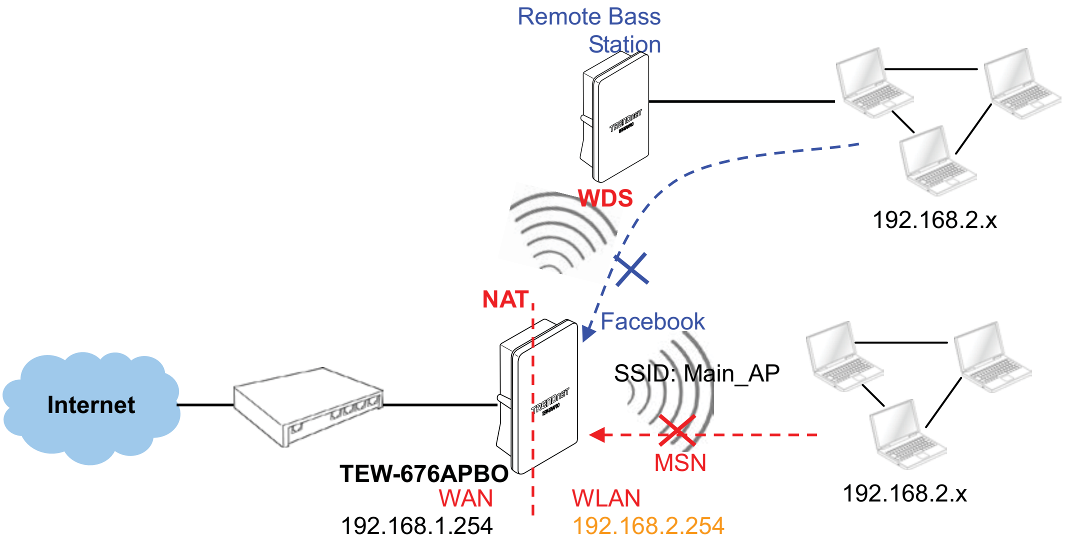
- **MAC Address :** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.

There are a maximum of **20** clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Delete** buttons***.***

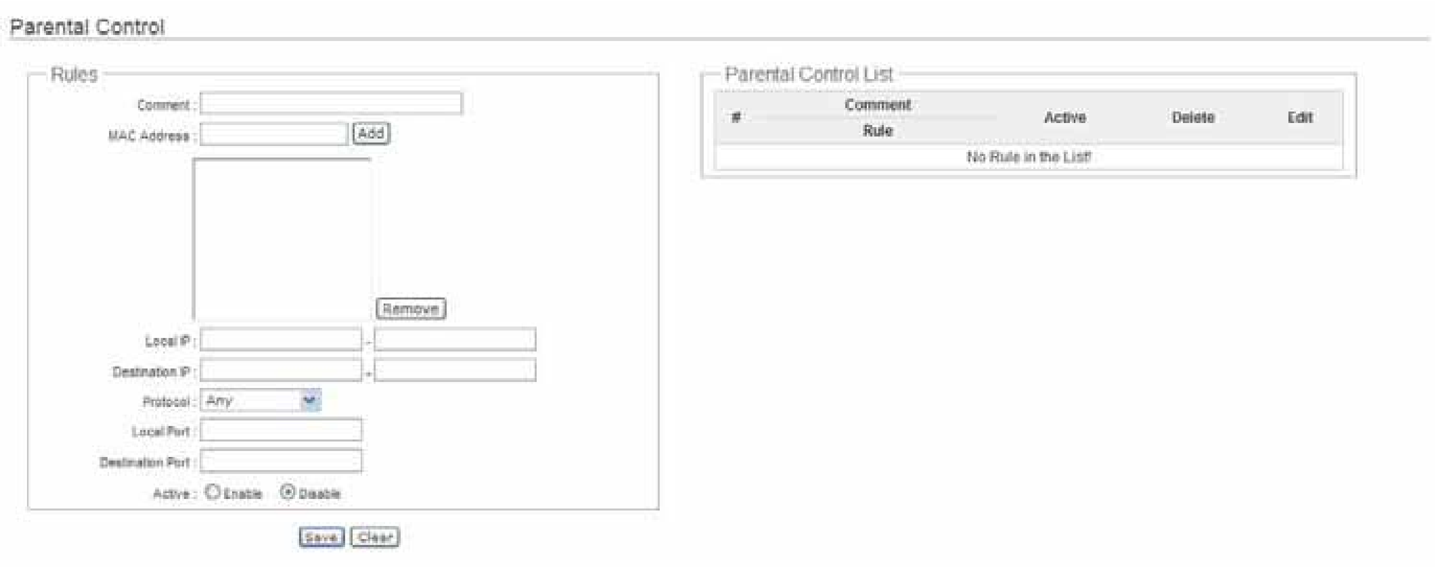
Click ***Reboot*** button to activate your changes

Parental Control Setup

Parental Control allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites.



Please click on **Advance -> Parental Control** and follow the below setting.


Parental Control

Rules

Comment :

MAC Address : Add

Remove

Local IP : -

Destination IP : -

Protocol : Any

Local Port :

Destination Port :

Active : ○ Enable ● Disable

Save Clear

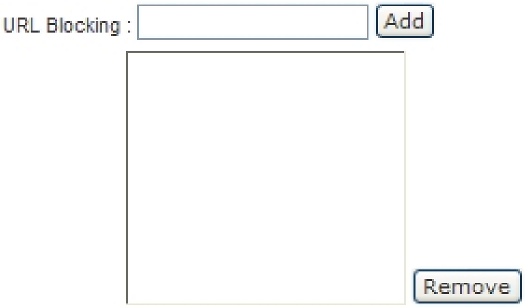
Parental Control List

#	Comment Rule	Active	Delete	Edit
No Rule in the List!				

- **Rules :** control can be managed by a rule. Use the settings on this screen to establish an access policy.
  - ➔ **Comment :** Enter a descriptive name for this rule for identifying purposes.
  - ➔ **MAC Address :** Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click "**Add**" button to add in the MAC group of each rule. Click "**Remove**" button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
  - ➔ **Local / Destination IP :** Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.

- **Protocol :** Select **Any** or specify protocol(**TCP**, **UDP**, **ICMP**, **URL Blocking** and **Application**) from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Local(LAN)/ Destination Port can not used.

  If you want to block websites with specific URL address or using specific keywords, enter each URL or keyworks in the "**URL Blocking**" field and click "**Add**" button to add in the URL Blocking list of each rule. Click "**Remove**" button can remove URL or keywords.



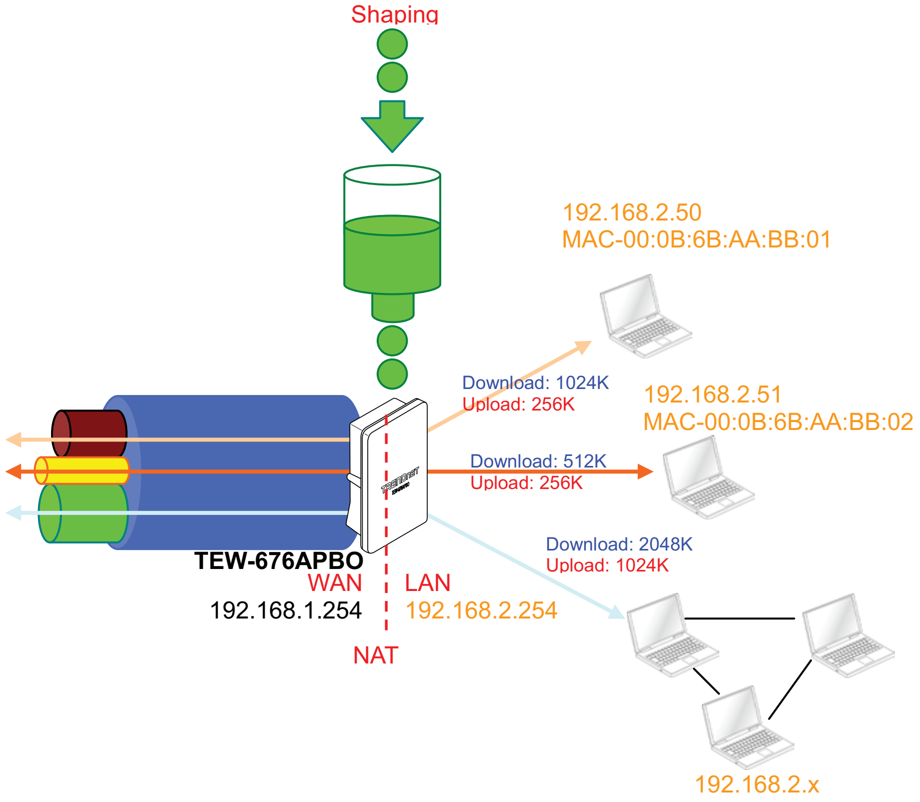
- **Local Port :** Specify local port(LAN port) range required for this rule
- **Destination Port :** Specify destination port range required for this rule
- **Active :** Check ***Enable*** button to activate this rule, and ***Disable*** to deactivate.

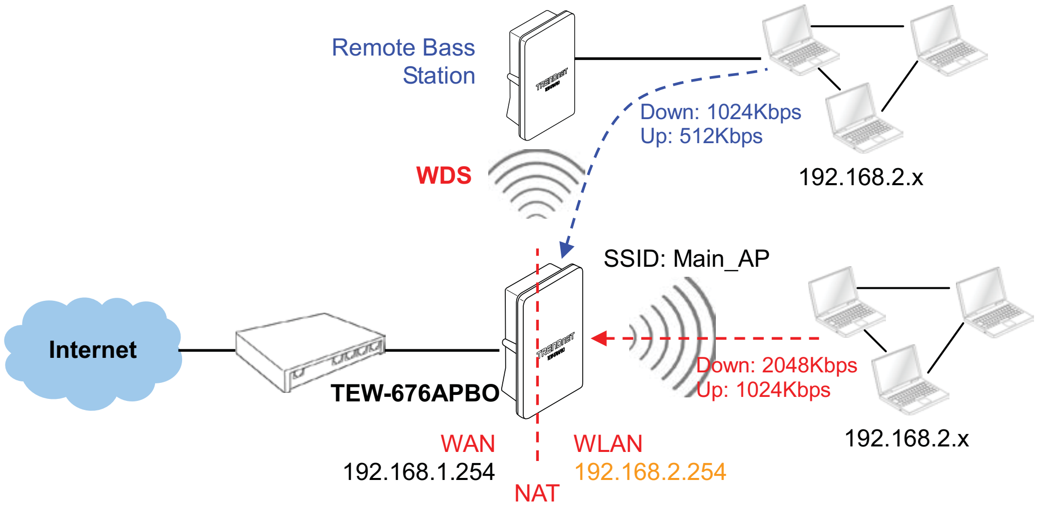
Click "**Add**" button to add control rule to List. There are **10** rules maximum allowed in this Control List. All rules can be removed or edited on the List. Click ***Reboot*** button to activate your changes.

QoS Setup

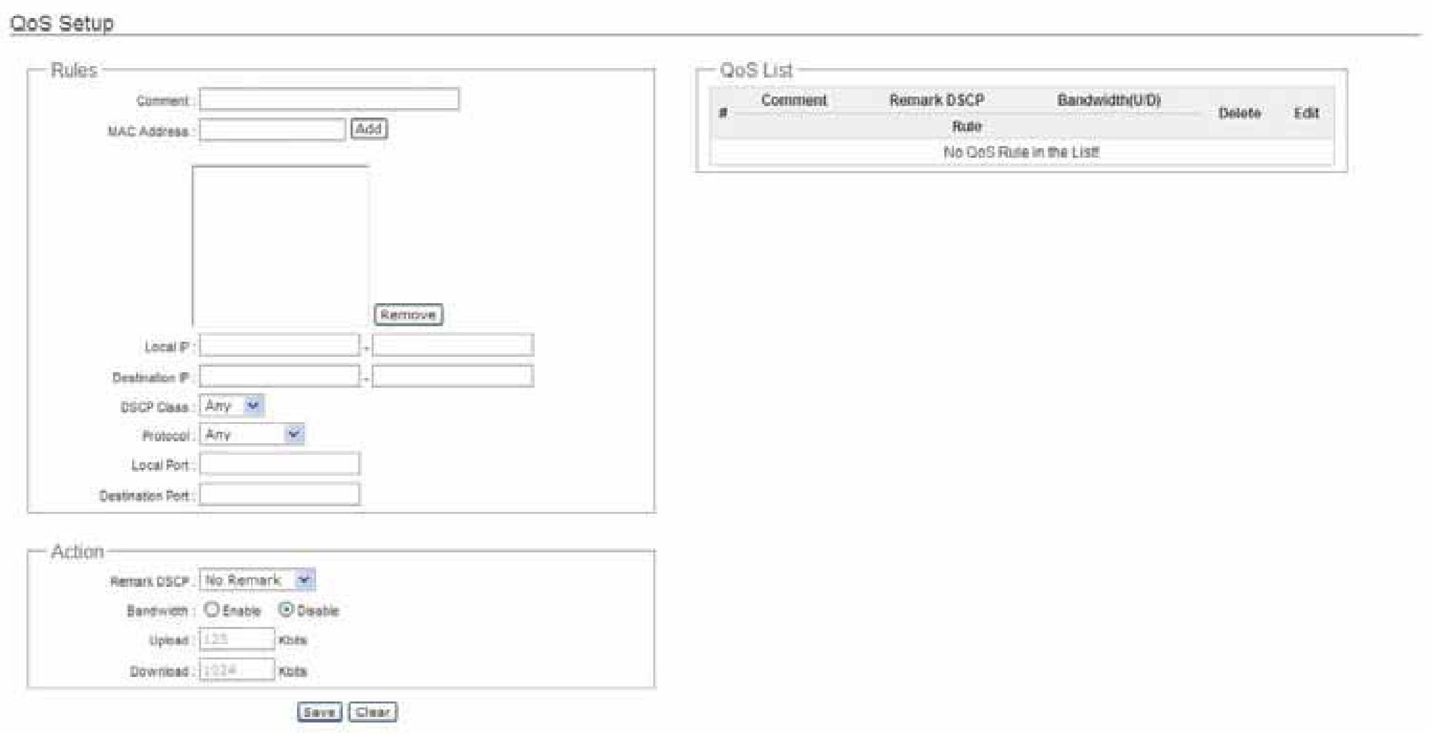
Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as FTP) to form a flow.





Please click on **Advance -> QoS** and follow the below setting.



Comment :

MAC Address :

Local IP : -

Destination IP : -

DSCP Class : Any

Protocol : Any

Local Port :

Destination Port :

Remark DSCP : No Remark

Bandwidth : ○ Enable ● Disable

Upload : 128 Kbits

Download : 1024 Kbits

#	Comment	Remark DSCP	Bandwidth(U/D)	Delete	Edit
	Rule				
	No QoS Rule in the List!				

- **Rules :** Use the rules to define the classifiers. After you define the rules, you can specify action to act upon the traffic that matches the rules
  - ➔ **Comment :** Enter a descriptive name for this rule for identifying purposes.
  - ➔ **MAC Address :** Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click "**Add**" button to add in the MAC group of each rule. Click "**Remove**" button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
  - ➔ **Local / Destination IP :** Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.
  - ➔ **DSCP Class** : Differentiated services code point, DSCP. Select Any or specify classify traffic from drop-down list.

    The Per-Hop Behavior (PHB) is indicated by encoding a 6-bit value—called the Differentiated Services Code Point (DSCP)—into the 8-bit Differentiated Services (DS) field of the IP packet header. Below depicts class for DSCP.
    - ✓ **BE :** *Default* PHB, which is typically best-effort traffic
    - ✓ **EF :** *Expedited Forwarding* PHB, dedicated to low-loss, low-latency traffic
    - ✓ **AF :** *Assured Forwarding* PHB, which gives assurance of delivery under conditions. The AF behavior group defines four separate AF classes. Within each class, packets are given a drop precedence (high, medium or low). The combination of classes and drop precedence yields twelve separate DSCP encodings from **AF11** through **AF43** (see table)

DROP Precedence	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11	AF21	AF31	AF41
Medium Drop	AF12	AF22	AF32	AF42
High Drop	AF13	AF23	AF33	AF43

- ➔ **Protocol :** Select **Any** or specify protocol from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Source/ Destination Port can not used.
- ➔ **Local Port :** Specify local port(LAN port) range required for this rule
- ➔ **Destination Port :** Specify destination port range required for this rule

- ■ **Action :** After configuring rule, a policy rule ensures that a traffic flow gets the requested treatment in the network.
  - ➔ **Remark DSCP :** Specify a new DSCP class, if you want to replace or remark the DSCP
  - ➔ **Bandwidth :** Click "**Enable**" to activate function, and click "**Disable**" to deactivate function
  - ➔ **Upload / Download :** Specify the bandwidth in kilobit per second (Kbps). Enter a number between **8** to **8192**, default upload is **128** Kbps, download is **1024** Kbps.

Click "**Add**" button to add QoS rule to List. There are **10** rules maximum allowed in this QoS List. All rules can be removed or edited on the List. Click ***Reboot*** button to activate your changes.

When you create rules on the QoS List, the previous rules have higher priority. . Below depict the examples for explaining priority of QoS setup.

- ➢ **Example 1 :** On this setting, the FTP has **1024** Kbps upload and **8196** Kbps download on **192.168.2.10**. The remaining IP address and other remaining protocol of IP address 192.168.2.10 only can use total bandwidth **512** Kbps bandwidth. Because rule 1's priority is higher than rule 2

Rule	Source IP	Destination IP	DSCP	Protocol	Remark DSCP	Bandwidth (Up/Down)
1	192.168.2.10		ANY	FTP	NO	1024/8196
2			ANY	ANY	NO	512/512

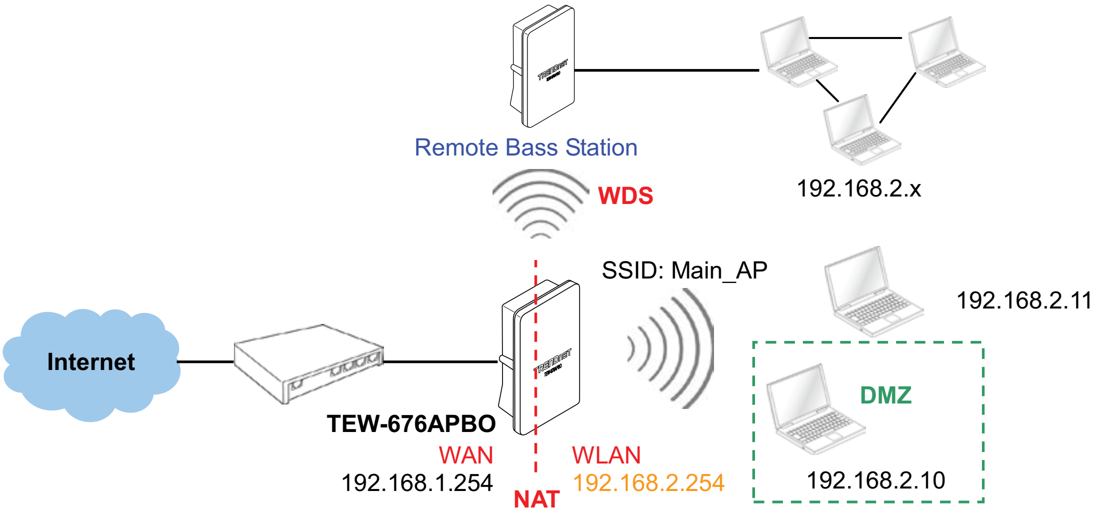
- ➢ **Example 2 :** On this setting, the FTP has **512** Kbps upload and **512** Kbps download on **192.168.2.10** Because rule 1's priority is higher than rule 2

Rule	Source IP	Destination IP	DSCP	Protocol	Remark DSCP	Bandwidth (Up/Down)
1			ANY	ANY	NO	512/512
2	192.168.2.10		ANY	FTP	NO	1024/8196

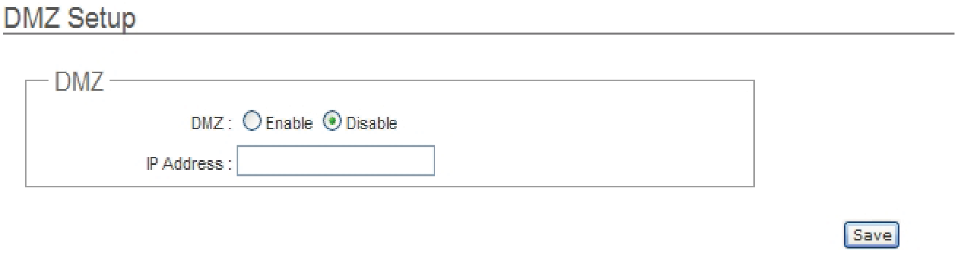
Resource Sharing

DMZ

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding*)* while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.



Please click on **Advance -> DMZ** and follow the below setting.



DMZ Setup

DMZ

DMZ : ○ Enable ● Disable

IP Address :

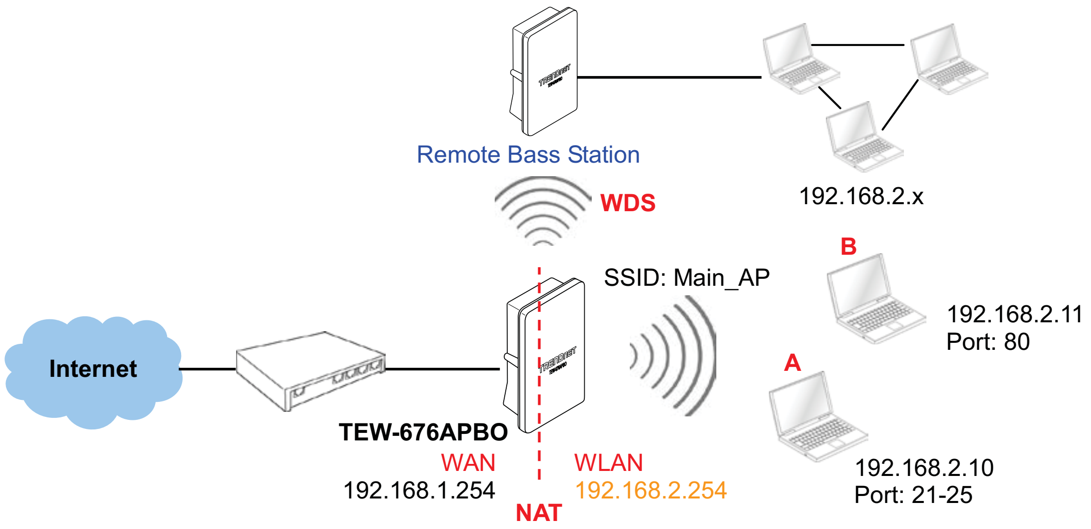
- **DMZ :** By default, it's *"**Disable**"*. Check ***Enable*** radial button to enable DMZ.
- **IP Address :** Enter IP address of DMZ host and only one DMZ host is supported.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

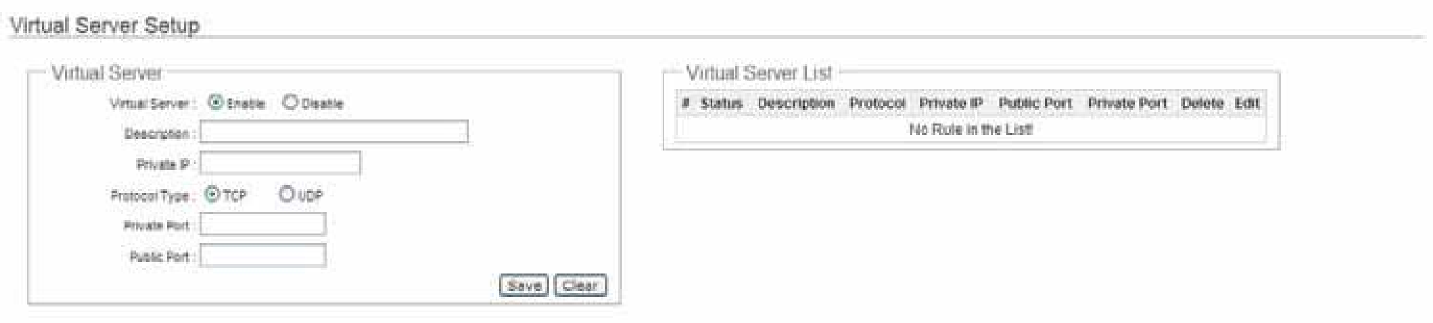
Virtual Server (Port Forwarding)

“Virtual Server” can also referred to as “Port Forward” as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don’t repeat ports’ usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.



Please click on **Advance -> Virtual Server** and follow the below setting.



Virtual Server Setup

Virtual Server

Virtual Server : ● Enable ○ Disable

Description :

Private IP :

Protocol Type : ● TCP ○ UDP

Private Port :

Public Port :

Save Clear

Virtual Server List

#	Status	Description	Protocol	Private IP	Public Port	Private Port	Delete	Edit
No Rule in the List!								

- **Virtual Server :** By Default, It’s “***Disable***”***.*** Check ***Enable*** radial button to enable Virtual Server.
- **Description :** Enter appropriate message for resource sharing via Virtual Server.
- **Private IP :** Enter corresponding IP address of internal resource to share.
- **Protocol Type :** Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.
- **Private Port :** A port or a range of ports may be specified as ***start:end***; i.e. port 20:80
- **Public Port :** A port or a range of ports may be specified as ***start:end***; i.e. port 20:80

.

The Private Port and Public Port can be different. However, total number of ports need to be the same.
Example : Public Port is 11 to 20 and the Private Port can be a 10 ports range.

Click “**Add**” button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List. Click ***Reboot*** button to activate your changes.

While creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ one while both rules exist. Example 1 and 2 demonstrate proper usage of DMZ and Virtual Server rules.

- **Example 1 :** All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all connections to TCP port 22 will be directed to TCP port 22 of 192.168.2.10 and remaining connections to port TCP ***20~80*** will be redirected to port TCP ***20~80*** of ***192.168.2.11***

DMZ Enabled : 192.168.2.12

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.10	22	22
2	TCP	192.168.2.11	20:80	20:80

- **Example 2 :** All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all other connections to TCP port ***20~80*** will be redirected to port ***20~80*** of ***192.168.2.11***. The rule 2 won’t take effect.

DMZ Enabled : 192.168.2.12

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.11	20:80	20:80
2	TCP	192.168.2.10	22	22

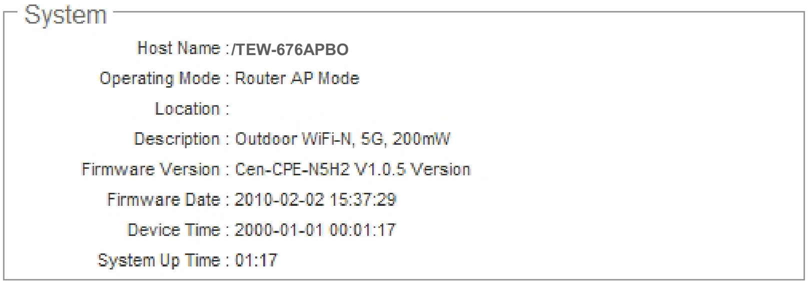
System Status

This section breaks down into subsections of ***System Overview***, ***Associated Clients Status***, ***WDS Link Status***, ***Extra Information*** and ***Event Log***.

Overview

Detailed information on **System**, **WAN Information**, **LAN Information**, **Wireless Information** and **DHCP Server Status** can be reviewed via this page.

- **System :** Display the information of the system.

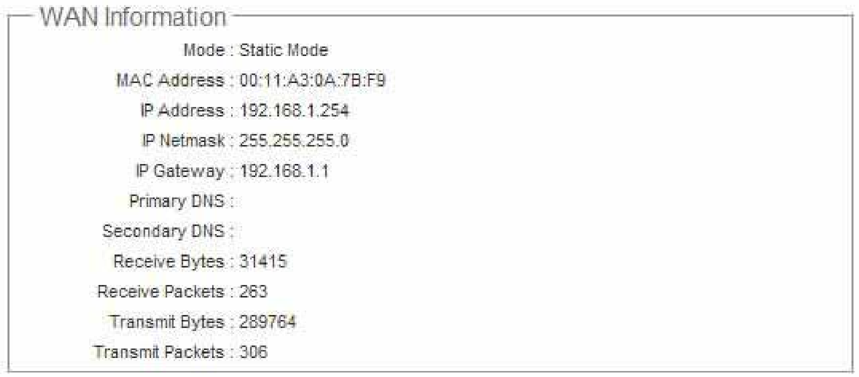


System

Host Name : /TEW-676APBO
Operating Mode : Router AP Mode
Location :
Description : Outdoor WiFi-N, 5G, 200mW
Firmware Version : Cen-CPE-N5H2 V1.0.5 Version
Firmware Date : 2010-02-02 15:37:29
Device Time : 2000-01-01 00:01:17
System Up Time : 01:17

- **System Name :** The name of the system.
- **Operating Mode :** The mode currently in service.
- **Location :** The reminding note on the geographical location of the system.
- **Description :** The reminding note of the system.
- **Firmware Version :** The current firmware version installed.
- **Firmware Date :** The build time of the firmware installed.
- **Device Time :** The current time of the system.
- **System Up Time :** The time period that system has been in service since last reboot.

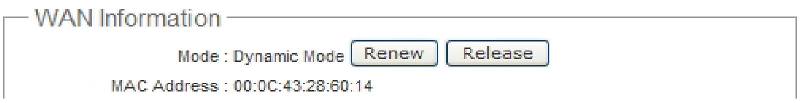
- **WAN Information :** Display the information of the WAN interface.



WAN Information

Mode : Static Mode
MAC Address : 00:11:A3:0A:7B:F9
IP Address : 192.168.1.254
IP Netmask : 255.255.255.0
IP Gateway : 192.168.1.1
Primary DNS :
Secondary DNS :
Receive Bytes : 31415
Receive Packets : 263
Transmit Bytes : 289764
Transmit Packets : 306

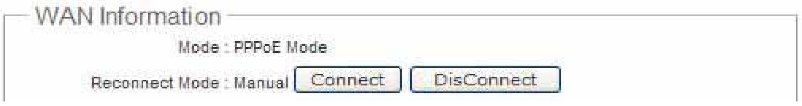
The WAN port specified **Dynamic IP**, the Release and Renew button will be show-up, click **Release** button to release IP address of WAN port, **Renew** button to renew IP address through DHCP server.


WAN Information

Mode : Dynamic Mode

MAC Address : 00:0C:43:28:60:14

The WAN port specified **PPPoE** or **PPTP**, and the **Connect** and **DisConnect** button will be show up. Click “**Connect**” button to assigned IP address from PPPoE or PPTP server, “**DisConnect**” button to release IP address of WAN port.

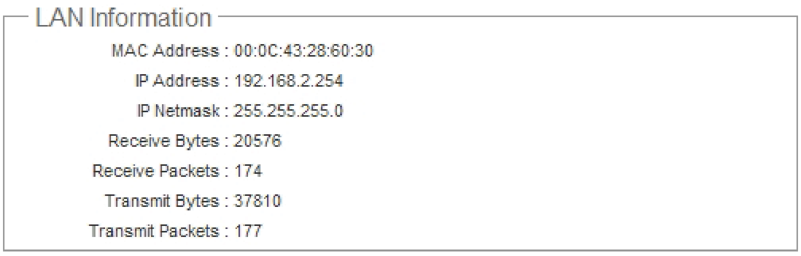

WAN Information

Mode : PPPoE Mode

Reconnect Mode : Manual

- ➔ **Mode :** Supports Static, Dynamic, PPPoE and PPTP modes.
- ➔ **Reconnect Mode :** The current reconnect mode of the PPPoE or PPTP.
- ➔ **MAC Address :** The MAC address of the WAN port.
- ➔ **IP Address :** The IP address of the WAN port.
- ➔ **IP Netmask :** The IP netmask of the WAN port.
- ➔ **IP Gateway :** The gateway IP address of the WAN port.
- ➔ **Primary DNS :** The primary DNS server in service.
- ➔ **Secondary DNS :** The secondary DNS server in service.
- ➔ **Receive bytes :** The total received packets in bytes on the WAN port.
- ➔ **Receive packets :** The total received packets of the WAN port.
- ➔ **Transmit bytes :** The total transmitted packets in bytes of the WAN port.
- ➔ **Transmit packets :** The total transmitted packets of the WAN port.

- ■ **LAN Information :** Display total received and transmitted statistics on the LAN interface.


LAN Information

MAC Address : 00:0C:43:28:60:30

IP Address : 192.168.2.254

IP Netmask : 255.255.255.0

Receive Bytes : 20576

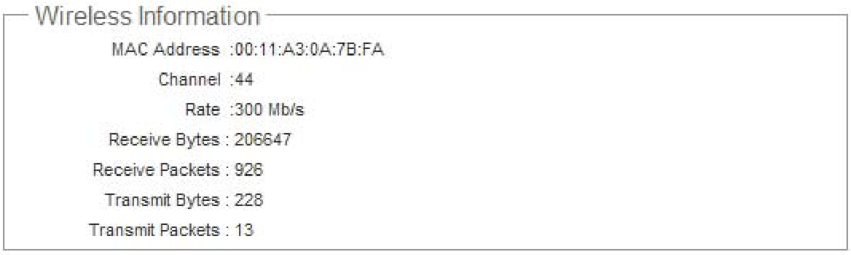
Receive Packets : 174

Transmit Bytes : 37810

Transmit Packets : 177

- ➔ **MAC Address :** The MAC address of the LAN port.
- ➔ **IP Address :** The IP address of the LAN port.
- ➔ **IP Netmask :** The IP netmask of the LAN port.
- ➔ **Receive bytes :** The total received packets in bytes on the LAN port.
- ➔ **Receive packets :** The total received packets of the LAN port.
- ➔ **Transmit bytes :** The total transmitted packets in bytes of the LAN port.
- ➔ **Transmit packets :** The total transmitted packets of the LAN port.

- **Wireless Information :** Display the detailed receive and transmit statistics of Wireless interface.

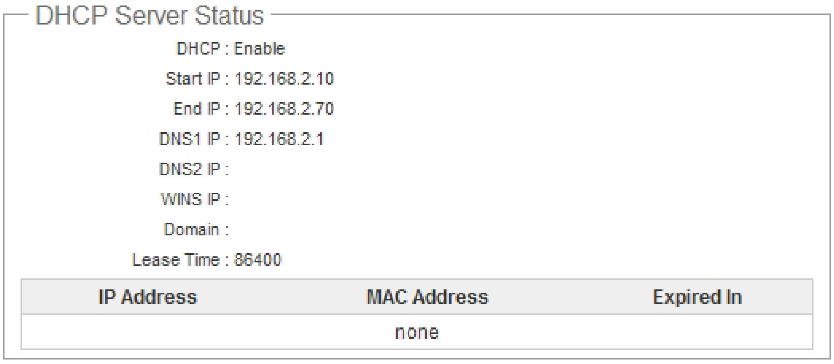


Wireless Information

MAC Address :00:11:A3:0A:7B:FA
Channel :44
Rate :300 Mb/s
Receive Bytes : 206647
Receive Packets : 926
Transmit Bytes : 228
Transmit Packets : 13

- ➔ **MAC Address :** The MAC address of the Wireless Port.
- ➔ **Channel :** The current channel on the Wireless port.
- ➔ **Rate :** The current Bit Rate on the Wireless port.
- ➔ **Receive bytes :**The total received packets in bytes on the Wireless port.
- ➔ **Receive packets :** The total received packets on the Wireless port.
- ➔ **Transmit bytes :** The total transmitted packets in bytes on the Wireless port.
- ➔ **Transmit packets :** The total transmitted packets on the Wireless port.

- **DHCP Server Status :** Users could retrieve DHCP server and DHCP clients' IP/MAC address via this field.



DHCP Server Status

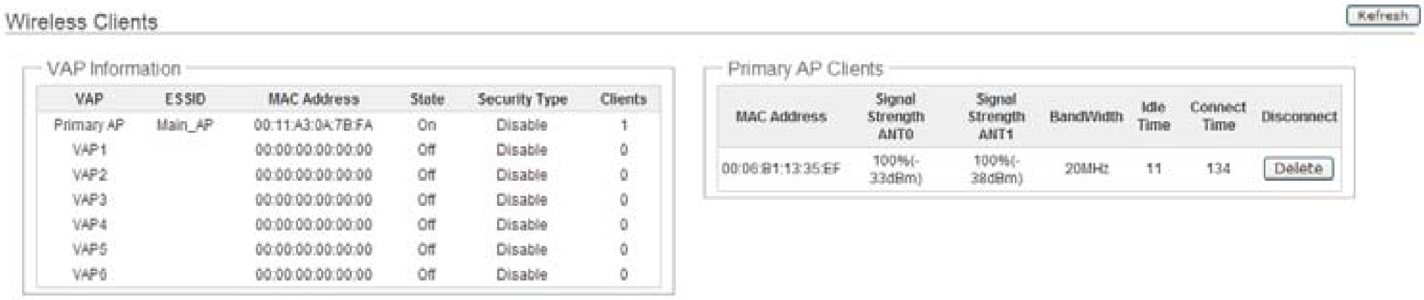
DHCP : Enable
Start IP : 192.168.2.10
End IP : 192.168.2.70
DNS1 IP : 192.168.2.1
DNS2 IP :
WINS IP :
Domain :
Lease Time : 86400

IP Address	MAC Address	Expired In
	none	

- ➔ **IP Address :** IP addresses to LAN devices by DHCP server.
- ➔ **MAC Address :** MAC addresses of LAN devices.
- ➔ **Expired In :** Shows how long the leased IP address will expire.

Associated Clients

It displays ESSID, on/off Status, Security Type, total number of wireless clients associated with all Virtual AP.



Wireless Clients

VAP Information

VAP	ESSID	MAC Address	State	Security Type	Clients
Primary AP	Main_AP	00:11:A3:0A:7B:FA	On	Disable	1
VAP1		00:00:00:00:00:00	Off	Disable	0
VAP2		00:00:00:00:00:00	Off	Disable	0
VAP3		00:00:00:00:00:00	Off	Disable	0
VAP4		00:00:00:00:00:00	Off	Disable	0
VAP5		00:00:00:00:00:00	Off	Disable	0
VAP6		00:00:00:00:00:00	Off	Disable	0

Primary AP Clients

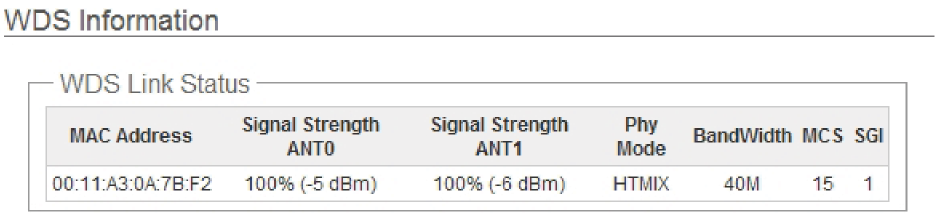
MAC Address	Signal Strength ANT0	Signal Strength ANT1	BandWidth	Idle Time	Connect Time	Disconnect
00:06:B1:13:35:EF	100%(-33dBm)	100%(-38dBm)	20MHz	11	134	Delete

- **VAP Information :** Highlights key VAP information.
  - ➔ **VAP :** Available VAP from Primary AP to VAP6.
  - ➔ **ESSID :** Display name of ESSID for each VAP.
  - ➔ **MAC Address :** Display MAC address for each VAP.
  - ➔ **Status :** On/Off
  - ➔ **Security Type :** Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
  - ➔ **Clients :** Display total number of wireless connections for each VAP.

- **VAP Clients :** Display all associated clients on each Virtual AP.
  - ➔ **MAC Address :** MAC address of associated clients
  - ➔ **Signal Strength ANT0/ANT1 :** Signal Strength of from associated clients.
  - ➔ **Bandwidth :** Channel bandwidth of from associated clients
  - ➔ **Idle Time :** Last inactive time period in seconds for a wireless connection.
  - ➔ **Connect Time :** Total connection time period in seconds for a wireless connection.
  - ➔ **Disconnect :** Click "**Delete**" button to manually disconnect a wireless client in a Virtual AP.

Show WDS Link

Peers MAC Address, antenna 0/1 received signal strength, phy mode and channel bandwidth for each WDS are available.



WDS Information

WDS Link Status

MAC Address	Signal Strength ANT0	Signal Strength ANT1	Phy Mode	BandWidth	MCS	SGI
00:11:A3:0A:7B:F2	100% (-5 dBm)	100% (-6 dBm)	HTMIX	40M	15	1

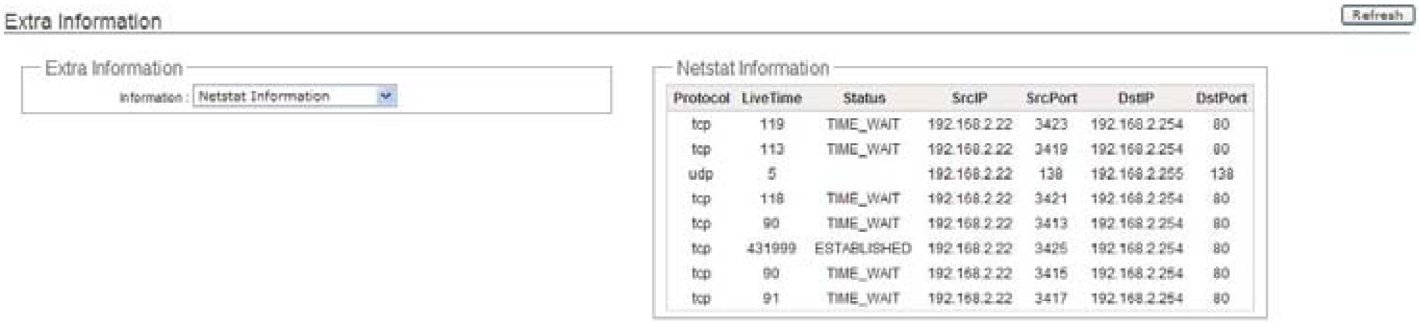
- **MAC Address :** Display MAC address of WDS peer.
- **Signal Strength ANT0/ANT1 :** Indicate the signal strength of the respective WDS links.
- **Phy Mode :** Indicate the phy mode of the respective WDS linked.

- **BandWidth :** Indicate the channel bandwidth of the respective WDS linked.
- **MCS :** Indicate the MCS of the respective WDS linked.
- **SGI :** Indicate the SGI (Short Guard Interval) of the respective WDS linked. “1” indicate the Short Guard Interval, “0” indicate the Long Guard Interval.

*If display “**no signal**” Signal Strength ANT0/ANT1, you need check WDS configuration. Things to verify are **MAC Address**, **Channel** and **Security type.** Also, adjust antenna angle and Tx Power.*

Extra Info

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.



Extra Information

Refresh

Extra Information

Information : Netstat Information

Netstat Information

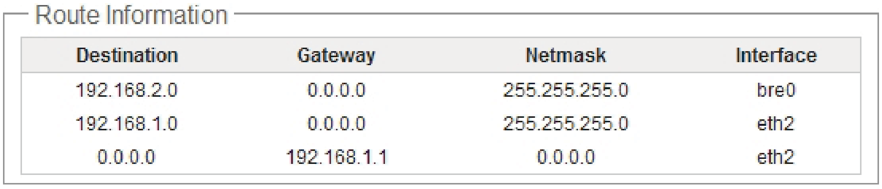
Protocol	LiveTime	Status	SrcIP	SrcPort	DstIP	DstPort
tcp	119	TIME_WAIT	192.168.2.22	3423	192.168.2.254	80
tcp	113	TIME_WAIT	192.168.2.22	3419	192.168.2.254	80
udp	5		192.168.2.22	138	192.168.2.255	138
tcp	118	TIME_WAIT	192.168.2.22	3421	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3413	192.168.2.254	80
tcp	431999	ESTABLISHED	192.168.2.22	3425	192.168.2.254	80
tcp	90	TIME_WAIT	192.168.2.22	3415	192.168.2.254	80
tcp	91	TIME_WAIT	192.168.2.22	3417	192.168.2.254	80

- **Netstat Information :** Select “**NetStatus Information**” on the drop-down list, the connection track list should show-up, the list can be updated using the Refresh button.

  NetStatus will show all connection track on the system, the information include *Protocol*, *Live Time*, *Status* , *Source/Destination IP address* and *Port*.

- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

  TEW-676APBO could be used as a L2 or L3 device. It doesn’t support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it’s capable of being a gateway to route packets inward and outward.

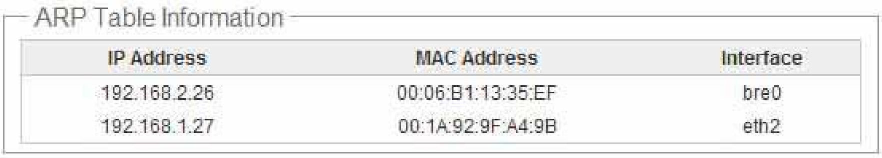


Route Information

Destination	Gateway	Netmask	Interface
192.168.2.0	0.0.0.0	255.255.255.0	bre0
192.168.1.0	0.0.0.0	255.255.255.0	eth2
0.0.0.0	192.168.1.1	0.0.0.0	eth2

- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

  ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

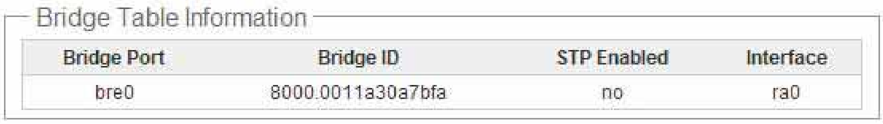


ARP Table Information

IP Address	MAC Address	Interface
192.168.2.26	00:06:B1:13:35:EF	bre0
192.168.1.27	00:1A:92:9F:A4:9B	eth2

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

  Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces e.g. ra0 ~ra6 and wds0~wds3).



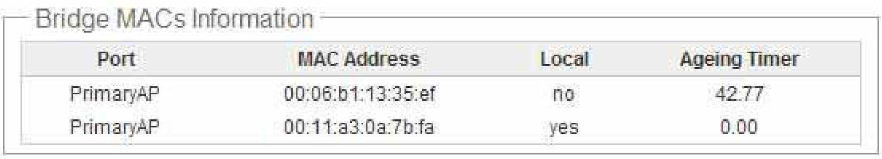
Bridge Table Information

Bridge Port	Bridge ID	STP Enabled	Interface
bre0	8000.0011a30a7bfa	no	ra0

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

  This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

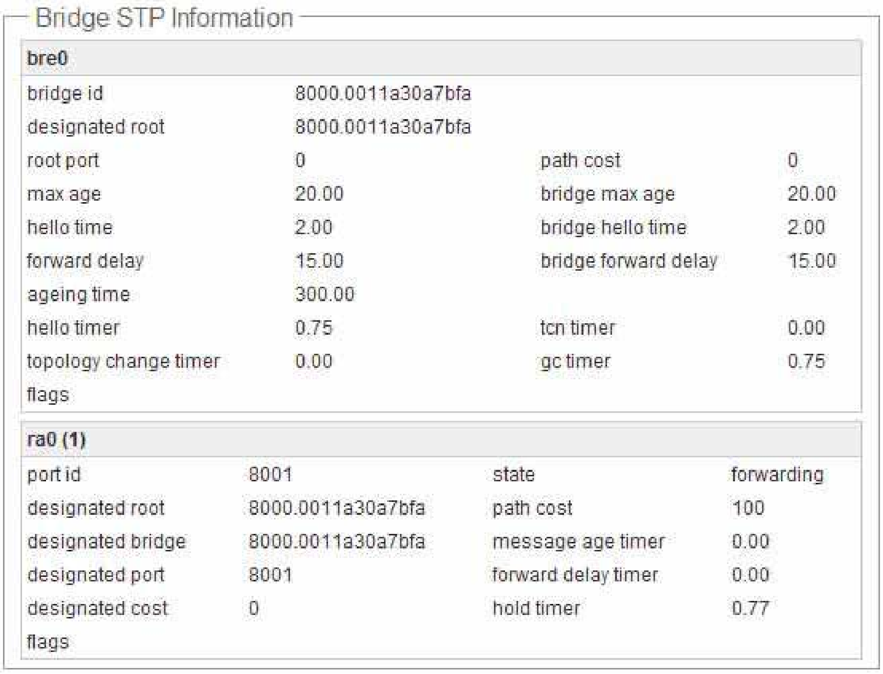
  Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.



Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
PrimaryAP	00:06:b1:13:35:ef	no	42.77
PrimaryAP	00:11:a3:0a:7b:fa	yes	0.00

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.



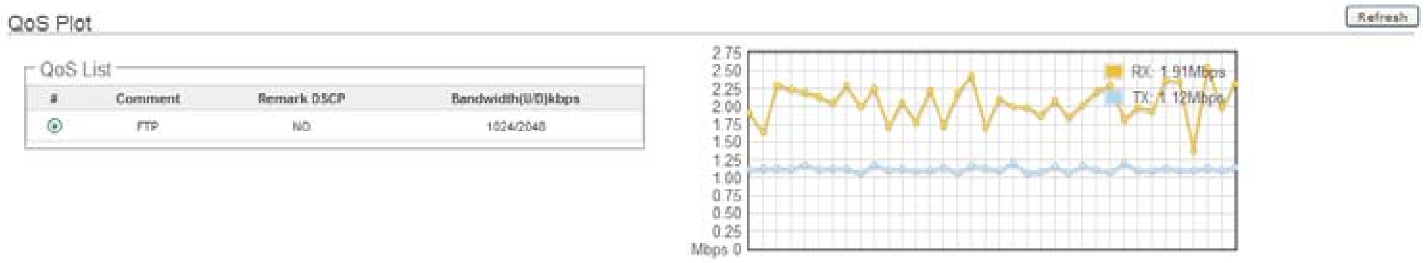
Bridge STP Information

bre0			
bridge id	8000.0011a30a7bfa		
designated root	8000.0011a30a7bfa		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00		
hello timer	0.75	tcn timer	0.00
topology change timer	0.00	gc timer	0.75
flags			

ra0 (1)			
port id	8001	state	forwarding
designated root	8000.0011a30a7bfa	path cost	100
designated bridge	8000.0011a30a7bfa	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.77
flags			

QoS Plot

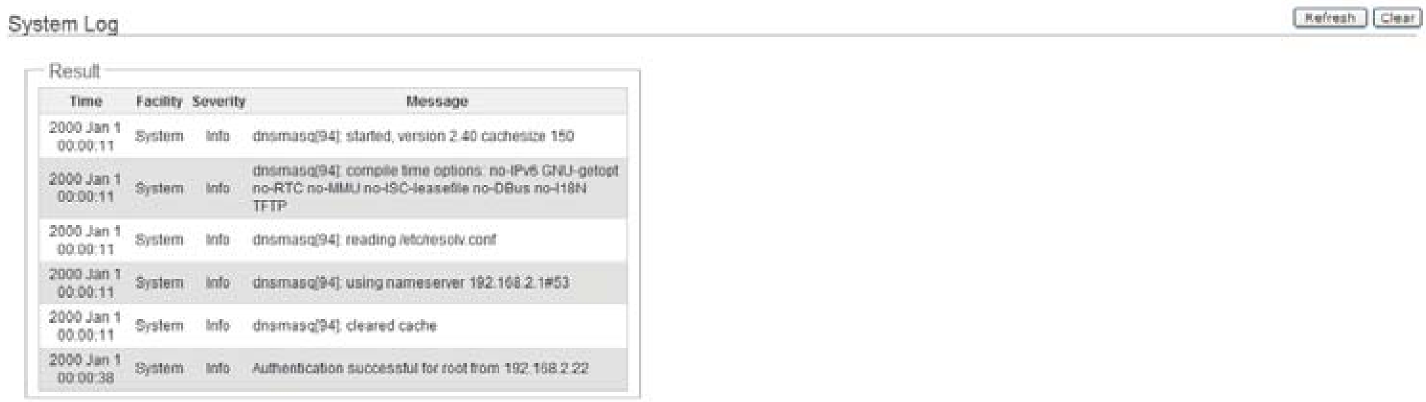
The QoS Plot show graphs which continuously represents the current data traffic on each QoS rule. The chart scale and throughput dimension (bps, Kbps, Mbps) changes dynamically according to the mean throughput value. The statistics is updated automatically every 5 seconds. The throughput statistics of QoS can be updated manually using the ***Refresh*** button.



#	Comment	Remark DSCP	Bandwidth(U/D)kbps
⦿	FTP	NO	1024/2048

Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.



Time	Facility	Severity	Message
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: started, version 2.40 cachesize 150
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-I18N TFTP
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: reading /etc/resolv.conf
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: using nameserver 192.168.2.1#53
2000 Jan 1 00:00:11	System	Info	dnsmasq[94]: cleared cache
2000 Jan 1 00:00:38	System	Info	Authentication successful for root from 192.168.2.22

- **Time :** The date and time when the event occurred.
- **Facility :** It helps users to identify source of events such “System” or “User”
- **Severity :** Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message :** Description of the event.

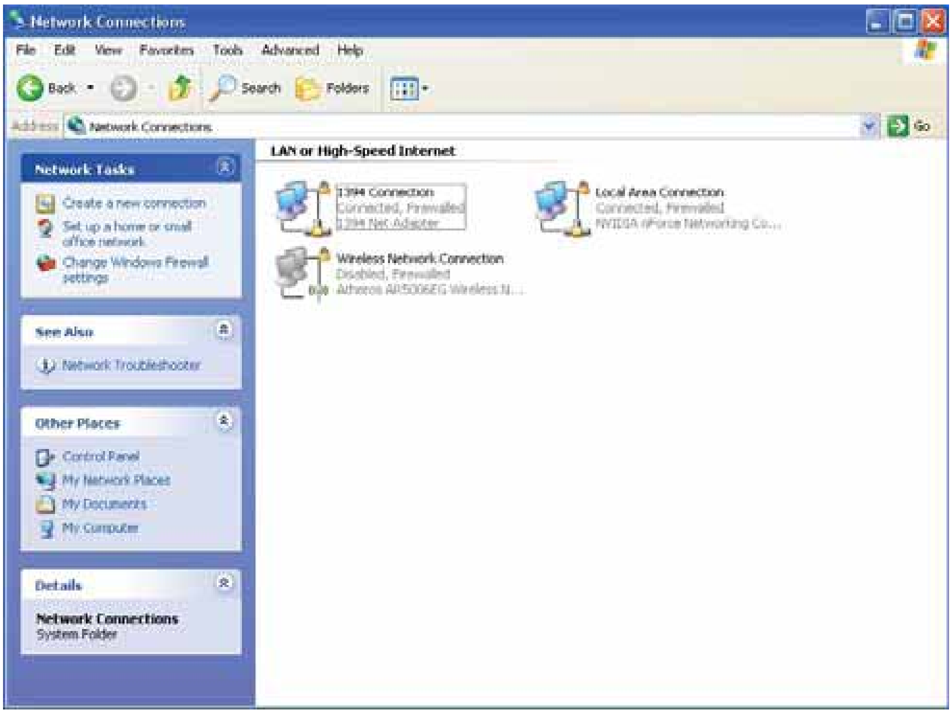
Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

Appendix

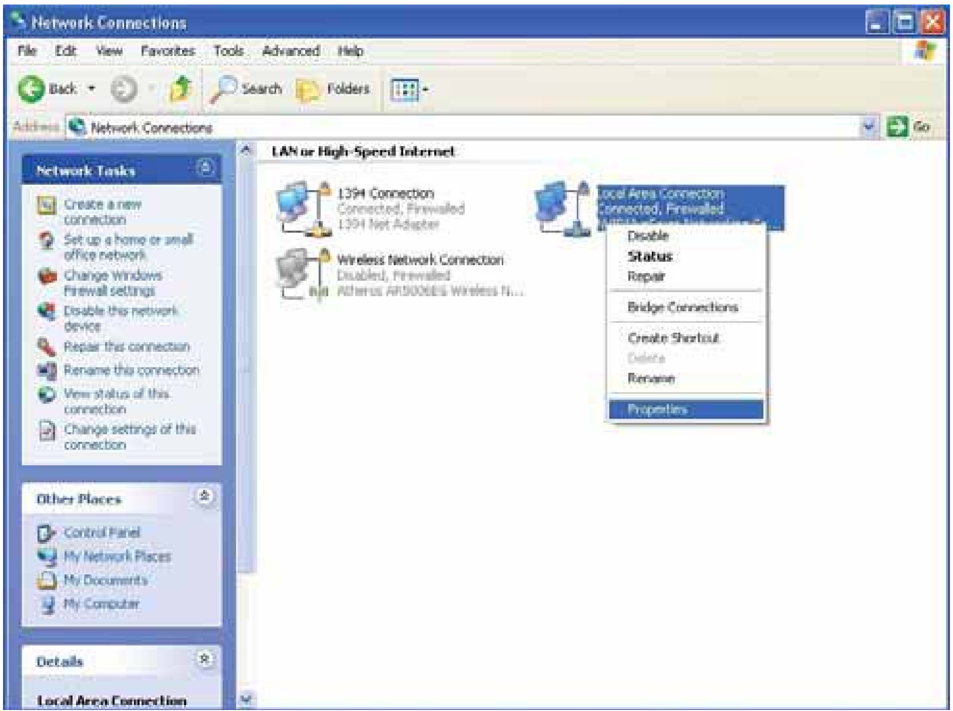
Windows TCP/IP Settings

■ Windows XP

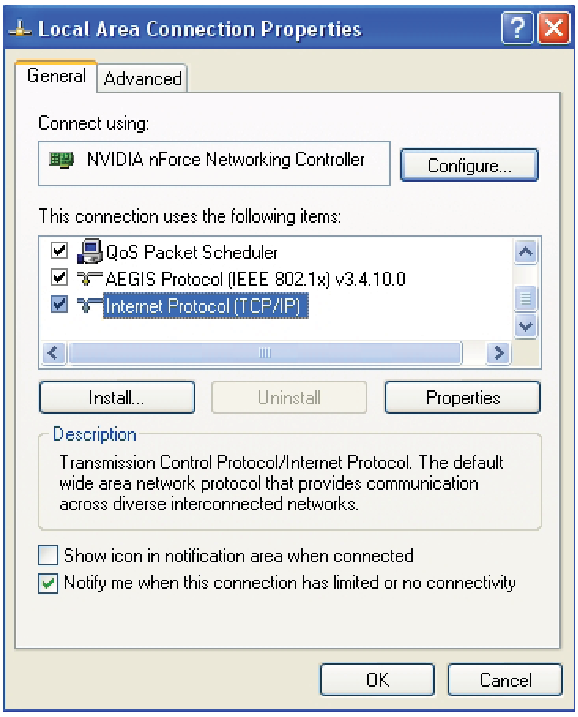
1. Click **Start -> Settings -> Control Panel**, and then "**Control Panel**" window appears. Click on "**Network Connections**", and then "**Network Connections**" window appears.



2. Click right on "**Local Area Connection**", and select ***Properties***.



3. In “**Local Area Connection Properties**” window, select “**Internet Protocol (TCP/IP)**” and click on ***Properties*** button.



Local Area Connection Properties

General | Advanced

Connect using:

NVIDIA nForce Networking Controller — Configure...

This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.4.10.0
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

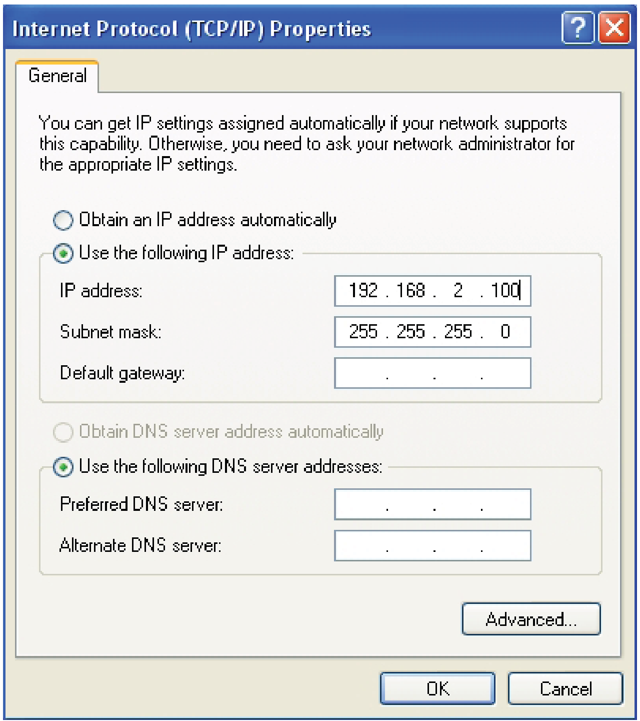
□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

OK | Cancel

4. Select “Use the following IP address”, and type in

IP address :
192.168.2.100

Subnet mask :
255.255.255.0



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 2 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

OK | Cancel

WEB GUI Valid Characters

Table B WEB GUI Valid Characters

Block	**Field**	**Valid Characters**
LAN	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Primary DNS	IP Format; 1-254
	Secondary DNS	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
WAN	Manual MAC Address	12 HEX chars
	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	User name Password	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	MTU	576 ~ 1492 for PPPoE; 1400 ~ 1460 for PPTP
	Idle Time	0 ~ 60 minutes
	Primary DNS	IP Format; 1-254
	Secondary DNS	IP Format; 1-254
DDNS	Hostname	Length : 32 0-9, A-Z, a-z @ - _ .
	User Name	Length : 32

	Password	0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
DHCP Server	Start IP	IP Format; 1-254
	End IP	IP Format; 1-254
	DNS1 IP	IP Format; 1-254
	DNS2 IP	IP Format; 1-254
	WINS IP	IP Format; 1-254
	Domain	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Lease Time	600 ~ 99999999

Table B WEB GUI Valid Characters (continued)

Block	**Field**	**Valid Characters**
Management	System Name/ Location	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Description	32 chars
	Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	HTTP/ HTTPS Port	1 ~ 65535
	Telnet/ SSH Port	1 ~ 65535
SNMP	RO/RW community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO/RW user	Length : 31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO/RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	Community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	IP	IP Format; 1-254
General Setup	Tx Power	1-100 %
Wireless Profile	Profile Name	32 chars
	ESSID	Length : 31 Space 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	Pre-shared Key	8 ~ 63 ASCII chars; 64 HEX chars
Advanced Setup	Beacon Interval	20 ~ 1024

Block	Field	Valid Characters
	Date Beacon Rate	1 ~ 255
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2347

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
Virtual AP Setup	ESSID	Length : 31 Space 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Maximum Clients	1 ~ 32
	VLAN ID	1 ~ 4094
	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	Group Key Update Period	>=60 seconds
	PMK Cache Period	> 0 minute
	Pre-Shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Radius Server IP	IP Format; 1-254
	Radius Port	1 ~ 65535
	Shared Secret	8 ~ 64 characters
	Session Timeout	>= 60 seconds; 0 is disable
WDS Setup	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	TKIP Key	8 ~ 63 ASCII chars; 64 HEX chars
	AES Key	8 ~ 63 ASCII chars; 64 HEX chars
	Peer's MAC Address	12 HEX chars
	Description	32 chars
IP Filter	Source Address	IP Format; 1-254
	Source Mask	0 ~ 32
	Source Port	1 ~ 65535
	Destination Address	IP Format; 1-254
	Destination Mask	0 ~ 32
	Destination Port	1 ~ 65535
MAC Filter	MAC address	MAC Format; 12 HEX chars
Virtual Server	Description	32 chars
	Private IP	IP Formate; 1-254
	Private/ Public Port	1 ~ 65535
DMZ	IP Address	IP Format; 1-254
QoS/ Parental Control	Comment	32 chars
	MAC Address	MAC Format; 12 HEX chars
	Local/ Destination IP	IP Formate; 1-254

Block	Field	Valid Characters
	Local/ Destination Port	1 ~ 65535
	Upload & Download	8 ~ 8192 digital number

MCS Data Rate

The table below shows the relationships between the variables that allow for the maximum data rate

Table C MCS Data Rate

MCS Index	Modulation	Data Rate (Mb/s)			
		Channel Bandwidth = 20		Channel Bandwidth = 40	
		Long Guard Interval	Short Guard Interval	Long Guard Interval	Short Guard Interval
0	BPSK	6.5	7.2	13.5	15.0
1	QPSK	13.0	14.4	27.0	30.0
2	QPSK	19.5	21.7	40.5	45.0
3	16-QAM	26.0	28.9	54.0	60.0
4	16-QAM	39.0	43.3	81.0	90.0
5	64-QAM	52.0	57.8	108.0	120.0
6	64-QAM	58.5	65.0	121.5	135.0
7	64-QAM	65.0	72.2	135.0	157.5
8	BPSK	13.0	14.4	27.0	30.0
9	QPSK	26.0	28.9	54.0	60.0
10	QPSK	39.0	43.3	81.0	90.0
11	16-QAM	52.0	57.8	108.0	120.0
12	16-QAM	78.0	86.7	162.0	180.0
13	64-QAM	104.0	115.6	216.0	240.0
14	64-QAM	117.0	130.0	243.0	270.0
15	64-QAM	130.0	114.4	270.0	300.0

Note :

- ✓ When MCS=32, only Short Guard Interval option is supported, Channel Bandwidth=20 is not supported. If Channel Bandwidth=40, the HT duplicate 6Mbps.
- ✓ When MCS=0~7(One Tx Stream), Guard Interval and Channel Bandwidth are supported
- ✓ When MCS=8~15(Two Tx Stream), Guard Interval and Channel Bandwidth are supported

System Manager Privileges

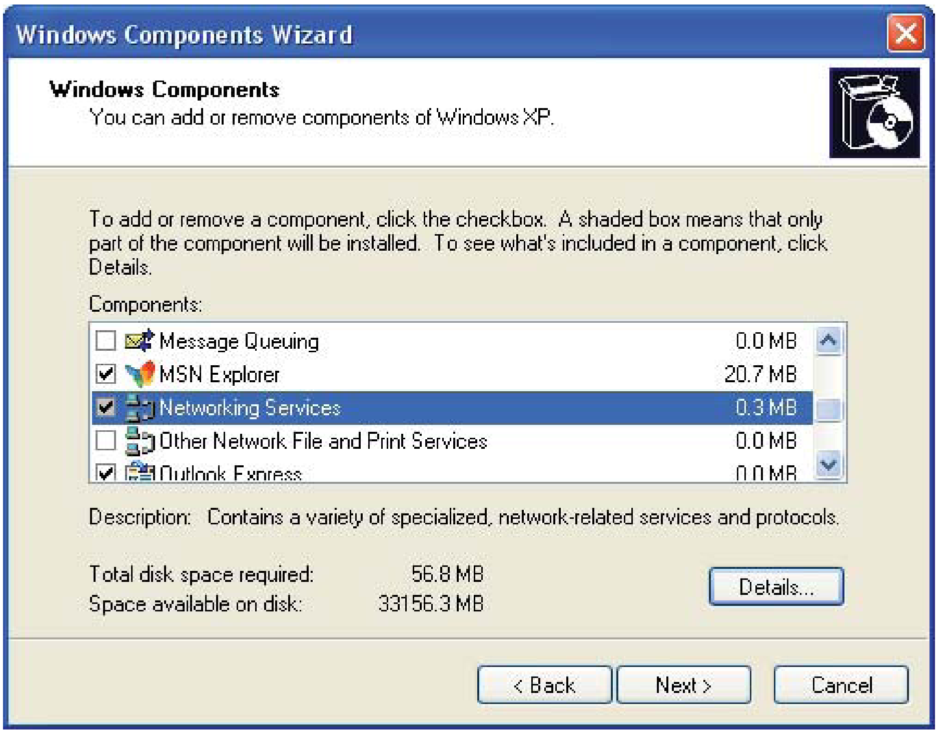
There are two system management accounts for maintaining the system; namely, the **root** and **admin** accounts are with different levels of privileges. The root manager account is empowered with full privilege to Read & Write while the admin manager account is Read only.

The following table display CPE admin account’s privileges.

Main Menu	Sub Menu	Group	Admin Privilege
System	Operating Mode		Read
	WAN		Read
	LAN		Read & Write
	DDNS		Read & Write
	Time Server		Read & Write
	UPNP		Read & Write
	SNMP		Read
Wireless	General		Read
	Advanced		Read
	Site Survey		Read
Advance	DMZ		Read
	IP Filter		Read
	MAC Filter		Read
	Virtual Server		Read
	Parental Control		Read
	QoS		Read
Administrator	Management	System Information	Read
		Root Password	Read
		Admin Password	Read & Write
		Login Methods	Read
		Ping Watchdog	Read
	Profile Settings	Backup Settings	Read & Write
		Restore Settings	Read
		Reset to Default	Read
	System Upgrade		Read
	Network Utility		Read & Write
	Reboot		Read & Write

Enabling UPnP in Windows XP

1. Open the "***Add/Remove Programs***" control panel, and then click on "***Add/Remove Windows Components***" in the sidebar. Scroll down and find "***Networking Services***", highlight it, and then click ***Details***.



Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

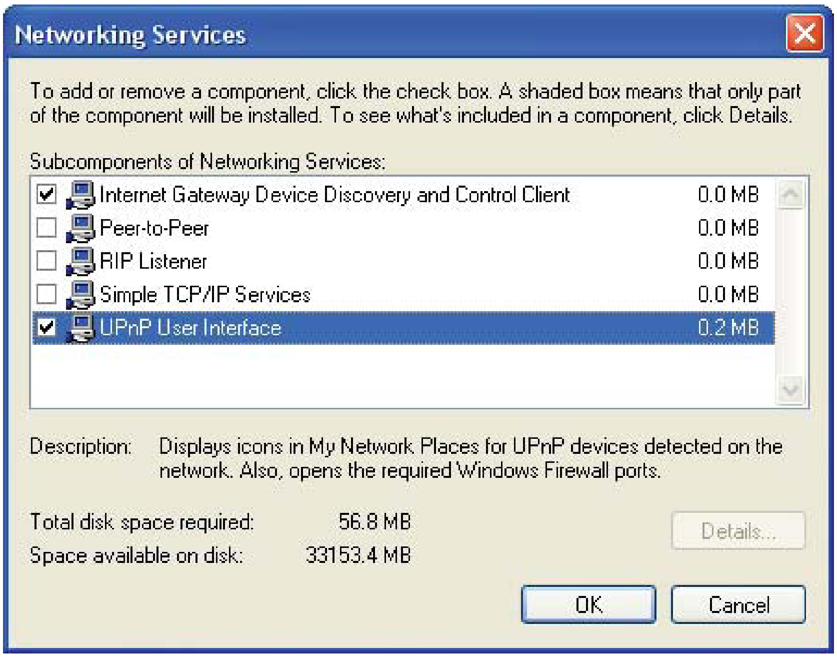
Components:

☐	Message Queuing	0.0 MB
☑	MSN Explorer	20.7 MB
☑	Networking Services	0.3 MB
☐	Other Network File and Print Services	0.0 MB
☑	Outlook Express	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 56.8 MB
Space available on disk: 33156.3 MB

2. In the "**Networking Services**" window, ensure that the "***Internet Gateway Device***" and "***UPnP User Interface***" options are checked. If they are not, check it to enable them, as shown below, and click OK to continue.



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

☑	Internet Gateway Device Discovery and Control Client	0.0 MB
☐	Peer-to-Peer	0.0 MB
☐	RIP Listener	0.0 MB
☐	Simple TCP/IP Services	0.0 MB
☑	UPnP User Interface	0.2 MB

Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.

Total disk space required: 56.8 MB
Space available on disk: 33153.4 MB

3. Next, in the “**Control panel**”, open the “***Administrative Tools”*** and then open “***Services”***. Scroll down until you find the “***SSDP Discovery Interface”***. If the Status is not ***Started***, double-click on *SSDP Discovery Interface* to open the service properties. Change the startup type to ***Automatic***, then close the properties. Now, right-click on *SSDP Discovery Services*, and choose ***Start*** from the pop-up menu. The SSDP Discovery Service will then be running and start each time you boot.
4. After enabling UPnP and starting the SSDP Discovery Service, it may take few minutes for the “TEW-675APBO/ TEW-676APBO” to be discovered and appear in your “***My Network Places”***.

Specification

Hardware	
Standards	Wired: IEEE 802.3u (100Base-TX) Wireless: IEEE 802.11a/n (5 GHz)
LED Indicator	Power, LAN, WLAN (wireless activity)
Antenna	12dBi patch antenna (polarization: V30°, H30°)
PoE	1 x 10/100Mbps RJ-45 PoE port, Passive only (non-802.3af compliant)
Dimension (L x W x H)	215 x 122 x 66 mm (8.5 x 4.8 x 2.6 in)
Weight	1 kg (2.2 lbs)
Power Consumption	6 Watts (max.)
Management	Web browser (HTTP/HTTPS), SNMP (v2c and 3), Telnet, SSH
Wind Speed Support	210 km/hr
Waterproof	IP66/67 compliant
Temperature	
Humidity	Max. 95% (non-condensing)
Overload Current Protection	1.1 A
Power	PoE power injector DC output: 48VDC, 0.4A
Certifications	CE, FCC
Wireless	
Frequency	5.18 ~ 5.805 GHz
Modes	Router, Access Point + WDS, WDS, CPE, Client Bridge + Repeater, CPE + Access Point
Virtual Access Points	7
Associated Clients (max)	224 (AP Mode), 32 (Repeater Mode)
Modulation Technique	802.11a: OFDM with BPSK, QPSK, QAM and 64QAM 802.11n: BPSK, QPSK, 16-QAM, 64-QAM
Data Rate (auto-fallback)	802.11a: up to 54Mbps 802.11a/n: up to 300Mbps
Security	64/128/152-bit WEP, WPA /WPA2-PSK, WPA/WPA2-RADIUS for AP/CPE mode, WEP/WPA2-PSK for WDS mode MAC filter (20 entries) and IP filter (20 entries)

Transmit Power :
5745~5825 GHz
IEEE 802.11a mode:20.31dBm
IEEE 802.11n HT 20 MHz Channel mode:14.76dBm
IEEE 802.11n HT 40 MHz Channel mode:16.26dBm
5180~5230 GHz
IEEE 802.11a mode:2.50dBm
IEEE 802.11n HT 20 MHz Channel mode:4.89dBm
IEEE 802.11n HT 40 MHz Channel mode:4.94dBm

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

TEW-676APBO – 3 Years Warranty

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to http://www.trendnet.com/gpl or http://www.trendnet.com Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

PWP05202009v2