802.11a/n Wireless LAN Outdoor CPE AP/Router

WNAP-7200

Version: 1.0

User's Manual

Copyright

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes..

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

FCC Caution

To assure continued compliance. (Example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

CE Mark Warning

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

Energy Saving Note of the Device

This power required device does not support Stand by mode operation.

For energy saving, please remove the DC-plug or push the hardware Power Switch to OFF position to disconnect the device from the power circuit.

Without remove the DC-plug or switch off the device, the device will still consuming power from the power circuit. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to switch off or remove the DC-plug for the device if this device is not intended to be active.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328-2 has been conducted. These are considered relevant and sufficient.

CE in which Countries where the product may be used freely:

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.

France: except the channel 10 through 13, law prohibits the use of other channels.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User’s Manual for PLANET 802.11a/n Wireless LAN Outdoor CPE AP/Router

Model: WNAP-7200

Rev: 1.0 (January, 2010)

Part No. EM-WNAP7200_v1.0

Table of Contents

1. INTRODUCTION

PLANET Technology Co., provides a high performance outdoor wireless solution for higher coverage and stronger functions - the 5GHz Wireless Outdoor Access Point (WNAP-7200). The PLANET WNAP-7200 is compatible with IEEE802.11a and IEEE802.11a/n, the data rate up to 150Mbps. With built-in 18dBi patch antenna and the high transmit output power, quite suitable for widely open space applications.

The most different with previous product, WNAP-7200 offers WISP mode. CPE users could easily connect to internet via WISP provider or connect to wired network, as well as supporting routing function and offering wireless multiple modes: AP, client, WDS to versatile solutions in a wide range of wireless scenarios. Except 64/128 WEP encryption, it integrates WPA, WPA-PSK, WPA2, WPA2-PSK and 802.1x Authority for securing and protecting your wireless LAN, besides, MAC/IP filter help restrict illegal accessing your local network.

WNAP-7200 is designed to install in outdoor environments, also exposed locations under the rigorous weather conditions including heavy rain and wind. With web-based interface, WNAP-7200 is easy to be managed and configured; PoE (Power over Ethernet) design allows you to install the device in the areas where power outlets aren’t readily available. It is the best way using WNAP-7200 to build outdoor wireless access applications between building to building of campus, business or rural areas…etc.

1.1 Feature

- IEEE 802.11a/n Dual Standards Compatible
- Built-in 18dBi patch Antenna
- Multiple Operating Modes: Bridge, Gateway and WISP
- Supports WEP, WPA, WPA2, 802.1x Authentication
- Firewall supports Content / MAC / IP / Port Filtering
- Power over Ethernet design
- Provides protection against rigorous weather conditions
- High transmit output power
- Web base configuration
- IP65 Enclosure

1.2 Package Contents

- WNAP-7200 x 1
- PoE Injector x 1
- Power Adapter x 1
- Mounting Kit x 1
- CD x 1
- Quick Installation Guide x 1

Note: If any of the above items are missing or damaged, contact your local dealer for support.

1.3 Product Specification

Model	WNAP-7200
Standard	IEEE 802.11a/n
Frequency Band	5GHz 11a ISM Band ; 5.18 ~ 5.825GHz
LAN Port	1 x RJ-45 IEEE802.3, 802.3u, 10/100ase-TX, Auto-MDI
Antenna	Built-in 18dBi patch antenna Horizontal: 25 degree Vertical: 25 degree
Output Power	802.11a: 20±2dBm@54Mbps ; 23±2dBm@6Mbps 802.11a/n: 18±2 dBM
Sensitivity	-73dBm@54Mbps ; -90dBm@6Mbps -70dBm@802.11n rate MCS7
Data Rate	802.11a: Up to 54Mbps 802.11a/n: Up to 150Mbps
System Operating mode	Bridge, Gateway, WISP
Wireless Access Mode	AP, Client, WDS, AP+WDS
Security	WEP, WPA, WPA2 data encryption 802.1x authentication
Management	Web Management
IP Level	IP-65
Dimension (W x D x H)	215 x 98 x 260 mm
Power Adapter	12V DC, 1.25A (passive PoE)
Operating Environment	Temperature: 0~55 Degree C Humidity: 5~90% non-condensing

1.4 Wireless Performance

The following information will help you utilizing the wireless performance, and operating coverage of WNAP-7200.

1. Site selection

To avoid interferences, please locate WNAP-7200 and wireless clients away from transformers, microwave ovens, heavy-duty motors, refrigerators, fluorescent lights, and other industrial equipments. Keep the number of walls, or ceilings between AP and clients as few as possible; otherwise the signal strength may be seriously reduced. Place WNAP-7200 in open space or add additional WNAP-7200 as needed to improve the coverage.

2. Environmental factors

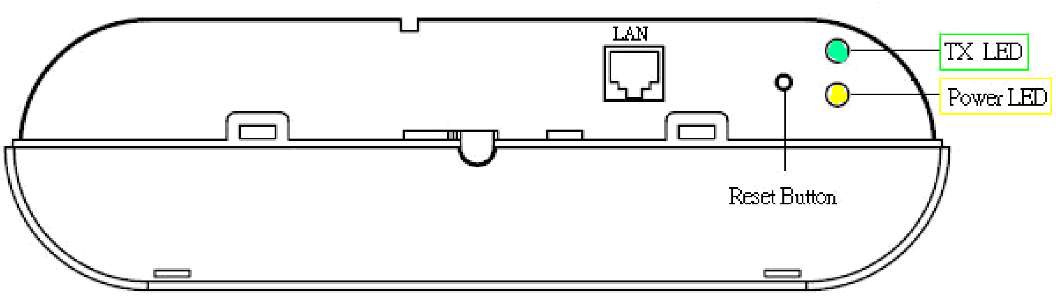
The wireless network is easily affected by many environmental factors. Every environment is unique with different obstacles, construction materials, weather, etc. It is hard to determine the exact operating range of WNAP-7200 in a specific location without testing.

2. INSTALLATION

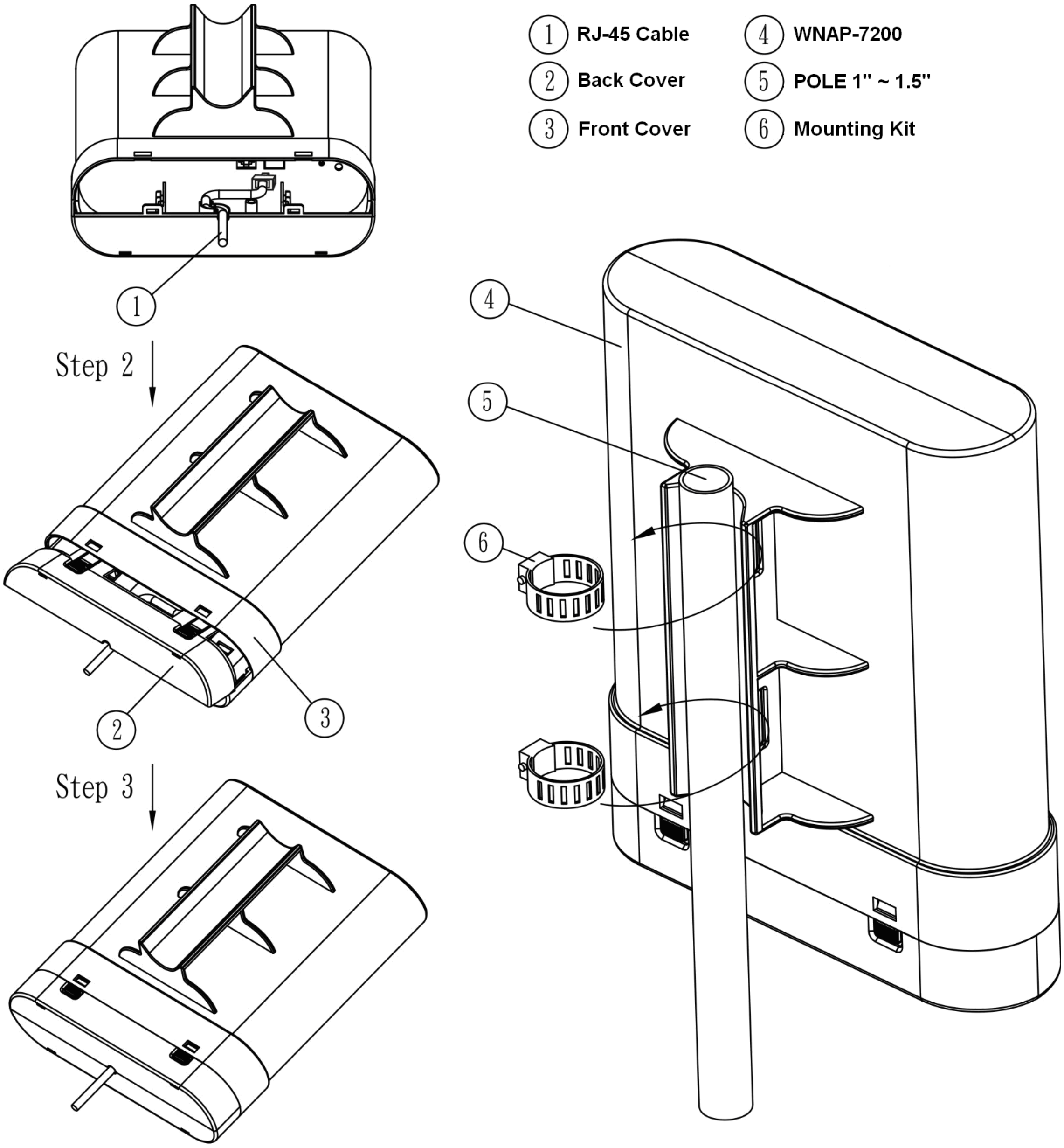
Before you proceed with the installation, it is necessary that you have enough information about the WNAP-7200.

2.1 Interfaces

Here shows the port, button and LED information inside the WNAP-7200.



2.2 Hardware Installation



Before you proceed with the installation, it is necessary that you have enough information about WNAP-7200.

1. Please connect right installation “PoE” port of PoE inject to WNAP-7200; “LAN” port of PoE injector to LAN PC, wrong installation will cause the device damage.

> **Note:** Strongly suggest using SFTP cable, for better protection of the data wire.
> 25-meter SFTP cable also available by order, the part no is CB-STP-25.
> Please contact with local dealer for more information.

2. Using Category 3 or higher UTP or STP cable, connect the “LAN” port of PoE Injector to a 10Mbps or 10/100Mbps Ethernet hub or switch, and connect the PC on the same LAN for management.

3. Locate an optimum location and use the provided Mounting kit to tie the WNAP-7200 to a pole.

> **Note:** 1. To avoid thunder strike, consider installing ELA-100, thunder arrester toward the CPE AP and the PoE injector.
> 2. For secured reason, while install the CPE AP, please be aware for the electric wires around, and tighten the pole. Without tighten the CPE AP, the pole and the installed site is with electric wire around, there could be danger of being hurt by falling or lethal injury.

4. Connect the 12V 1.25A DC power adapter to the PoE Injector socket, and plug it into an AC outlet to power on the WNAP-7200.

> **Note:** 1. The PoE Injector is a passive device. It will inject the DC power into the UTP cable right away once you connect the DC-plug in to the DC-jack of the PoE Injector.
> 2. DONOT connect the PoE Injector labeled as POE port to any devices but WNAP-7200, otherwise it will damage the device permanently.

5. For Ethernet port application, please refer to user’s manual for bridge, gateway and WISP application for the first installation, LAN port is suggested.

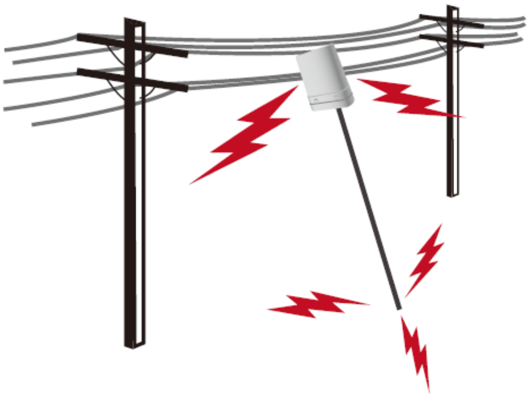
> **Note:** 1. ONLY use the power adapter supplied with the WNAP-7200. Otherwise, the product may be damaged.
> 2. Strongly suggest using STP cable whether the cable exposed outdoor for waterproof and avoiding thunder stroke.

2.3 Safety Precautions

⚠ **OUTDOOR INSTALLATION WARNING**
IMPORTANT SAFETY PRECAUTIONS:

LIVES MAY BE AT RISK! Carefully observe these instructions and any special instructions that are included with the equipment you are installing.

CONTACTING POWER LINES CAN BE LETHAL.
Make sure no power lines are anywhere where possible contact can be made. Antennas, masts, towers, guy wires or cables may lean or fall and contact these limes. People may be injured or killed if they are touching or holding any part of equipment when it contacts electric lines. Make sure there is NO possibility that equipment or personnel can come in contact directly or indirectly with power lines.



Assume all overhead lines are power lines.

The horizontal distance from a tower, mast or antenna to the nearest power line should be at least twice the total length of the mast/antenna combination. This will ensure that the mast will not contact power if it falls either during installation or later.

TO AVOID FALLING, USE SAFE PROCEDURES WHEN WORKING AT HEIGHTS ABOVE GROUND.

Select equipment locations that will allow safe, simple equipment installation.

- Don't work alone. A friend or co-worker can save your life if an accident happens.
- Use approved non-conducting lasers and other safety equipment. Make sure all equipment is in good repair.
- If a tower or mast begins falling, don't attempt to catch it. Stand back and let it fall.
- If anything such as a wire or mast does come in contact with a power line, **DON'T TOUCH IT OR ATTEMPT TO MOVE IT**. Instead, save your life by calling the power company.
- Don't attempt to erect antennas or towers on windy days.

MAKE SURE ALL TOWERS AND MASTS ARE SECURELY GROUNDED, AND ELECTRICAL CABLES CONNECTED TO ANTENNAS HAVE LIGHTNING ARRESTORS.

This will help prevent fire damage or human injury in case of lightning, static build-up, or short circuit within equipment connected to the antenna.

- The base of the antenna mast or tower must be connected directly to the building protective ground or to one or more approved grounding rods, using 1 OAWG ground wire and corrosion-resistant connectors.
- Refer to the National Electrical Code for grounding details.

IF A PERSON COMES IN CONTACT WITH ELECTRICAL POWER, AND CANNOT MOVE:

- **DON'T TOUCH THAT PERSON, OR YOU MAY BE ELECTROCUTED.**
- Use a non-conductive dry board, stick or rope to push or drag them so they no longer are in contact with electrical power.
- Once they are no longer contacting electrical power, administer CPR if you are certified, and make sure that emergency medical aid has been requested.

3. GETTING STARTED

The WLAN CPE is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: **192.168.0.1**
Default IP subnet mask: **255.255.255.0**
WEB login User Name: **admin**
WEB login Password: **admin**

The device has multiple operation modes (Bridge / Gateway / WISP). The default mode is Bridge mode and the default IP addresses for the device are 192.168.0.1, so you need to make sure the IP address of your PC is in the same subnet as the device, such as 192.168.0.2~254.

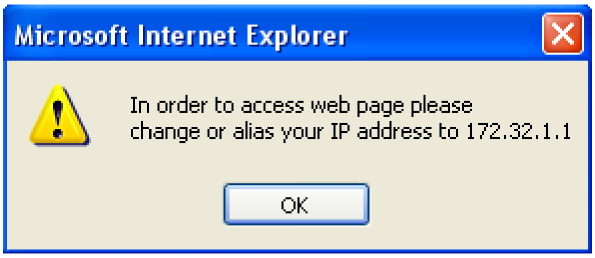
Note: It will take about 40 seconds to complete the boot up sequence after power on.

Default IP address of WISP mode:

Default IP Address: **172.32.1.254**
Default IP subnet mask: **255.255.255.0**

So you need to make sure the IP address of your PC is in the same subnet as the device, such as 172.32.1.1~253.

The system will prompt the message when you change the operating mode to WISP.



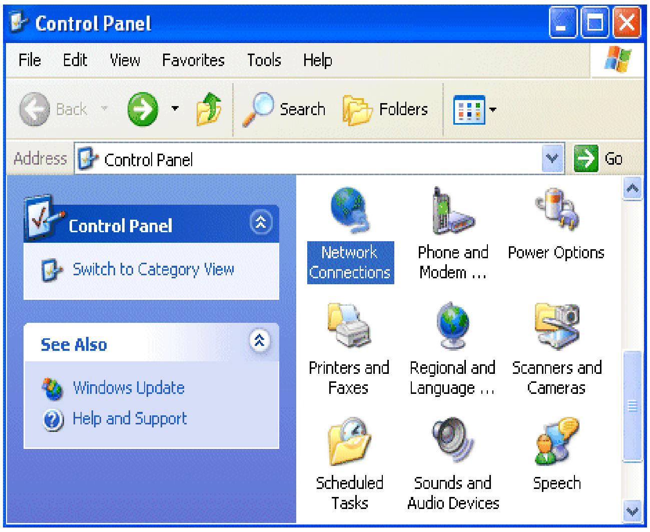
In order to access web page please
change or alias your IP address to 172.32.1.1

3.1 Prepare your PC

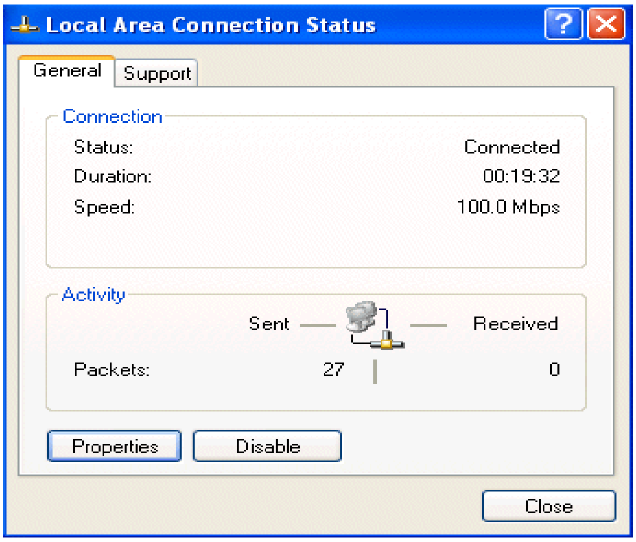
Configuring PC in Windows XP

1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**.

2. Double-click **Local Area Connection**.

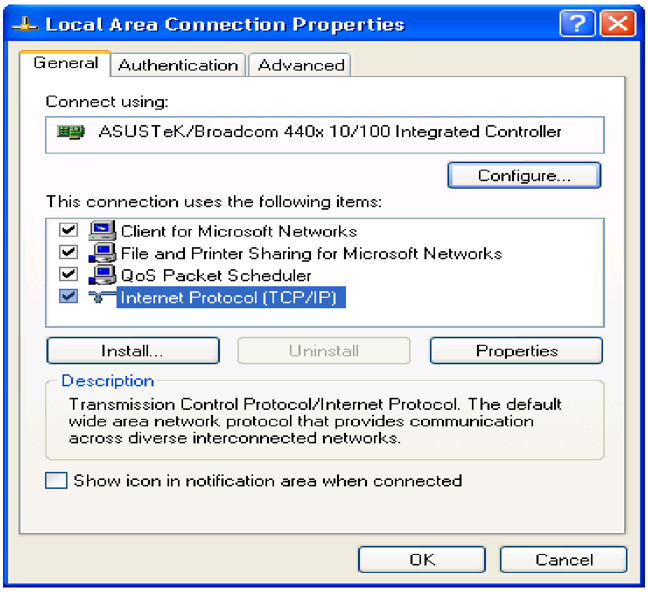


3. In the **Local Area Connection Status** window, click **Properties**.



Status: Connected
Duration: 00:19:32
Speed: 100.0 Mbps
Packets: 27 0

4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

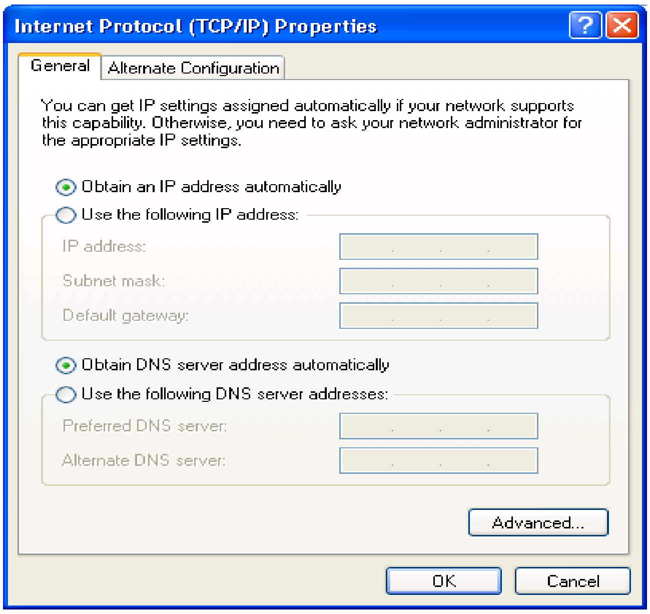
Description

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

5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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: . . .
Subnet mask: . . .
Default gateway: . . .

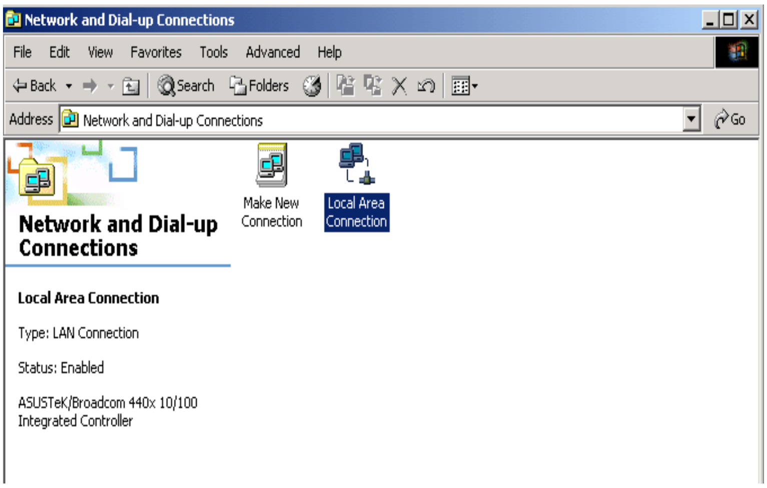
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Configuring PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.

2. Double-click **Local Area Connection**.



Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network and Dial-up Connections Go
Network and Dial-up Connections
Make New Connection
Local Area Connection

Local Area Connection

Type: LAN Connection

Status: Enabled

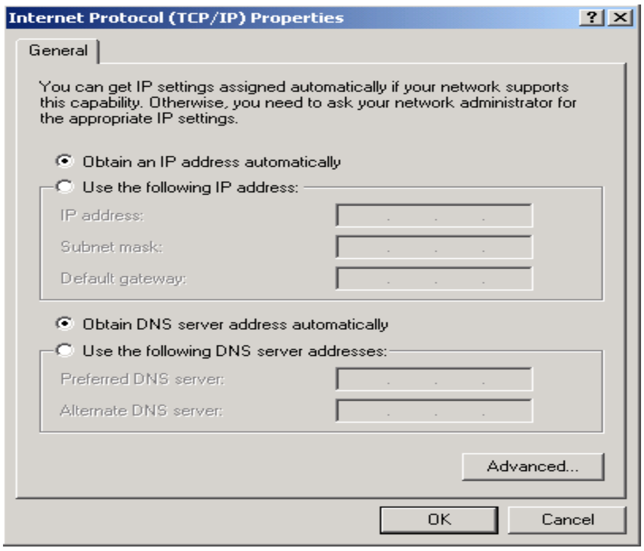
ASUSTeK/Broadcom 440x 10/100
Integrated Controller

3. In the **Local Area Connection Status** window click **Properties**.

4. Select **Internet Protocol (TCP/IP)** and click **Properties**.

5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.



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: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

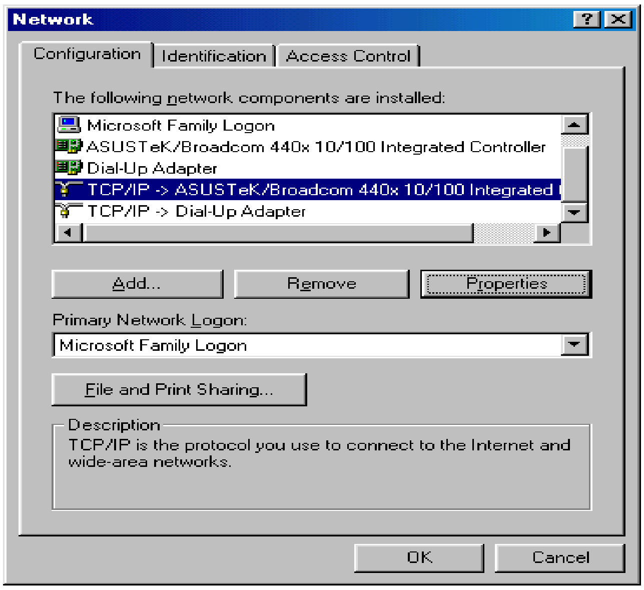
Preferred DNS server: . . .

Alternate DNS server: . . .

Configuring PC in Windows 98/Me

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.

2. Select **TCP/IP → NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.



The following network components are installed:

- Microsoft Family Logon
- ASUSTeK/Broadcom 440x 10/100 Integrated Controller
- Dial-Up Adapter
- TCP/IP -> ASUSTeK/Broadcom 440x 10/100 Integrated
- TCP/IP -> Dial-Up Adapter

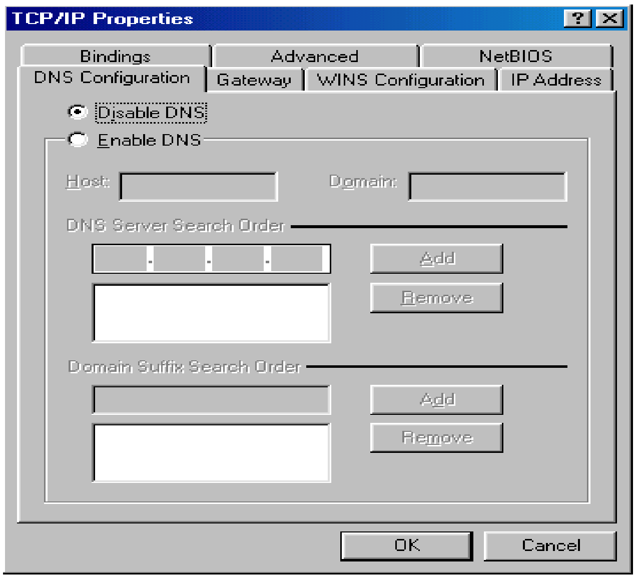
Primary Network Logon: Microsoft Family Logon

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

3. Select the **Obtain an IP address automatically** radio button.

4. Then select the **DNS Configuration** tab.

5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



● Disable DNS
○ Enable DNS

4. WEB MANAGEMENT

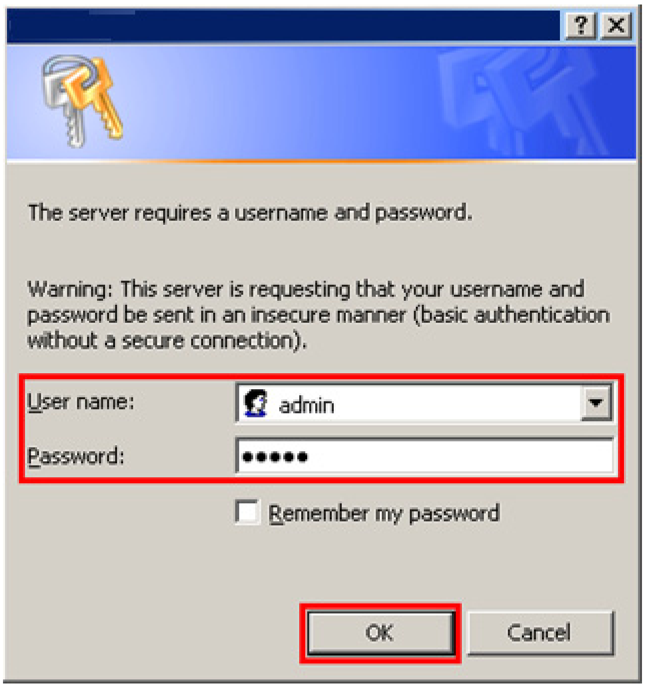
Web configuration provides a user-friendly graphical user interface (web pages) to manage your WNAP-7200. An AP with an assigned IP address will allow you to monitor and configure via web browser (e.g., MS Internet Explorer or Netscape).

4.1 Access the Web Management

To access the web management, you have to launch your Internet Browser.

- **Step1:** Enter Wireless Router's default IP address as **http://192.168.0.1** in the Address field then press Enter.

- **Step2:** Login dialog box will appear, enter **admin** as Administrator Name and **admin** as default administrator password, and then click "Login" to access configuration utility.



The server requires a username and password.

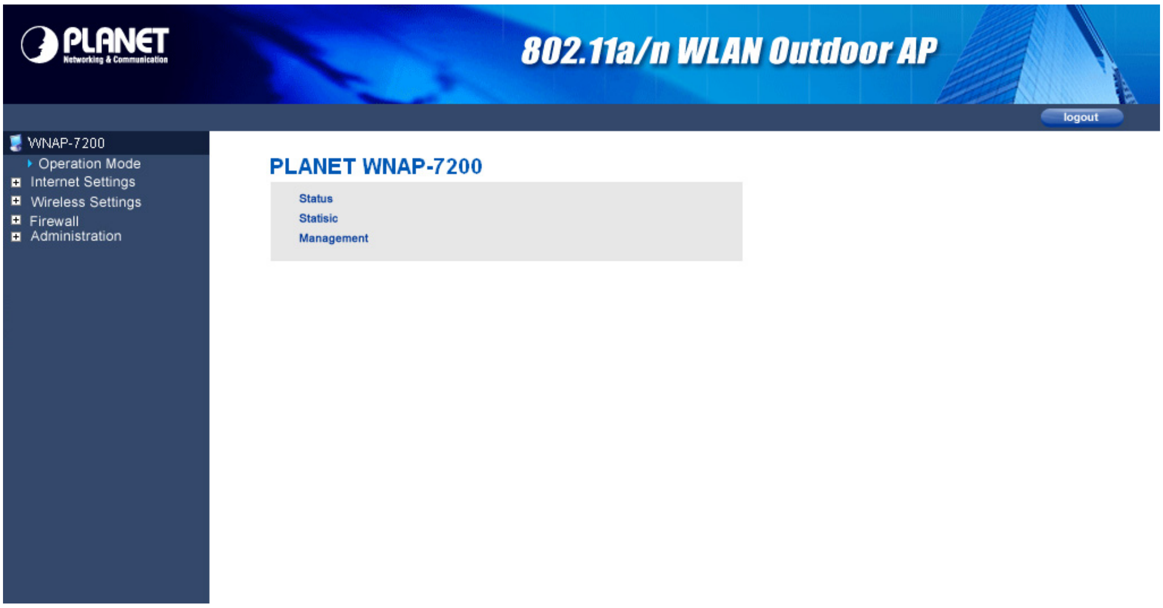
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password: ●●●●●

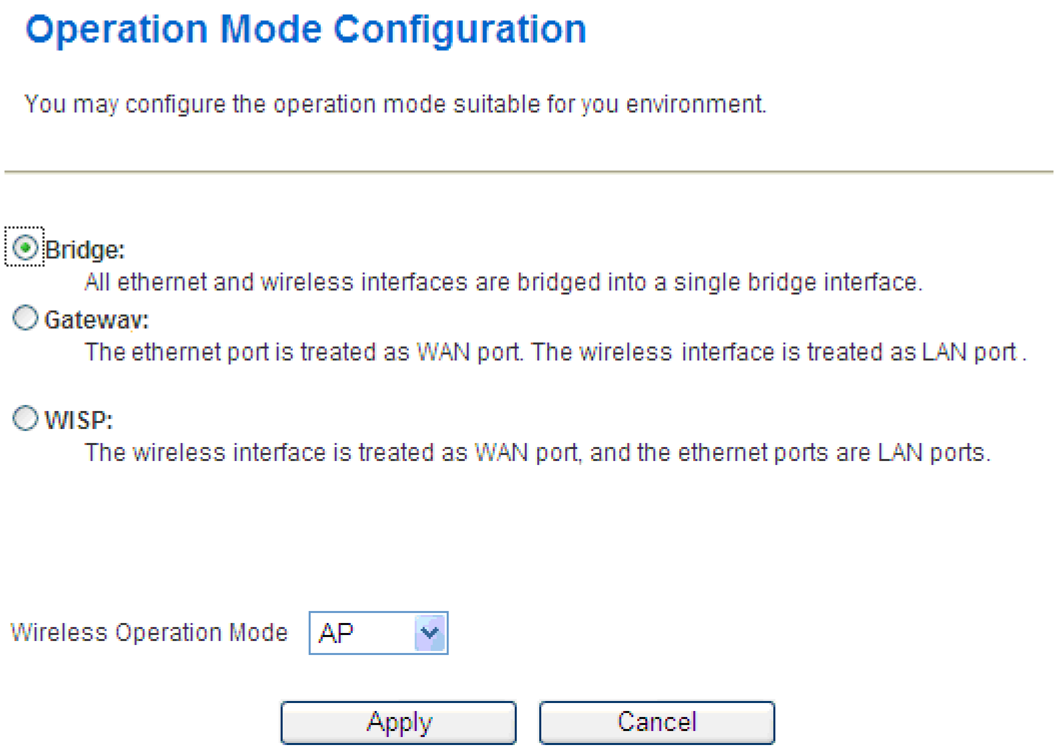
□ Remember my password

- **Step3:** After log in, you can see the Main menu as below.



4.2 Operation Mode

In this option, you can configure the operation mode which suitable for your environment. The default setting is **Bridge - AP**. There are multiple modes provided:



Operation Mode Configuration

You may configure the operation mode suitable for you environment.

● Bridge:
All ethernet and wireless interfaces are bridged into a single bridge interface.

○ Gateway:
The ethernet port is treated as WAN port. The wireless interface is treated as LAN port .

○ WISP:
The wireless interface is treated as WAN port, and the ethernet ports are LAN ports.

Wireless Operation Mode: AP

- **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface. When Bridge mode is applied, there have some functions change in Internet Settings section. As you can see in below, Internet Settings section only has **"LAN", "DHCP Client", "VPN Pass-through", "DNS"**, and **"Advanced Routing"** for Bridge Mode's configuration.

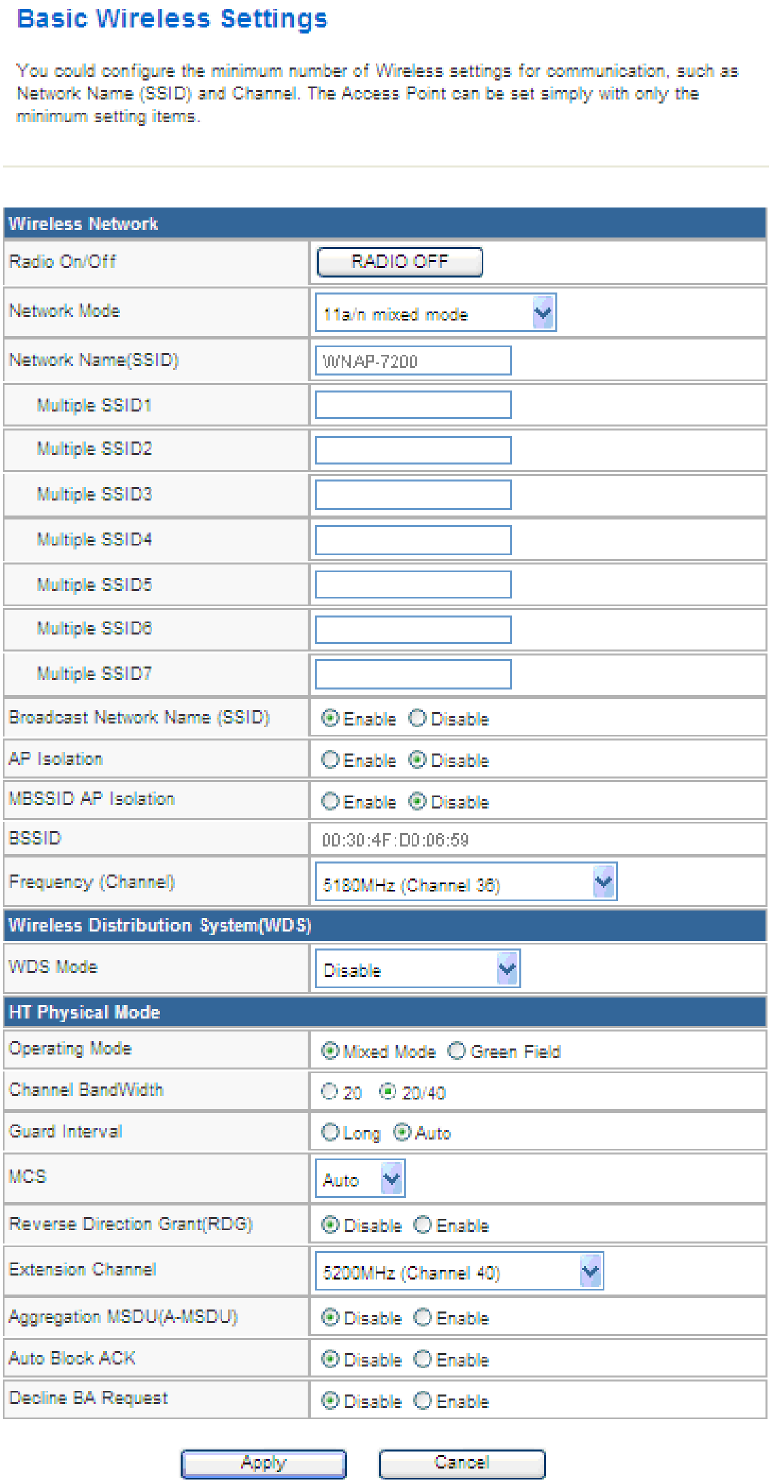
- **Gateway:** The Ethernet port is treated as WAN port. The wireless interface is treated as LAN port.

- **WISP:** The wireless interface is treated as WAN port and the Ethernet ports are LAN ports. After Ethernet Converter mode is applied, the WAN will change from Ethernet type to wireless type. There will be five LAN ports and one wireless WAN port. User must configure wireless encryption connection and set the necessary protocols.

4.3 Wireless Settings (AP)

4.3.1 Basic

You can configure the minimum number of wireless settings for communication, such as network name (SSID) and channel.



Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Radio On/Off	RADIO OFF
Network Mode	11a/n mixed mode
Network Name(SSID)	WNAP-7200
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Multiple SSID7	
Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:30:4F:D0:06:59
Frequency (Channel)	5180MHz (Channel 36)
Wireless Distribution System(WDS)	
WDS Mode	Disable
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
Extension Channel	5200MHz (Channel 40)
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	● Disable ○ Enable
Decline BA Request	● Disable ○ Enable

Wireless Network

Radio On/Off:

Enable or disable the wireless LAN.

Network Mode:

There are 11n only and 11a/g mixed mode.

Network Name (SSID):

The service set identification (SSID) is a unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Enter a descriptive name. Its length is up to 32 characters.

Multiple SSID 1/2/3/4/5/6/7:

There are 7 multiple SSIDs. Enter their descriptive names that you want to use.

Broadcast Network Name (SSID):

Select **Enable** to allow the SSID broadcast on the network, so that the STA can find it. Otherwise, the STA can not find it.

AP Isolation:

Enable or disable AP Isolation. When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can enable this function.

MBSSID AP Isolation:

Enable or disable MBSSID AP Isolation.

BSSID:

Basic Service Set Identifier. This is the assigned MAC address of the station in the access point. This unique identifier is in Hex format and can only be edited when Multi BSSID is enabled in the previous screen.

Frequency (Channel):

A channel is the radio frequency used by wireless device. Channels available depend on your geographical area. You may have a choice of channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. The Interference and degrading performance occurs when radio signals from different APs overlap.

Wireless Distribution System (WDS)

WDS Mode:

Enable or disable the WDS function.

HT Physical Mode

Operation Mode:

Select Mixed Mode or Green Field.

Channel Bandwidth:

Select 20 or 20/40.

Guard Interval:

Select Long or Auto.

MCS:

Select the proper value between 0 and15 or 32. Auto is the default value.

Reverse Direction Grant (RDG):

Select Disable or Enable.

Extension Channel:

Select the proper extension channel in the drop-down list.

Aggregation MSDU (A-MSDU):

Select Disable or Enable.

Auto Block ACK:

Select Disable or Enable.

Decline BA Request:

Select Disable or Enable.

4.3.1.1 Wireless Distribution System (WDS)

Wireless Distribution System (WDS)

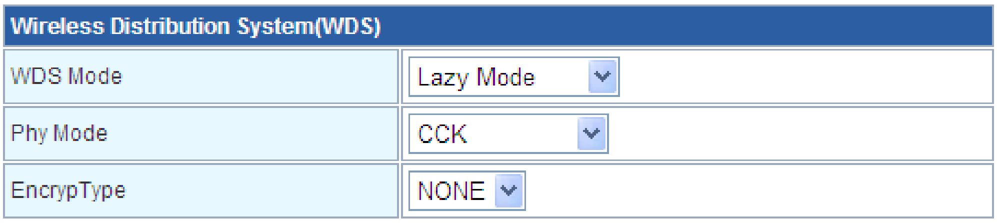
WDS Mode:

There are four options, including **Disable**, **Lazy Mode**, **Bridge Mode**, and **Repeater Mode**.

- **Disable**

Select Disable to disable the WDS mode.

- **Lazy Mode**



Wireless Distribution System(WDS)

WDS Mode	Lazy Mode
Phy Mode	CCK
EncrypType	NONE

WDS Mode:

Select Lazy Mode. The WDS Lazy mode is allowed the other WDS bridge / repeater mode link automatically.

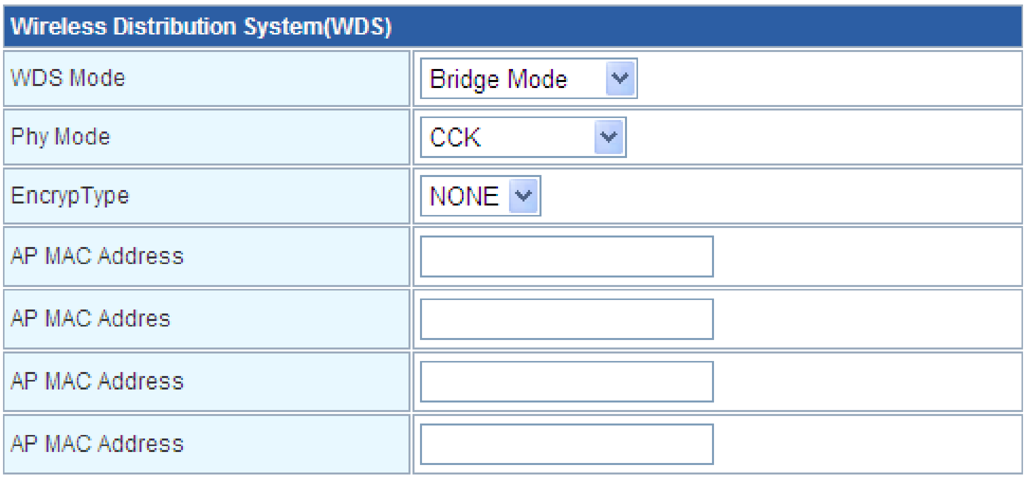
Phy Mode:

It provides 4 options, including **CCK**, **OFDM**, **HTMIX**, and **GREENFIELD**.

Encryp Type:

It provides 4 options, including **None, WEP, TKIP,** and **AES**.

- **Bridge Mode/ Repeater Mode**



Wireless Distribution System(WDS)

WDS Mode	Bridge Mode
Phy Mode	CCK
EncrypType	NONE
AP MAC Address	
AP MAC Addres	
AP MAC Address	
AP MAC Address	

WDS Mode:

Select **Bridge** Mode or **Repeater** Mode.

Phy Mode:

It provides 4 options, including CCK, OFDM, HTMIX, and GREENFIELD.

Encryp Type:

It provides 4 options, including **None, WEP, TKIP**, and **AES**.

AP MAC Address:

It provides 4 AP MAC Address. Enter the MAC address of the other APs.

WDS (Wireless Distribution System) allows access points to communicate with one another wirelessly in a standardized way. It can also simplify the network infrastructure by reducing the amount of cabling required. Basically the access points will act as a client and an access point at the same time.

WDS is incompatible with WPA. Both features cannot be used at the same time. A WDS link is bi-directional, so the AP must know the MAC address of the other AP, and the other AP must have a WDS link back to the AP.

Dynamically assigned and rotated encryption key are not supported in a WDS connection. This means that WPA and other dynamic key assignment technologies may not be used. Only Static WEP keys may be used in a WDS connection, including any STAs that are associated with a WDS repeating AP.

Enter the MAC address of the other APs that you want to link to and click enable.

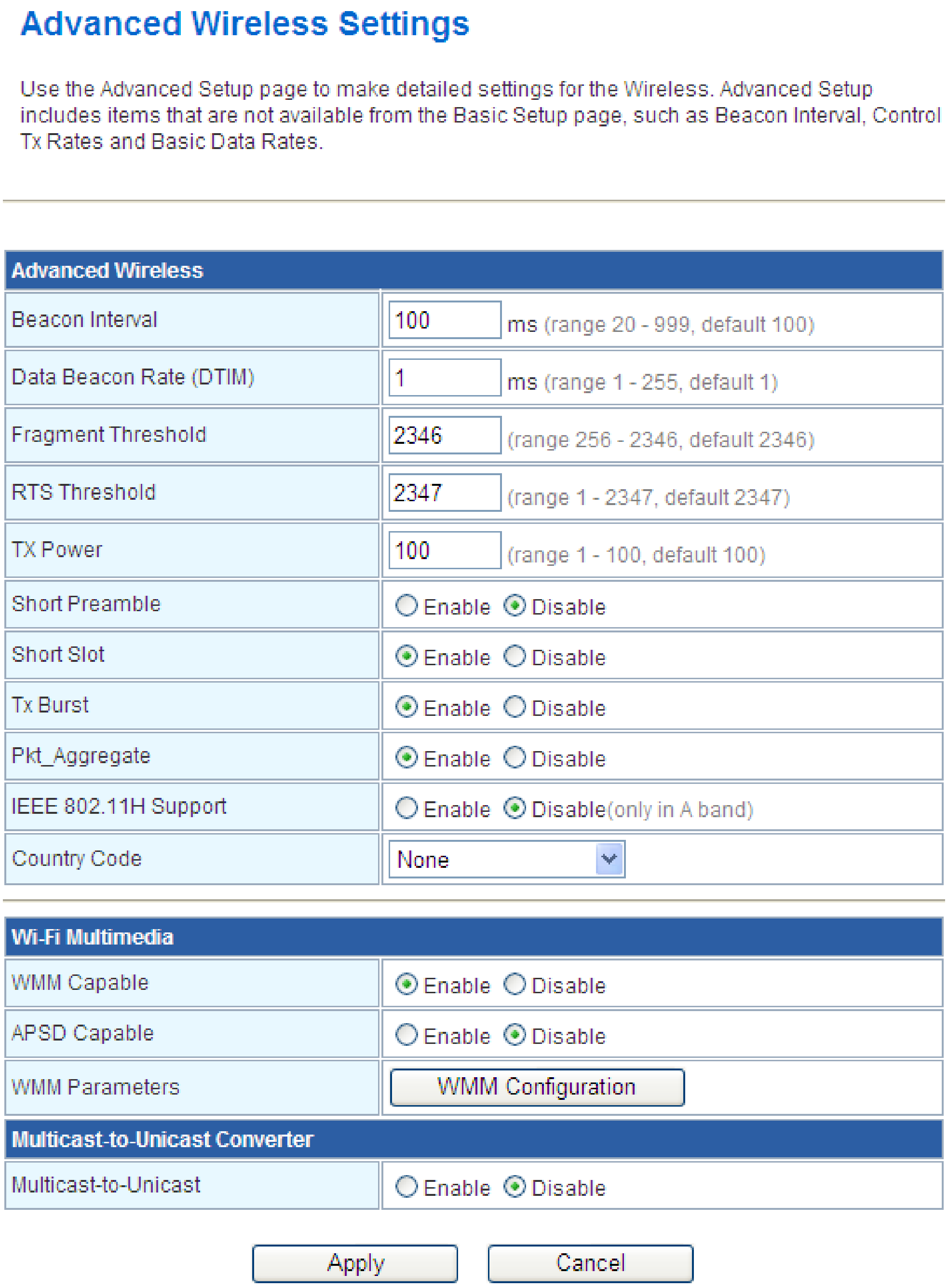
Supports up to 4 point to multipoint WDS links, check Enable WDS and then enable on the MAC addresses.

Example of a WDS topology:

AP1 <-- WDS --> Master AP <-- WDS --> AP3 <-- WDS --> AP4

4.3.2 Advanced

This page makes more detailed settings for the AP. **Advanced Wireless Settings** page includes items that are not available in the **Basic Wireless Settings** page, such as basic data rates, beacon interval, and data beacon rate.



Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	○ Enable ● Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
IEEE 802.11H Support	○ Enable ● Disable(only in A band)
Country Code	None

Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
WMM Parameters	WMM Configuration

Multicast-to-Unicast Converter	
Multicast-to-Unicast	○ Enable ● Disable

Advanced Wireless

Beacon Interval:

The interval time range is between 20ms and 999ms for each beacon transmission. The default value is 100ms.

Date Beacon Rate (DTM):

The DTM range is between 1 ms and 255 ms. The default value is 1ms.

Fragment Threshold:

This is the maximum data fragment size (between 256 bytes and 2346 bytes) that can be sent in the wireless network before the router fragments the packet into smaller data frames. The default value is 2346.

RTS Threshold:

Request to send (RTS) is designed to prevent collisions due to hidden node. A RTS defines the biggest size data frame you can send before a RTS handshake invoked. The RTS threshold value is between 1 and 2347. The default value is 2347.

If the RTS threshold value is greater than the fragment threshold value, the RTS handshake does not occur. Because the data frames are fragmented before they reach the RTS size.

Tx Power:

The Tx Power range is between 1 and 100. The default value is 100.

Short Preamble:

Select Disable or Enable.

Short Slot:

Select Disable or Enable.

Tx Burst:

Select Disable or Enable.

Pkt_Aggregate:

Select Disable or Enable.

Country Code:

Select the region which area you are. It provides six regions in the drop-down list.

Wi-Fi Multimedia

WMM Capable:

Enable or disable WMM.

APSD Capable:

Enable or disable APSD.

WMM Parameter:

Click WMM Configuration button to pop up WMM Parameters of Access Point page. You can configure WMM parameters in the page.

Multicast-to-Unicast Converter

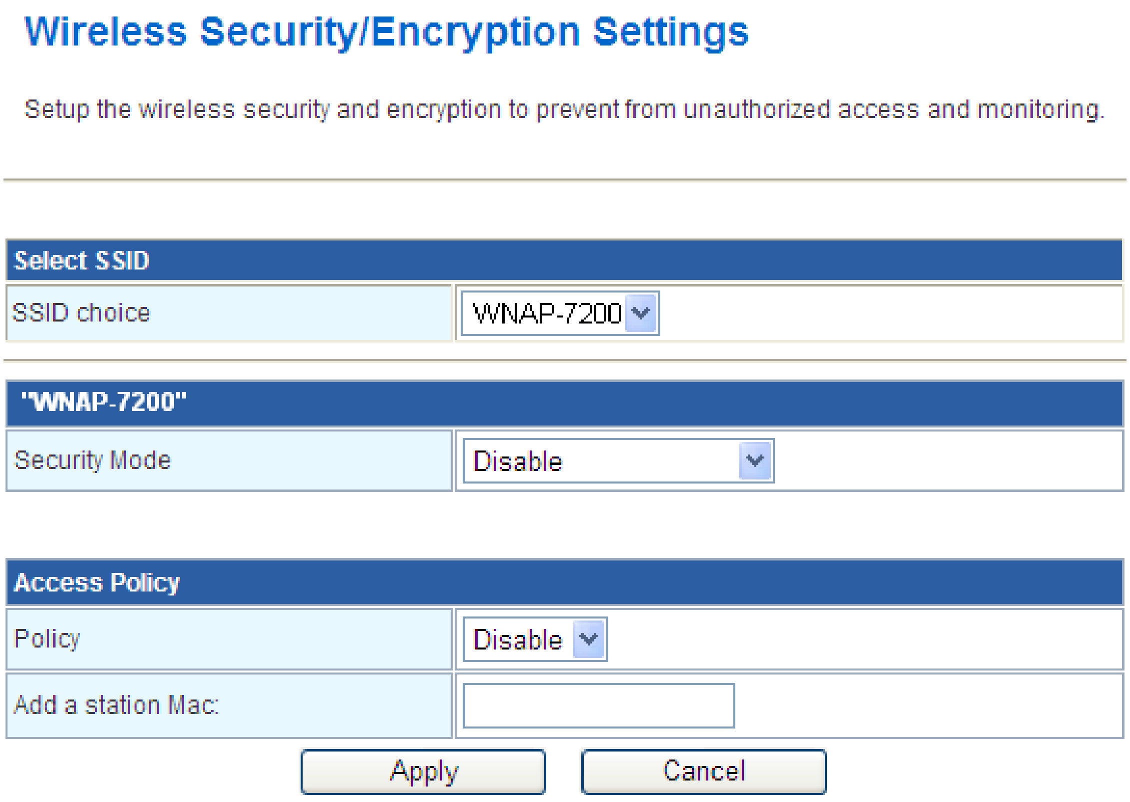
Multicast-to-Unicast Converter:

Enable or disable Multicast-to-Unicast Converter.

After finishing the settings above, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

4.3.3 Security

Choose **Wireless Settings > Security** and the following page appears. It allows you to modify the settings to prevent the unauthorized accesses.



Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	WNAP-7200

"WNAP-7200"	
Security Mode	Disable

Access Policy	
Policy	Disable
Add a station Mac:	

<u>Select SSID</u>

SSID choice:

Select SSID in the drop-down list**.**

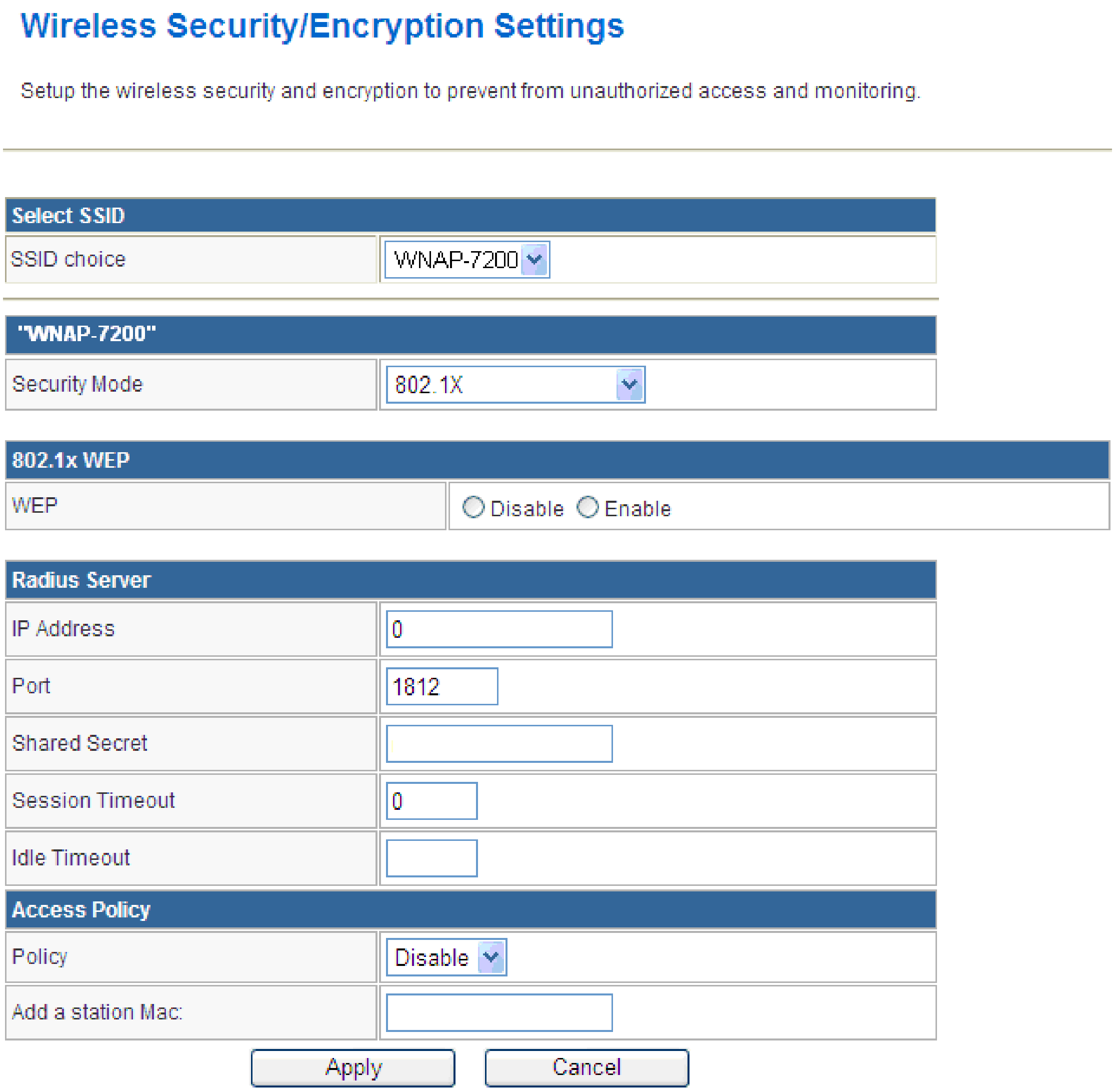
<u>Security</u>

Security Mode:

There are 11 options, including **Disable, OPEN, SHARED, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPAPSKWPA2PSK, WPA1WPA2,** and **802.1X**.

[EXAMPLE]

Take 802.1x for example. Select 802.1x in the **Security Mode** down-list. The page shown in the following page appears.



Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	WNAP-7200

"WNAP-7200"	
Security Mode	802.1X

802.1x WEP	
WEP	○ Disable ○ Enable

Radius Server	
IP Address	0
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	
Access Policy	
Policy	Disable
Add a station Mac:	

802.1x WEP

WEP:

Disable or enable WEP.

Radius Server

IP Address:

Enter the IP address of Radius Server.

Port:

The default port of the RADIUS server for authentication is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.

Shared Secret:

Enter a password as the key to be shared between the external authentication server and the access point. The key is not send over the network. This key must be the same on the external authentication server and your router.

Session Timeout:

Set the time interval for session. Enter the proper value in the field.

Idle Timeout:

Set the idle time interval. Enter the proper value in the field.

Access Policy

Policy:

There are three options, including Disable, Allow, and Reject. You can choose Disable, Allow or Reject. Select Allow, only the clients whose MAC address is listed can access the router. Select Reject, the clients whose MAC address is listed are denied to access the router.

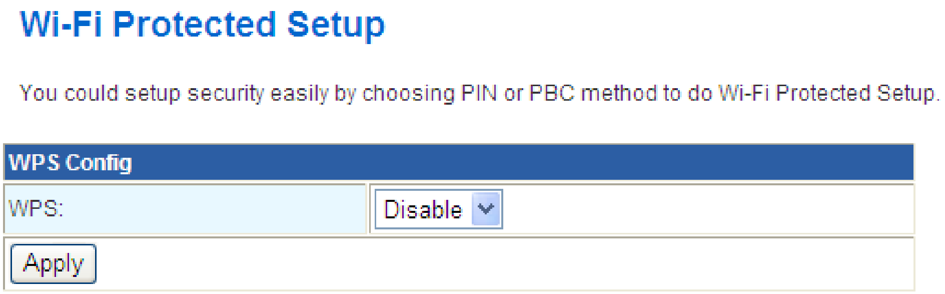
Add a station MAC:

If you want to add a station MAC, enter the MAC address of the wireless station that are allowed or denied access to your router in this address field.

After finishing the settings above, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

4.3.4 WPS

You can enable or disable the WPS function in this page.



Wi-Fi Protected Setup

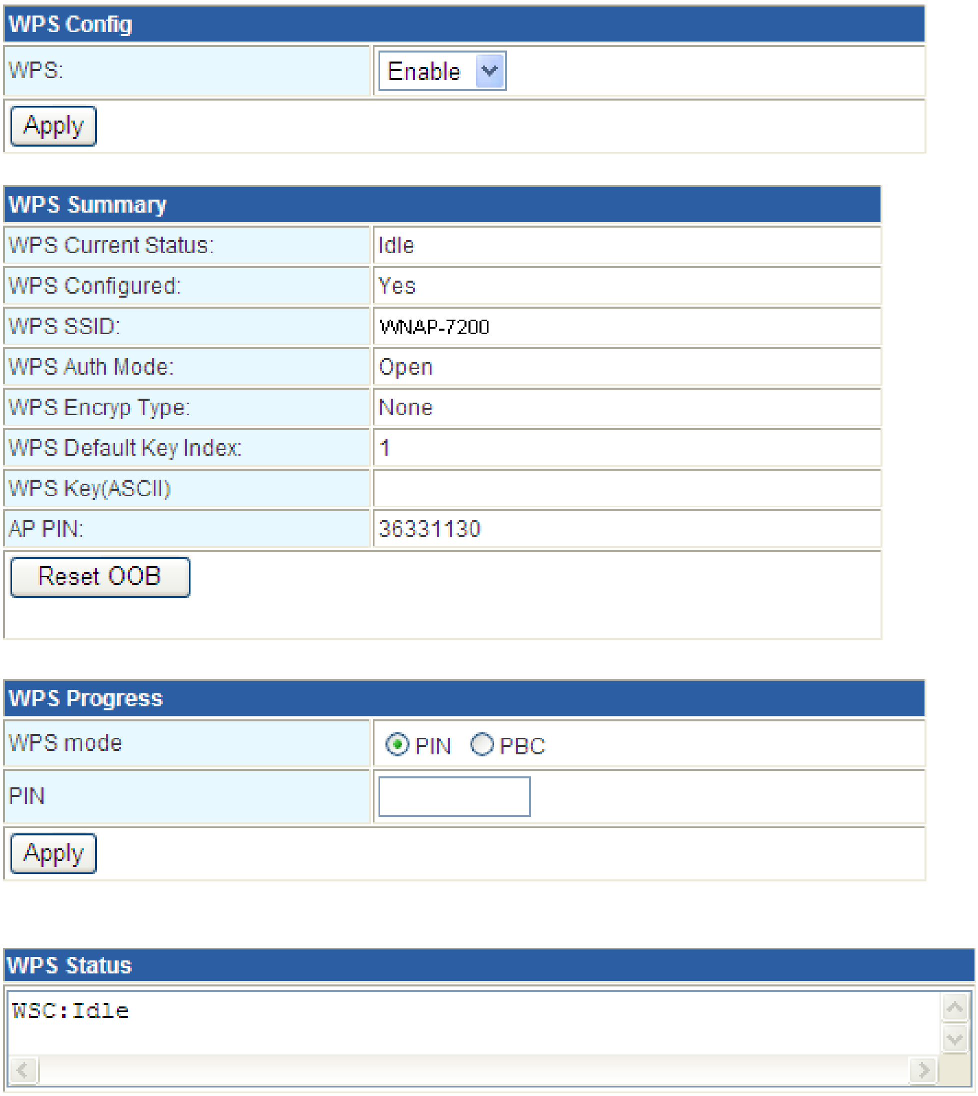
You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Config

WPS:	Disable

Apply

Select **Enable** in the WPS drop-down list. Click **Apply** and the following page appear.



WPS Config

WPS:	Enable

Apply

WPS Summary

WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	WNAP-7200
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	36331130

Reset OOB

WPS Progress

WPS mode	● PIN ○ PBC
PIN	

Apply

WPS Status

```
WSC:Idle
```

WPS Summary

It displays the WPS information, such as WPS Current Status, WPS Configured, and WPS SSID.

Reset OOB:

Reset to out of box (OoB) configuration

WPS Progress

WPS mode:

There are two way for you to enable WPS function: **PIN, PBC**. You can use a push button configuration (PBC) on the Wi-Fi router. If there is no button, enter a 4- or 8-digit PIN code. Each STA supporting WPS comes with a hard-coded PIN code.

PIN:

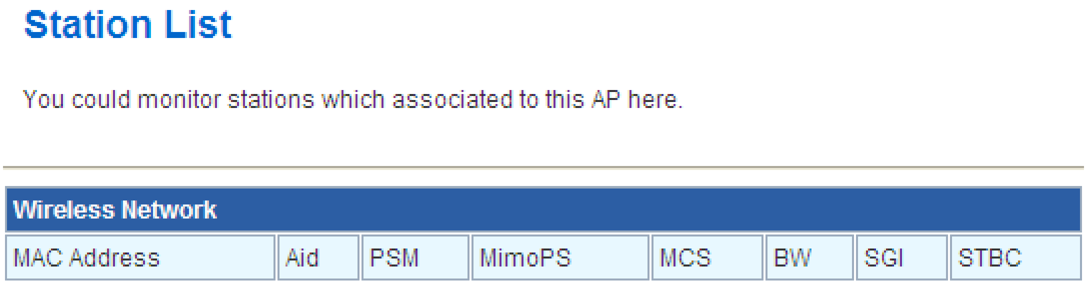
If you select PIN mode, you need enter the PIN number in the field.

WPS Status

It displays the information about WPS status.

4.3.5 Station List

Through this page, you can easily identify the connected wireless stations. It automatically observes the ID of connected wireless station (if specified), MAC address, SSID, and current status.



Station List

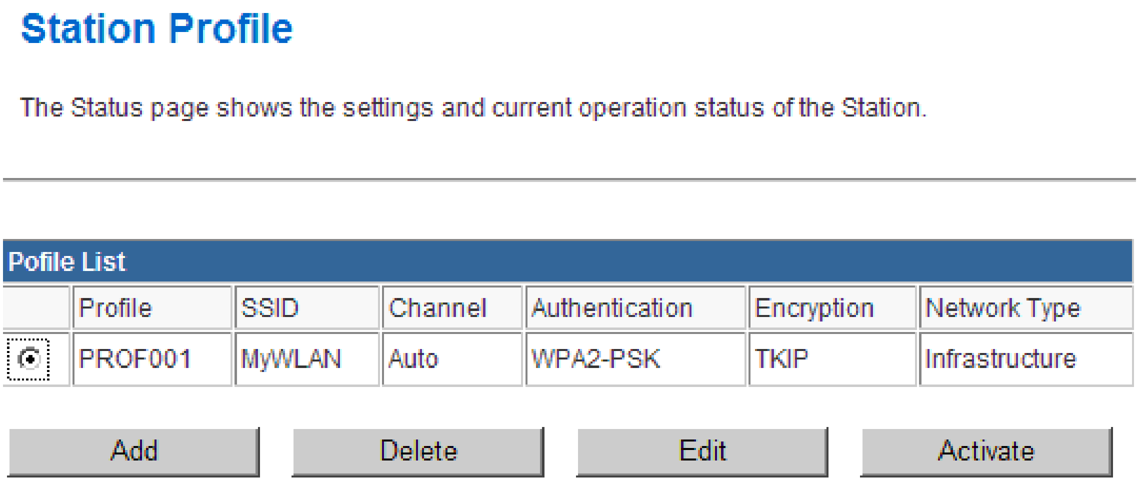
You could monitor stations which associated to this AP here.

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC

4.4 Wireless Settings (Client)

4.4.1 Profile

The Station Profile page shows the settings and current operation status of the station.



Station Profile

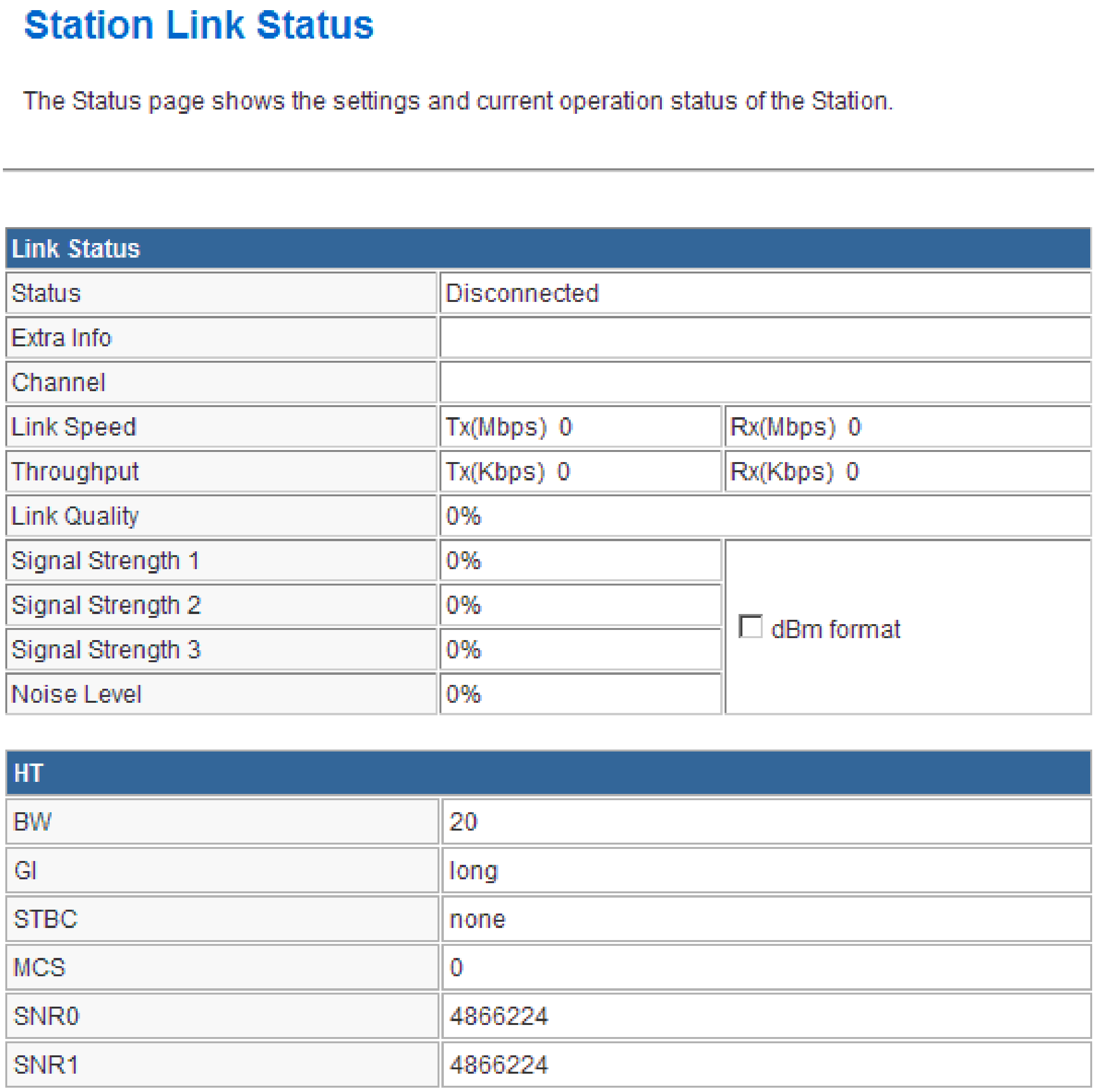
The Status page shows the settings and current operation status of the Station.

Pofile List

	Profile	SSID	Channel	Authentication	Encryption	Network Type
●	PROF001	MyWLAN	Auto	WPA2-PSK	TKIP	Infrastructure

4.4.2 Link Status

The Station Link Status page shows the settings and current operation status of the Station.



Station Link Status

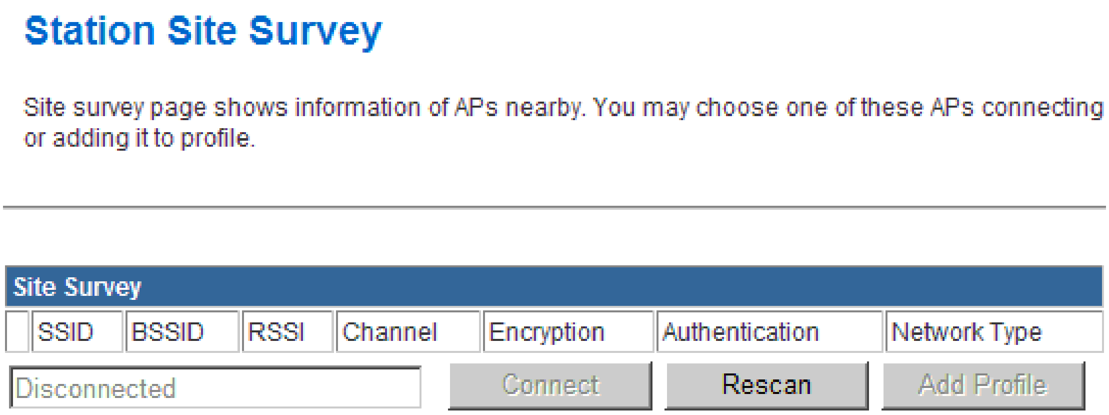
The Status page shows the settings and current operation status of the Station.

Link Status		
Status	Disconnected	
Extra Info		
Channel		
Link Speed	Tx(Mbps) 0	Rx(Mbps) 0
Throughput	Tx(Kbps) 0	Rx(Kbps) 0
Link Quality	0%	
Signal Strength 1	0%	□ dBm format
Signal Strength 2	0%	
Signal Strength 3	0%	
Noise Level	0%	

HT	
BW	20
GI	long
STBC	none
MCS	0
SNR0	4866224
SNR1	4866224

4.4.3 Site Survey

Station Site Survey page can shows information of APs nearby, you can choose one of these APs connecting or adding it to profile.



Station Site Survey

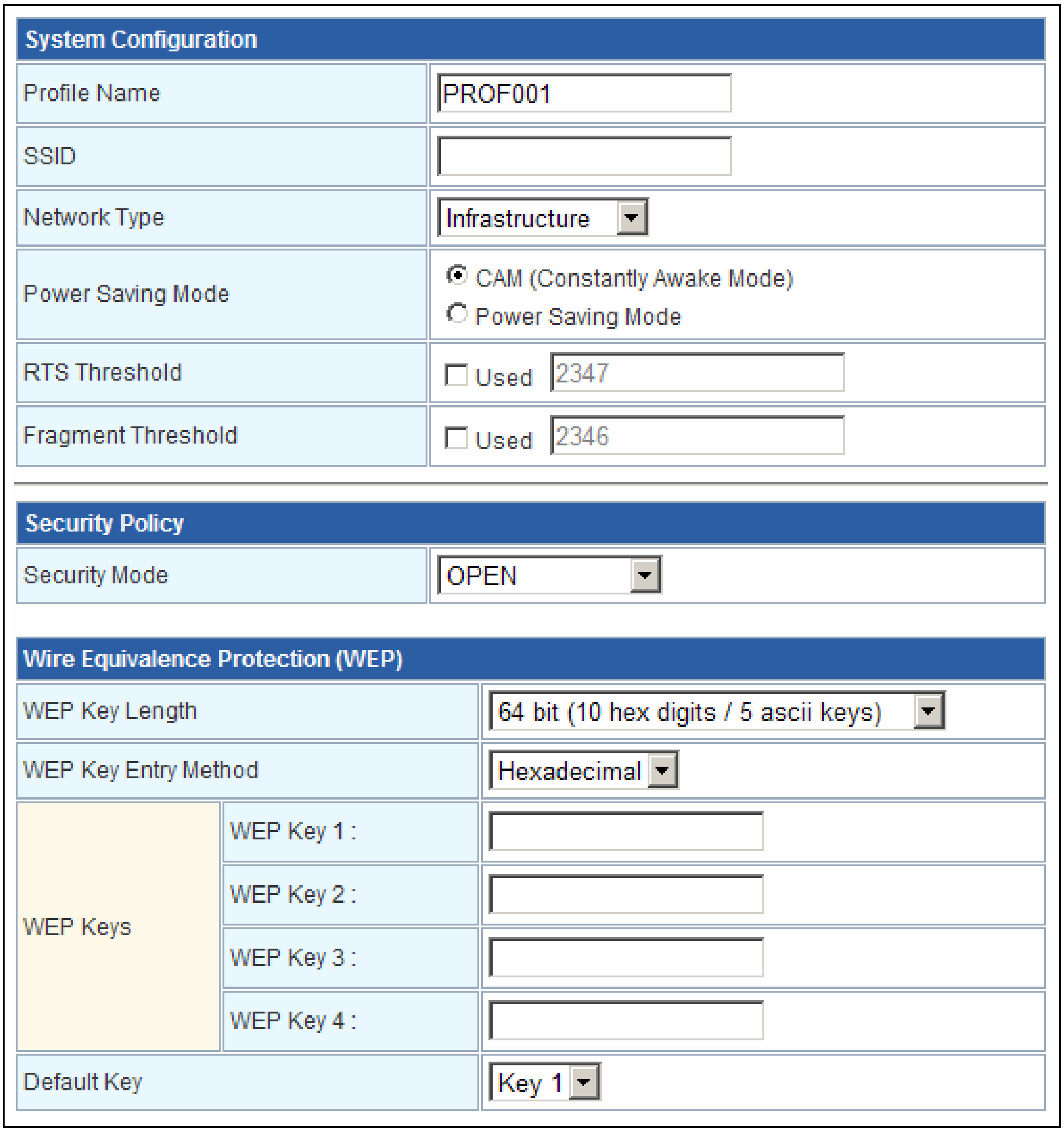
Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

Site Survey

	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Network Type

Disconnected

For adding a profile, choose one AP and click "Add Profile". And you will see the below screen for AP profile configuration. Enter the necessary information and apply the settings.



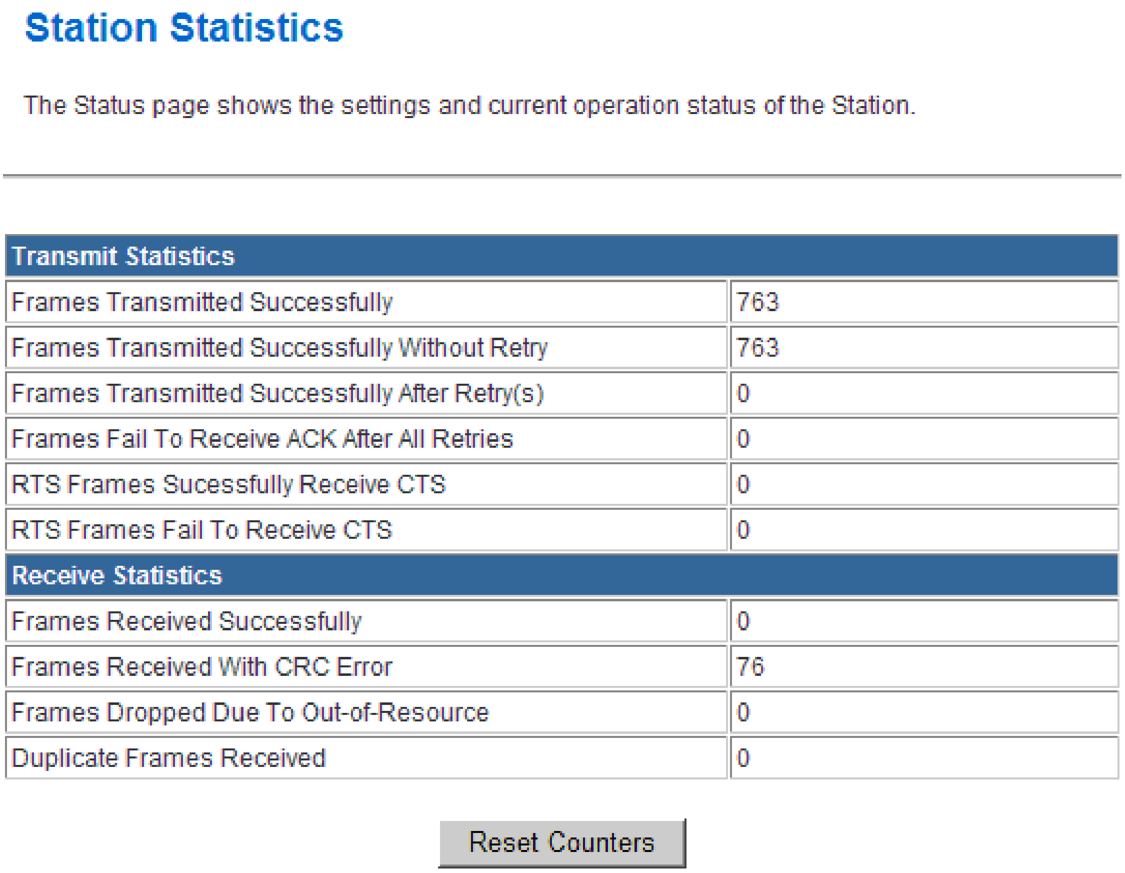
System Configuration	
Profile Name	PROF001
SSID	
Network Type	Infrastructure ▾
Power Saving Mode	● CAM (Constantly Awake Mode) ○ Power Saving Mode
RTS Threshold	□ Used 2347
Fragment Threshold	□ Used 2346

Security Policy	
Security Mode	OPEN ▾

Wire Equivalence Protection (WEP)		
WEP Key Length		64 bit (10 hex digits / 5 ascii keys) ▾
WEP Key Entry Method		Hexadecimal ▾
WEP Keys	WEP Key 1 :	
	WEP Key 2 :	
	WEP Key 3 :	
	WEP Key 4 :	
Default Key		Key 1 ▾

4.4.4 Statistics

The Station Statistics page shows the settings and current operation status of the Station.



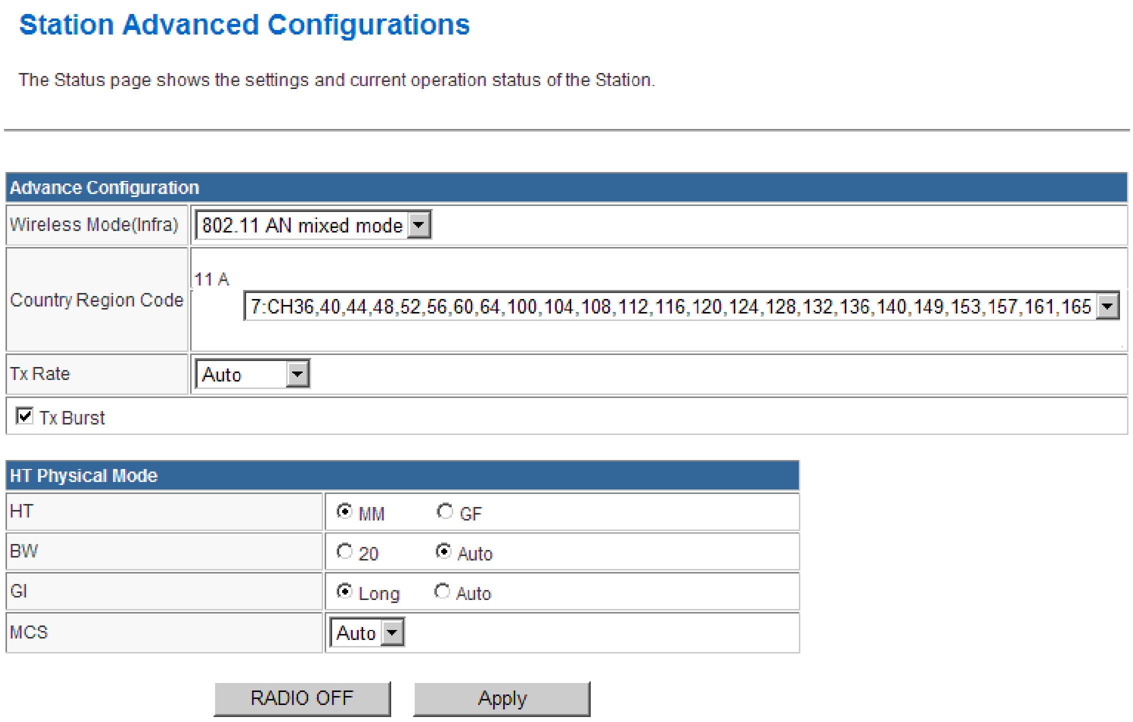
Station Statistics

The Status page shows the settings and current operation status of the Station.

Transmit Statistics	
Frames Transmitted Successfully	763
Frames Transmitted Successfully Without Retry	763
Frames Transmitted Successfully After Retry(s)	0
Frames Fail To Receive ACK After All Retries	0
RTS Frames Sucessfully Receive CTS	0
RTS Frames Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	0
Frames Received With CRC Error	76
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	0

4.4.5 Advance

The Station Advanced Configuration page shows the settings and current operation status of the station.



Station Advanced Configurations

The Status page shows the settings and current operation status of the Station.

Advance Configuration	
Wireless Mode(Infra)	802.11 AN mixed mode ▾
Country Region Code	11 A 7:CH36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,157,161,165 ▾
Tx Rate	Auto ▾
☑ Tx Burst	

HT Physical Mode	
HT	● MM ○ GF
BW	○ 20 ● Auto
GI	● Long ○ Auto
MCS	Auto ▾

Wireless Mode:

Select wireless mode. 802.11a Only, 802.11a/n mix mode are supported.

Country Region Code:

This field displays the region of operation for which the wireless interface is intended.

TX Rate:

Manually force the Transmit using selected rate. Default is auto.

TX Burst:

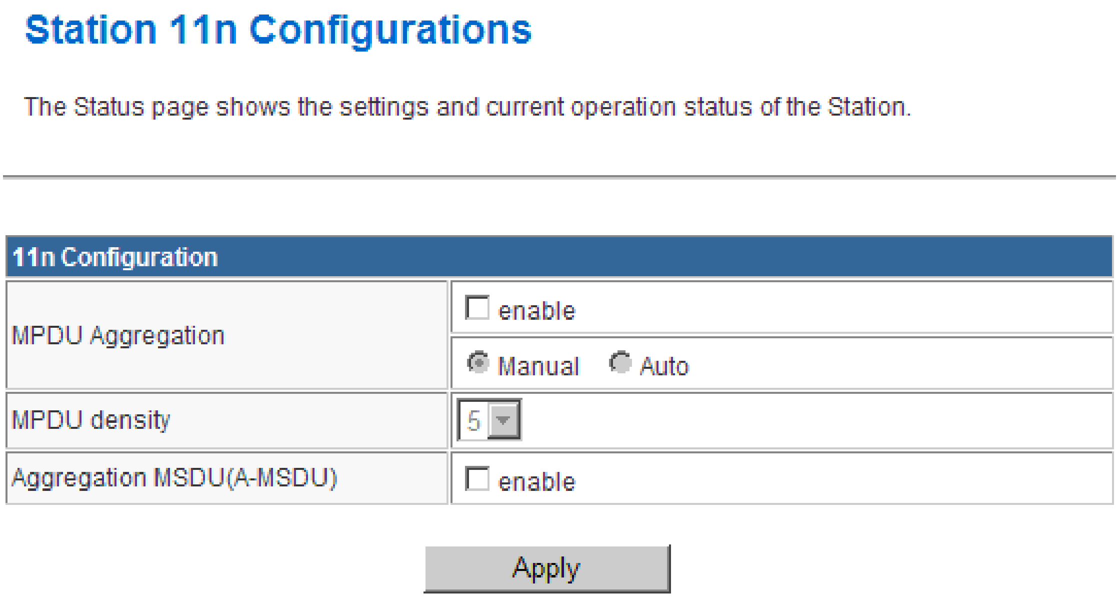
Frame burst mode.

HT Physical Mode:

Configure HT Status in use, containing HT(MM or GF), BW(20 or Auto), GI(Long or Auto), and MCS(0~15, 32, or Auto) settings.

4.4.6 11n Configuration

The Station 11n Configurations page shows the settings and current operation status of the station.



Station 11n Configurations

The Status page shows the settings and current operation status of the Station.

11n Configuration	
MPDU Aggregation	□ enable ● Manual ○ Auto
MPDU density	5
Aggregation MSDU(A-MSDU)	□ enable

MPDU Aggregation:

MPDU stands for MAC Protocol Data Unit. MPDUs are the fragmented units of MSDU, also called MAC frames, encapsulate the higher layer protocol data or contain MAC management messages.

MPDU Density:

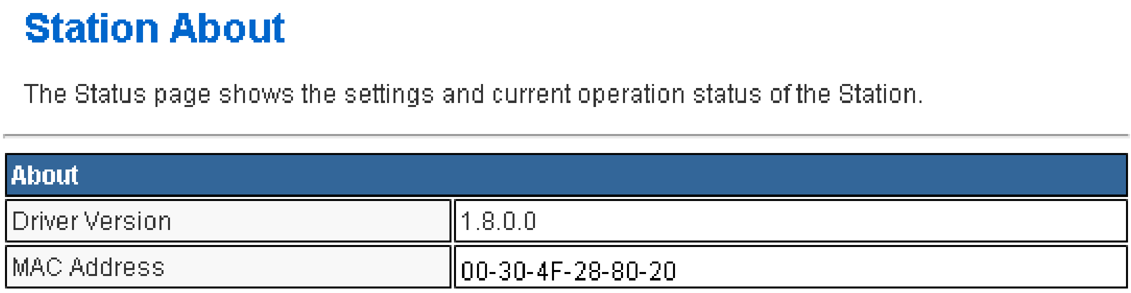
Select 0~7 to configure the MPDU density.

Aggregation MDSU (A-MSDU):

A-MSDU stands for Aggregate MAC service data unit. This option allows aggregation of multiple MSDU in one MPDU. The MSDU is that unit of data that is received from the LLC sub-layer which lies above the MAC sub-layer in a protocol stack. The LLC and MAC sub-layers are collectively referred to as the DLL.

4.4.7 About

The About page shows driver version and MAC address.



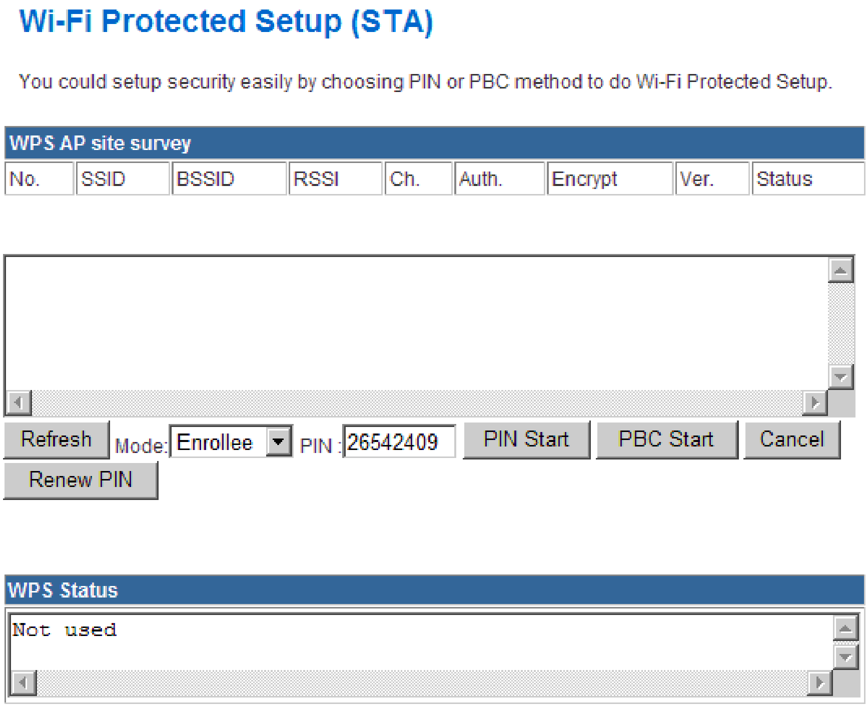
Station About

The Status page shows the settings and current operation status of the Station.

About	
Driver Version	1.8.0.0
MAC Address	00-30-4F-28-80-20

4.4.8 WPS

You can setup security easily by choosing PIN or PBC method to do Wi-Fi Protected setup.



Wi-Fi Protected Setup (STA)

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS AP site survey

No.	SSID	BSSID	RSSI	Ch.	Auth.	Encrypt	Ver.	Status

WPS Status

```
Not used
```

WPS AP Site Survey:

Display the information of surrounding APs with WPS IE from last scan result. List information includes SSID, BSSID, RSSI, Channel, ID (Device Password ID), Auth., Encrypt, Ver., and Status.

Refresh:

Issue a rescan command to wireless NIC to update information on surrounding wireless network.

Mode:

Our station role-playing as an Enrollee or an external Registrar.

PIN:

8-digit numbers. It is required to enter PIN Code into Registrar using PIN method. Each NIC Wireless has only one PIN Code of Enrollee.

PIN Start:

Start to add to Registrar using PIN configuration method. IF STA Registrar, remember that enter PIN Code read from you Enrollee before starting PIN.

PBC Start:

Start to add to AP using PBC configuration method.

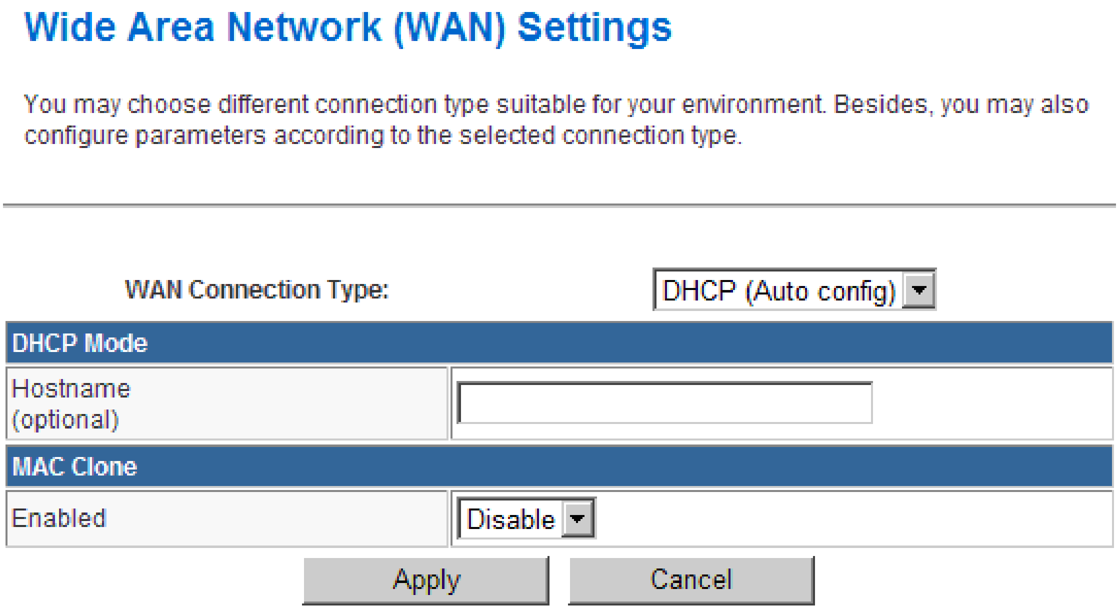
WPS Status:

Display the current status of the WPS function.

4.5 Internet Settings

4.5.1 WAN

The WAN port is the connection of the 802.11n AP Router module to existing broadband device such as Cable modem or ADSL CPE. Click WAN on Internet Setting, below screen will prompt for WAN setting.



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: DHCP (Auto config)

DHCP Mode	
Hostname (optional)	
MAC Clone	
Enabled	Disable

This AP Router supports 5 methods of obtaining the WAN IP Address:

Static IP (fixed IP):

Use static IP address to access Network. Your ISP will provide a static IP address.

DHCP (Auto Config):

Automatic gets IP address from your ISP.

PPPoE (ADSL):

PPPoE is a common connection type used for xDSL.

PPTP:

PPP Tunneling Protocol can support multi-protocol Virtual Private Network (VPN).

L2TP:

Layer 2 Tunneling Protocol can support multi-protocol Virtual Private Networks (VPN)

4.5.2 LAN

When the module operates in the Gateway mode, it supports the NAT (NAPT) feature. It means the WAN and LAN interfaces are located in different network segments and therefore the date traffic needs to be routed between the two interfaces.

To communicate with 802.11n router properly, must assign an IP address to the LAN port of the user's PC. There are two ways to assign a proper IP address to the user PC's LAN port:

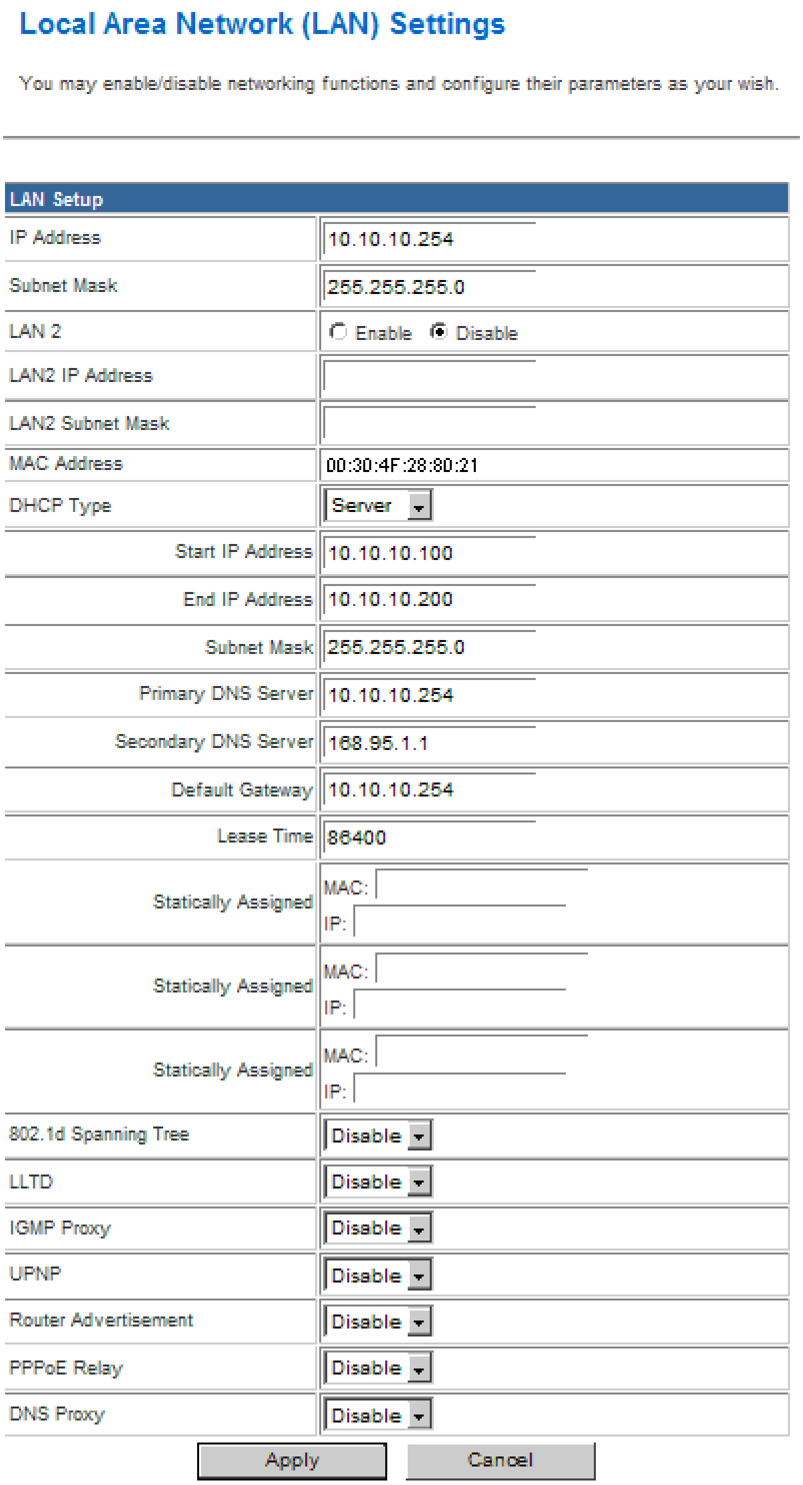
Manual configuration of the user PC:

This required if the user configures the 802.11n router WAN port with a static IP address.

Dynamic IP assignment with DHCP:

802.11n router can act as a DHCP server which dynamically assigns an IP address to user's PC located in the LAN-side network.

Click **LAN** on Internet Settings, below screen will prompt for LAN setting.



Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	10.10.10.254
Subnet Mask	255.255.255.0
LAN 2	○ Enable ● Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	00:30:4F:28:80:21
DHCP Type	Server
Start IP Address	10.10.10.100
End IP Address	10.10.10.200
Subnet Mask	255.255.255.0
Primary DNS Server	10.10.10.254
Secondary DNS Server	168.95.1.1
Default Gateway	10.10.10.254
Lease Time	86400
Statically Assigned	MAC: IP:
Statically Assigned	MAC: IP:
Statically Assigned	MAC: IP:
802.1d Spanning Tree	Disable
LLTD	Disable
IGMP Proxy	Disable
UPNP	Disable
Router Advertisement	Disable
PPPoE Relay	Disable
DNS Proxy	Disable

LAN IP Address:

The LAN IP address. Default: 192.168.0.1

Subnet Mask:

The LAN net-mask. Default: 255.255.255.0

DHCP Type:

Select Disable to disable this Router to distribute IP address. Select Server to enable this Router to distribute IP addresses (DHCP server). And the following field will be activated for you to enter this starting IP address.

Start IP address:

Specify the starting IP address of the IP address pool. Default Start IP: 192.168.0.100.

End IP address:

Specify the ending IP address of the IP address pool. Default End IP: 192.168.0.250.

Lease Time:

Specify the time duration for which the settings will be in effect. Default: 86400 seconds.

802.1d Spanning Tree:

Default: Disable.

LLTD:

Default: Disable.

IGMP Proxy:

Default: Disable.

UPnP:

UPuP is architecture for pervasive peer-to-peer network connectivity of PCs and intelligent devices or appliances, particularly within the home. UPnP builds on Internet standards and technologies, such as TCP/IP, HTTP, and XML, to enable these devices automatically connect with one another and work together to make networking – particularly home networking – possible for more people. Default: Disable. Router Advertisement: Default: Disable.

PPPoE Relay:

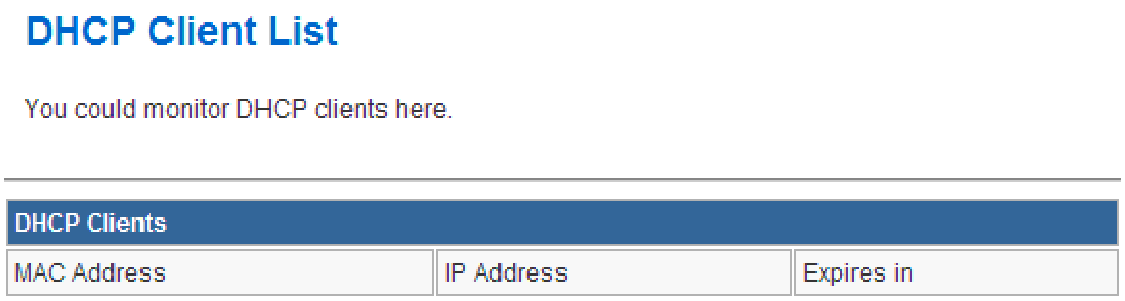
Default: Disable.

DNS Proxy:

Enable the DNS Proxy that will relay users'/clients' DNS requests to a real DNS server IP address. Users no need to specify real DNS server IP address. Default: Enabled.

4.5.3 DHCP Client

DHCP client computers connected to the device will have their information displayed in the DHCP Client List table. The table will show the MAC Address, IP Address and Expired in of the DHCP lease for each client computer.



DHCP Client List

You could monitor DHCP clients here.

DHCP Clients		
MAC Address	IP Address	Expires in

MAC Address:

Shows the client MAC address information.

IP address:

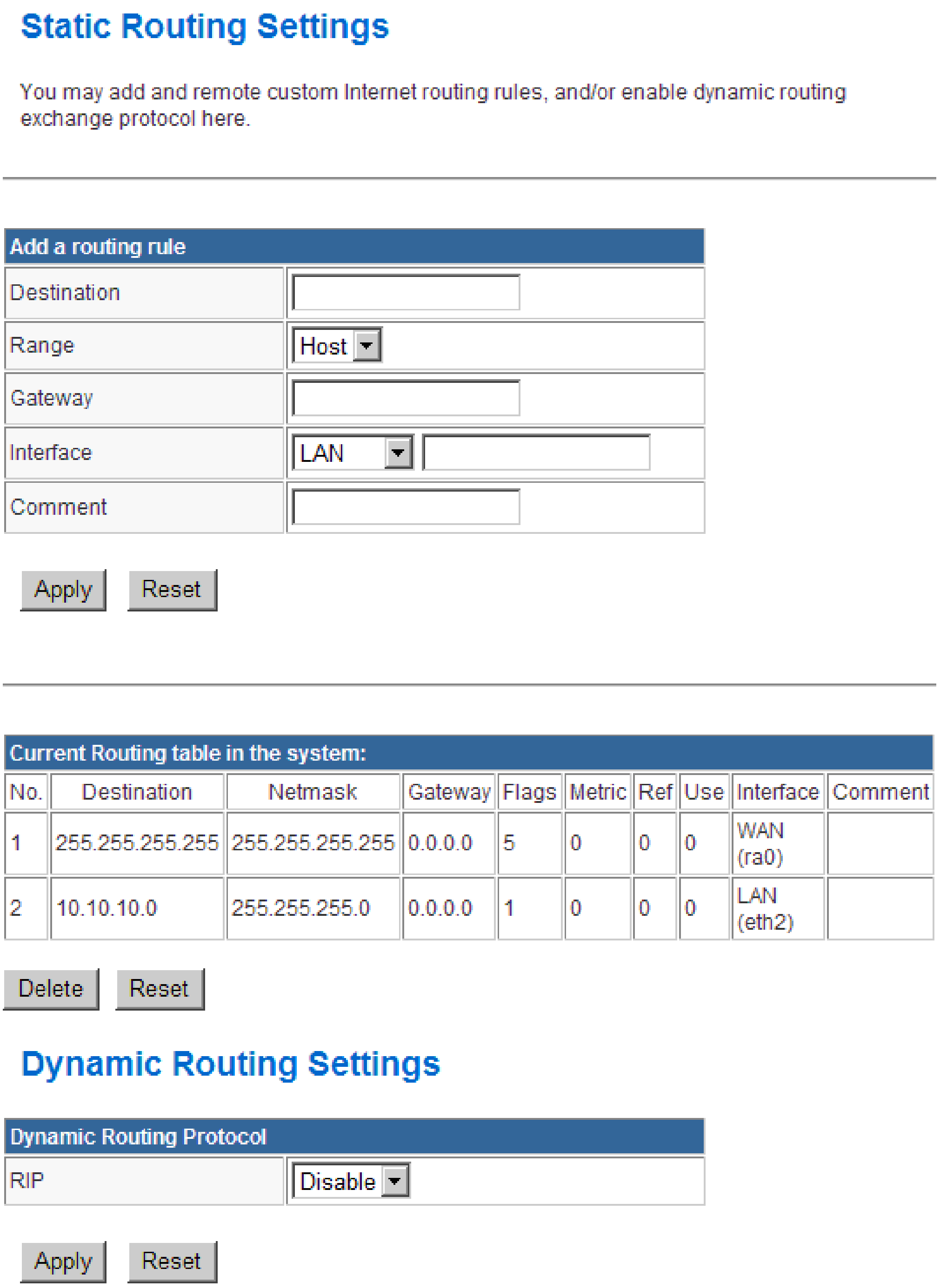
Shows the client IP address information.

Expires in:

Shows the expired time of the client.

4.5.4 Advanced Routing

Static routes are special routes that the network administrator manually enters into the router configuration. The route table allows the user to configure and define all the static routes supported by the router. You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here.



Static Routing Settings

You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here.

Add a routing rule

Destination	
Range	Host
Gateway	
Interface	LAN
Comment	

Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	WAN (ra0)	
2	10.10.10.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (eth2)	

Dynamic Routing Settings

Dynamic Routing Protocol

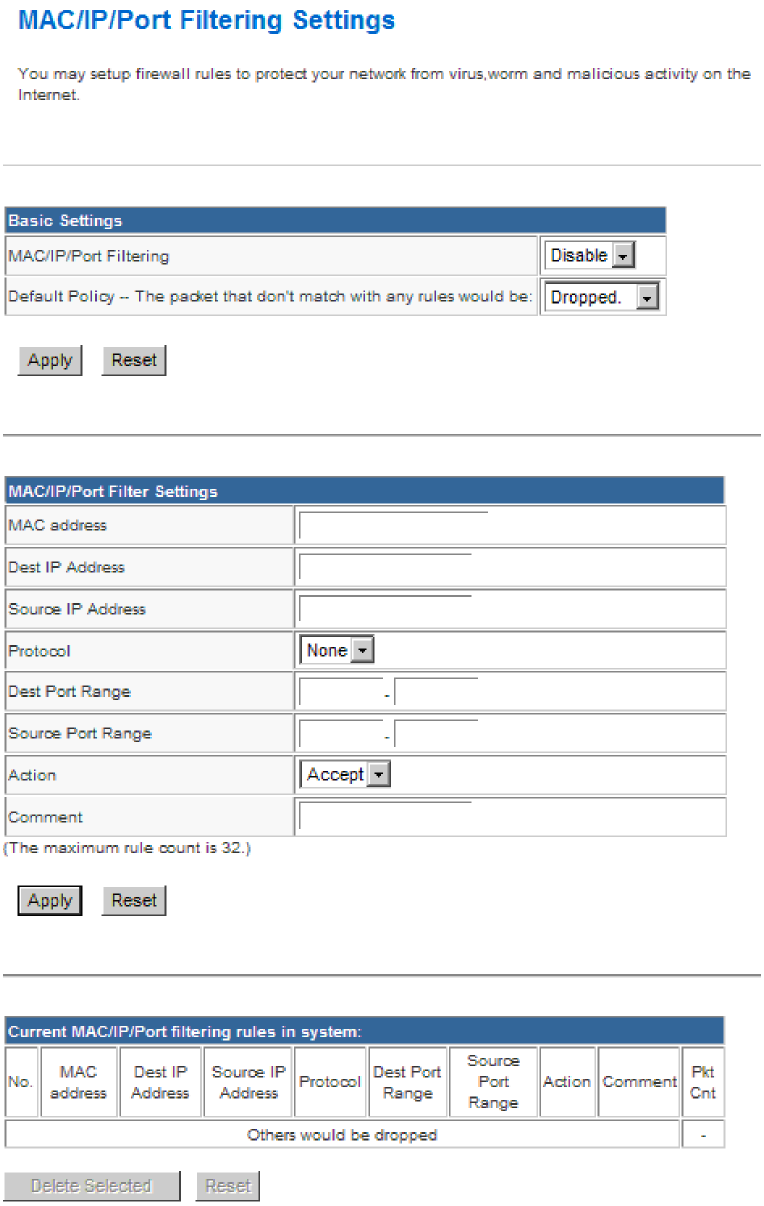
RIP	Disable

4.6 Firewall

The Firewall contains the following sections: MAC/IP/Port Filtering, Port Forwarding, DMZ, System Security Setting, Content Filtering, and Port Trigger.

4.6.1 MAC/IP/Port Filtering

You can setup firewall rules to protect your network from virus, worm and malicious activity on the internet. Filters are used to deny or allow LAN computers from access the Internet. Within the local area network, the unit can be setup to deny Internet access to computers using the assigned IP or MAC addresses. The unit can also block users from accessing restricted web site.



MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus,worm and malicious activity on the Internet.

Basic Settings	
MAC/IP/Port Filtering	Disable
Default Policy -- The packet that don't match with any rules would be:	Dropped.

MAC/IP/Port Filter Settings	
MAC address	
Dest IP Address	
Source IP Address	
Protocol	None
Dest Port Range	-
Source Port Range	-
Action	Accept
Comment	

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:

No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be dropped									-

MAC/IP/Port Filtering:

Enable this function, all list from the filtering will be deny the internet access.

Default Policy:

There have 2 options, Dropped and Accepted.

MAC Address:

The MAC address of the computer in the LAN (Local Area Network) to be used in the MAC filter table. Enter the MAC address of LAN port, e.g. 00:30:4F:88:81:18

Dest IP Address:

The IP address that will be denied to access.

Source IP Address:

The IP address that will be denied access to the Internet.

Protocol: This is the protocol type that will be used with the Port that will be blocked.

Destination Port Range:

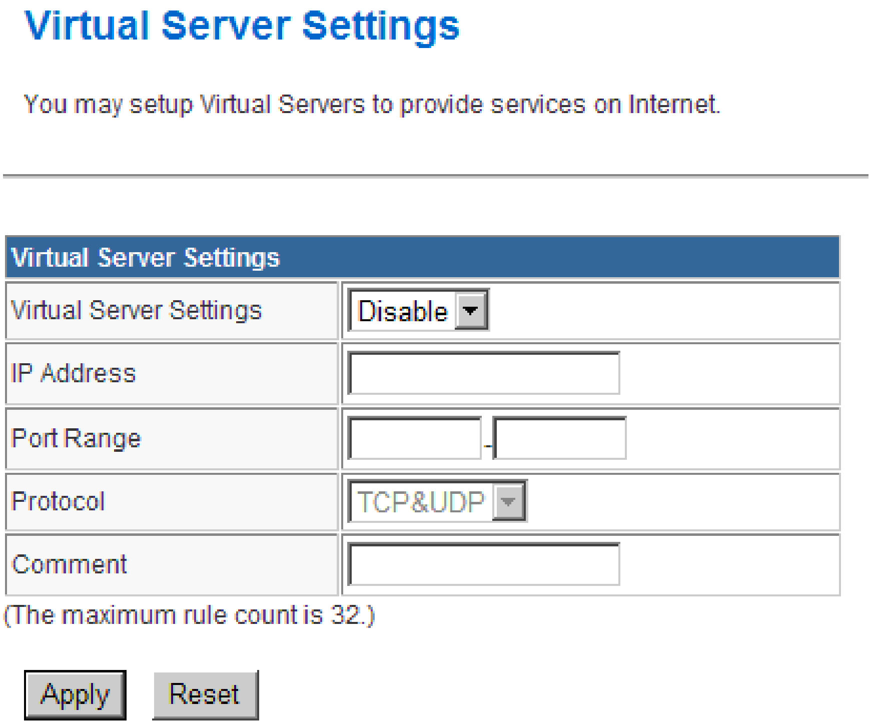
The single port or port range that will be denied to access. If no port is specified, all ports will be denied access.

Source Port Range:

The single port or port range that will be denied access to the Internet. If no port is specified, all ports will be denied access.

4.6.2 Port Forwarding

You may setup virtual servers to provide service on internet.



Virtual Server Settings

You may setup Virtual Servers to provide services on Internet.

Virtual Server Settings	
Virtual Server Settings	Disable ▾
IP Address	
Port Range	-
Protocol	TCP&UDP ▾
Comment	

(The maximum rule count is 32.)

Virtual Server Setting:

Enable/Disable the port forward.

IP Address:

This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

Port Range:

This is the port used to forward the application. It can be either a single port or a range of ports. For the TCP and UDP services enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

Protocol:

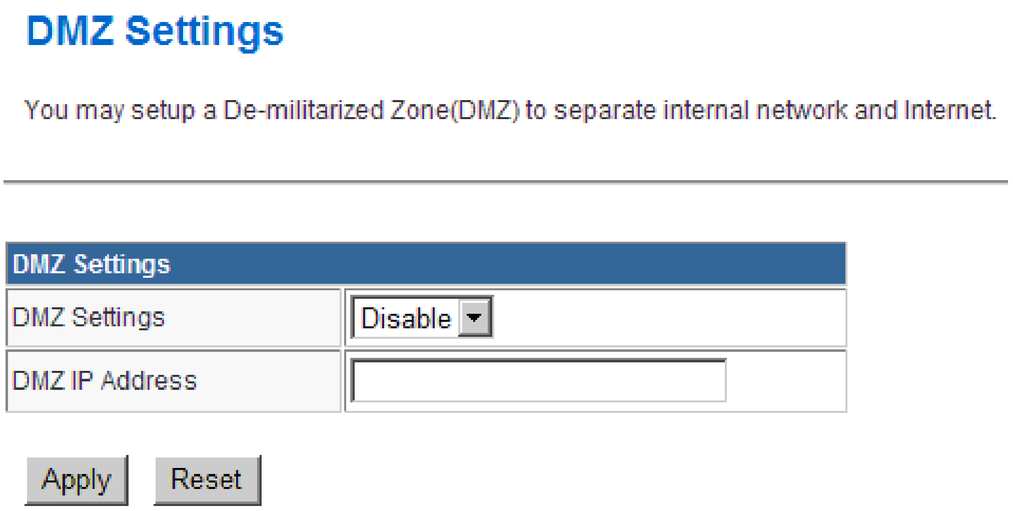
Select the protocol (TCP, UDP, or TCP & UDP) used to the remote system or service.

Comment:

You may key in a description for the IP address.

4.6.3 DMZ

You may setup a De-Militarized Zone (DMZ) to separate internet network and internet.



DMZ Settings

You may setup a De-militarized Zone(DMZ) to separate internal network and Internet.

DMZ Settings	
DMZ Settings	Disable
DMZ IP Address	

DMZ Setting:

If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet/Online game can have two-way connections. Select Enable or Disable from the pull-down menu.

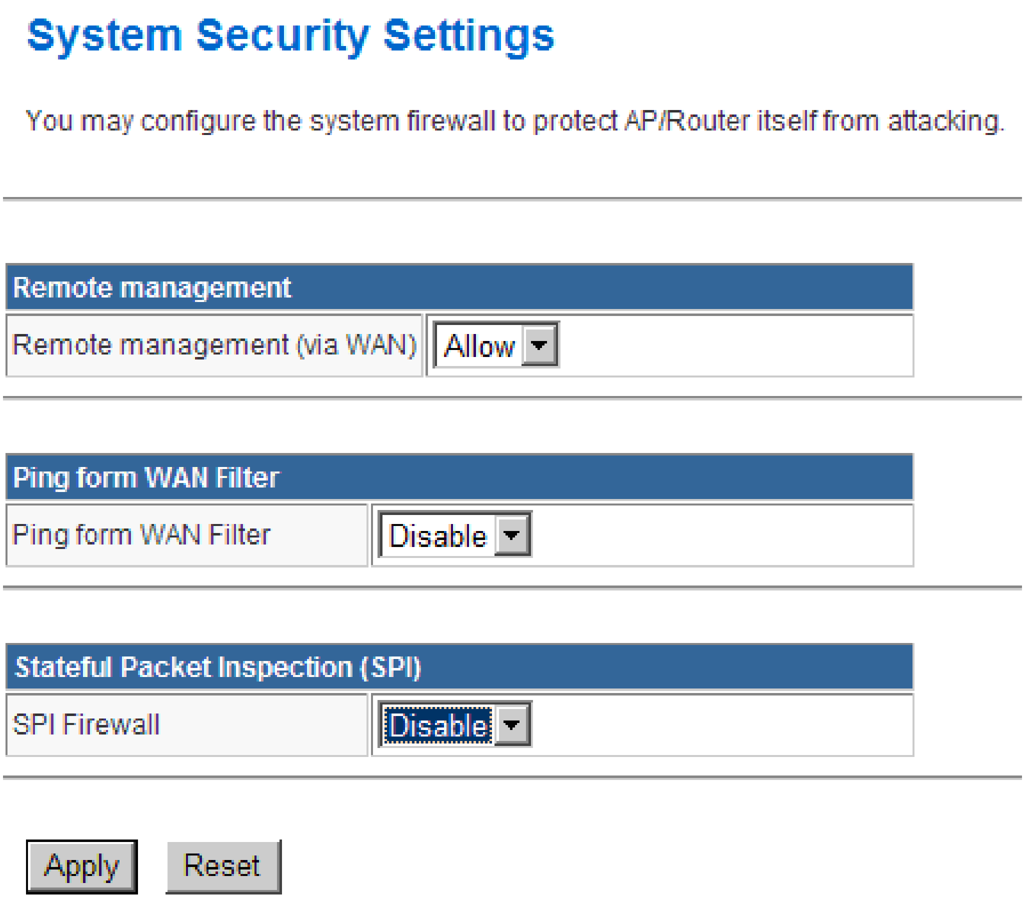
DMZ IP Address:

Enter the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above.

Note: You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

4.6.4 System Security

You may configure the system firewall to protect AP/Router itself from attacking.



System Security Settings

You may configure the system firewall to protect AP/Router itself from attacking.

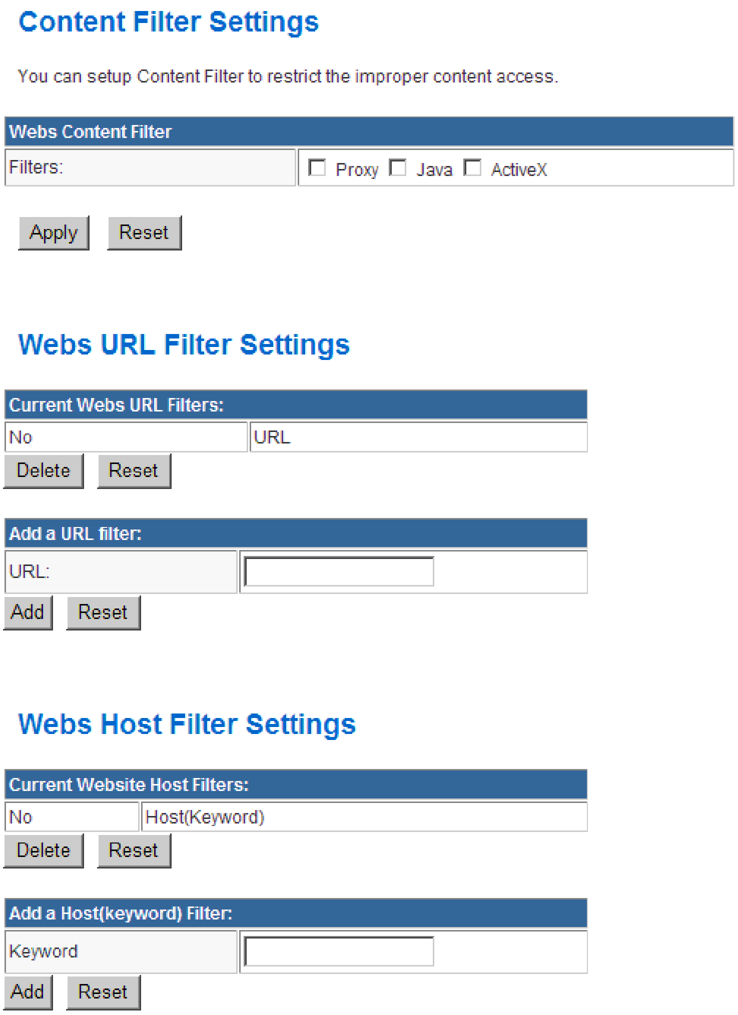
Remote management	
Remote management (via WAN)	Allow

Ping form WAN Filter	
Ping form WAN Filter	Disable

Stateful Packet Inspection (SPI)	
SPI Firewall	Disable

4.6.5 Content Filtering

You can setup content filter to restrict the improper content access.



Content Filter Settings

You can setup Content Filter to restrict the improper content access.

Webs Content Filter	
Filters:	□ Proxy □ Java □ ActiveX

Webs URL Filter Settings

Current Webs URL Filters:	
No	URL

Add a URL filter:	
URL:	

Webs Host Filter Settings

Current Website Host Filters:	
No	Host(Keyword)

Add a Host(keyword) Filter:	
Keyword	

Content Filter Setting:

There have three options for this filter – Proxy, Java, and ActiveX.When those options are checked, the content filter will deny computer from access to the internet by contented those options.

Web URL Filter Setting:

With security reason, the URL Filter provides the enterprise to manage and restrict employee access to non-business or undesirable content on the Internet. URL Filter is a web solution that blocks web-sites access according the URL Filter String no matter the URL string is found full or partial matched with a keyword.

Web Host Filter Settings:

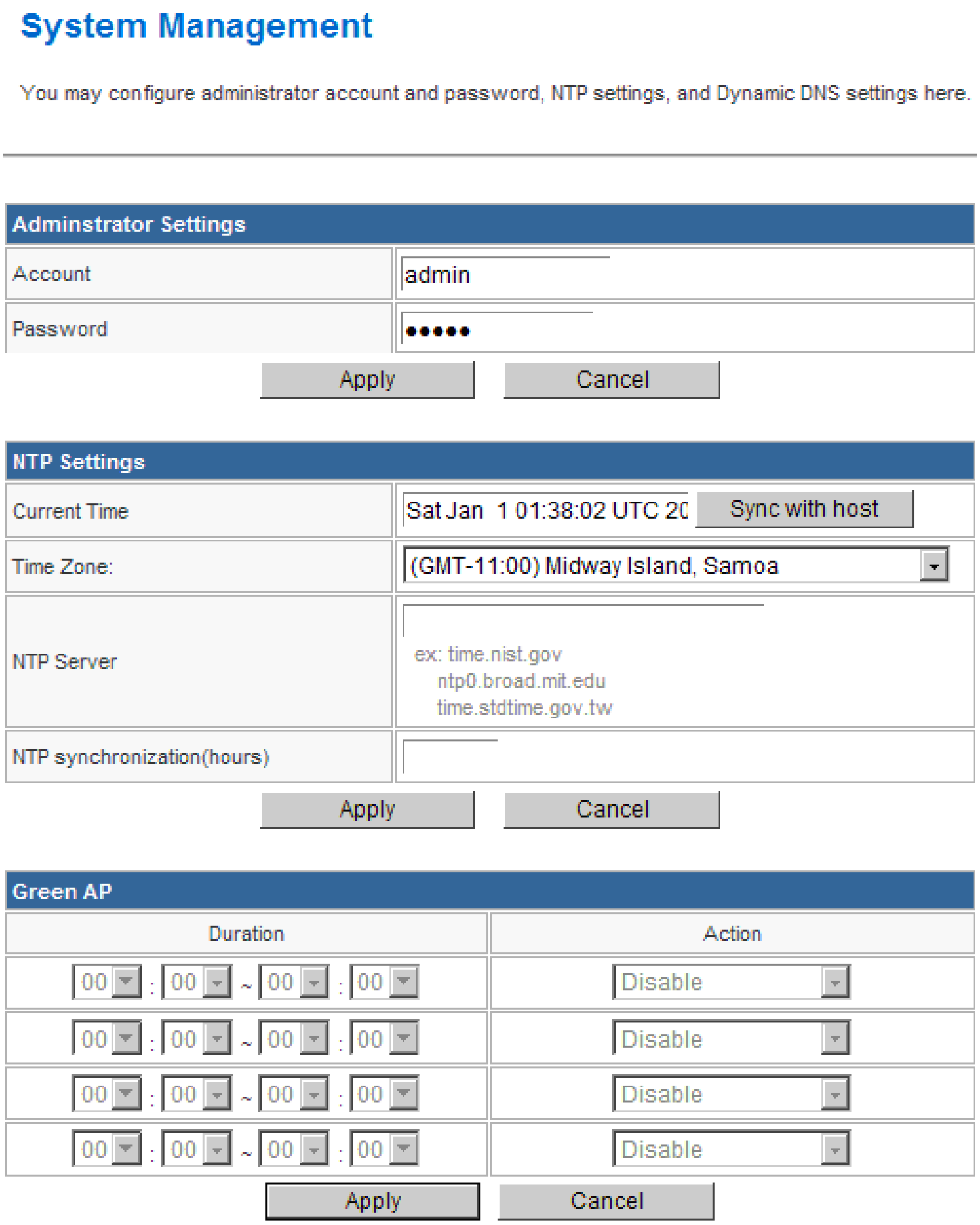
Web Host Filter is a web solution that blocks web-sites access according the Web Host name or partial matched with a keyword.

4.7 Administration

The Administration contains the following sections: Administration, Upload Firmware, Setting Management, Status, Statistics, System Command, and System Log

4.7.1 Management

You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.



System Management

You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.

Adminstrator Settings	
Account	admin
Password	●●●●●

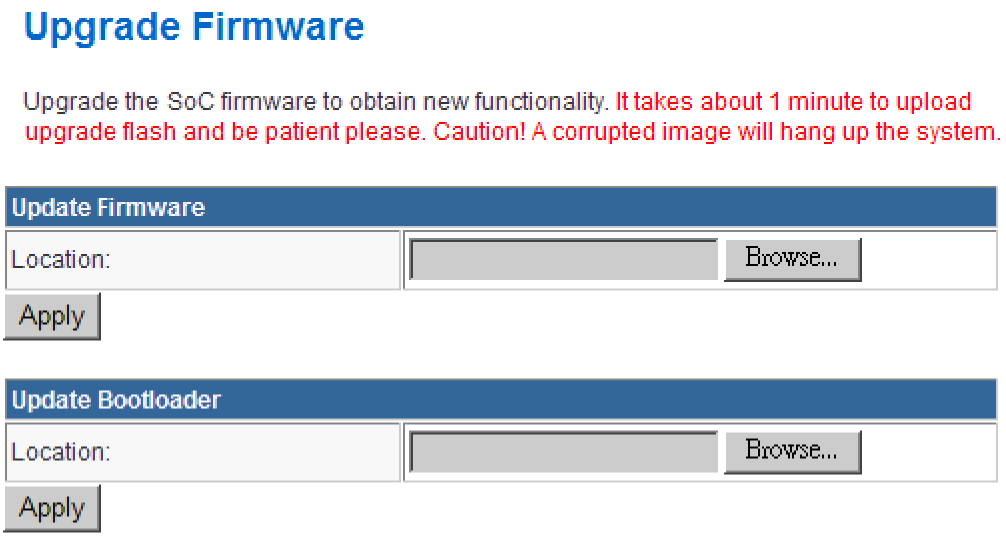
NTP Settings	
Current Time	Sat Jan 1 01:38:02 UTC 20 [Sync with host]
Time Zone:	(GMT-11:00) Midway Island, Samoa
NTP Server	ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
NTP synchronization(hours)	

Green AP	
Duration	Action
00 : 00 ~ 00 : 00	Disable
00 : 00 ~ 00 : 00	Disable
00 : 00 ~ 00 : 00	Disable
00 : 00 ~ 00 : 00	Disable

4.7.2 Upload Firmware

Firmware is the main software image, which the AP Router needs to perform all tasks in real time. Firmware upgrades are required for adding new features or to resolves bugs. It takes about 1 minute to upload/upgrade flash and be patient please.

Caution: A corrupted image will hang up the system.



Upgrade Firmware

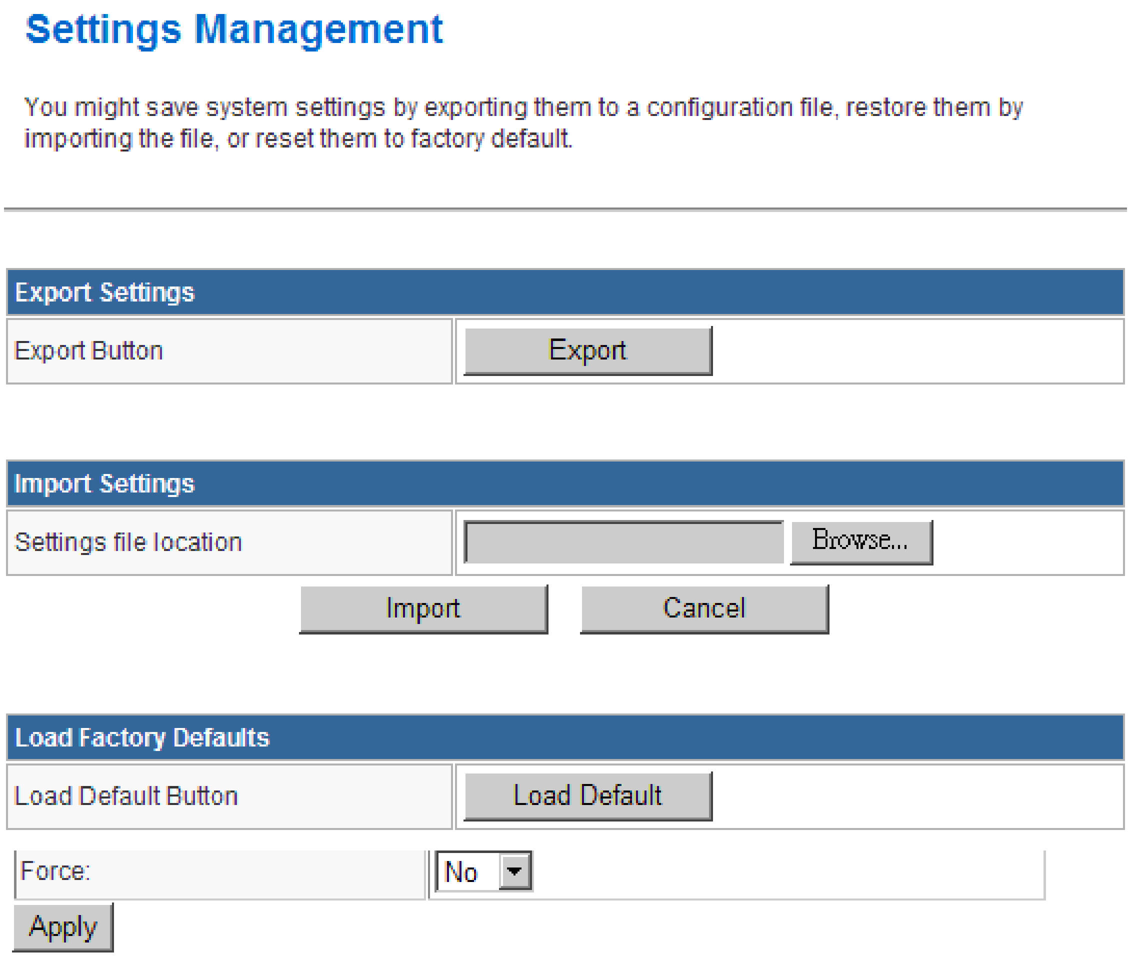
Upgrade the SoC firmware to obtain new functionality. It takes about 1 minute to upload upgrade flash and be patient please. Caution! A corrupted image will hang up the system.

Update Firmware	
Location:	Browse...

Update Bootloader	
Location:	Browse...

4.7.3 Settings Management

You might save system settings by exporting them to configuration file, restore them by import the file, or reset them to factory default.



Settings Management

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

Export Settings	
Export Button	

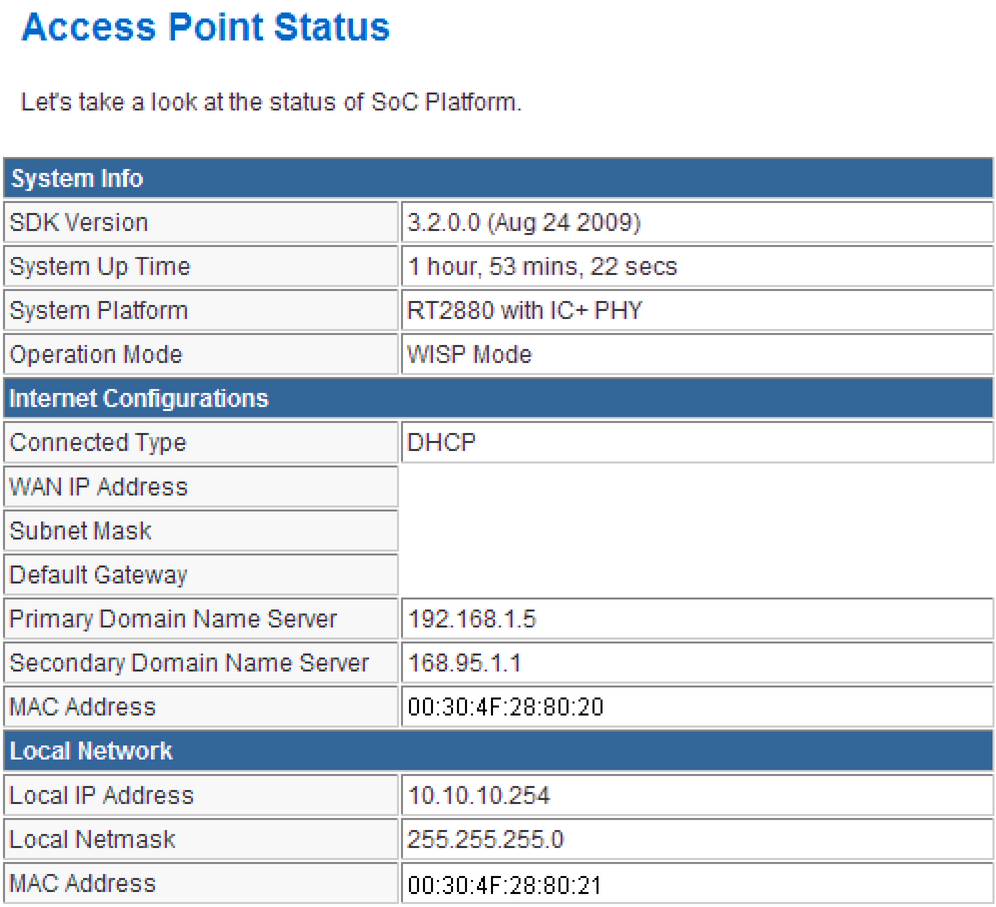
Import Settings	
Settings file location	

Load Factory Defaults	
Load Default Button	

Force:	No

4.7.4 Status

In this section, you can look at the status of this wireless 11n Router, such as System Info, Internet Configurations, and Local Network…etc.



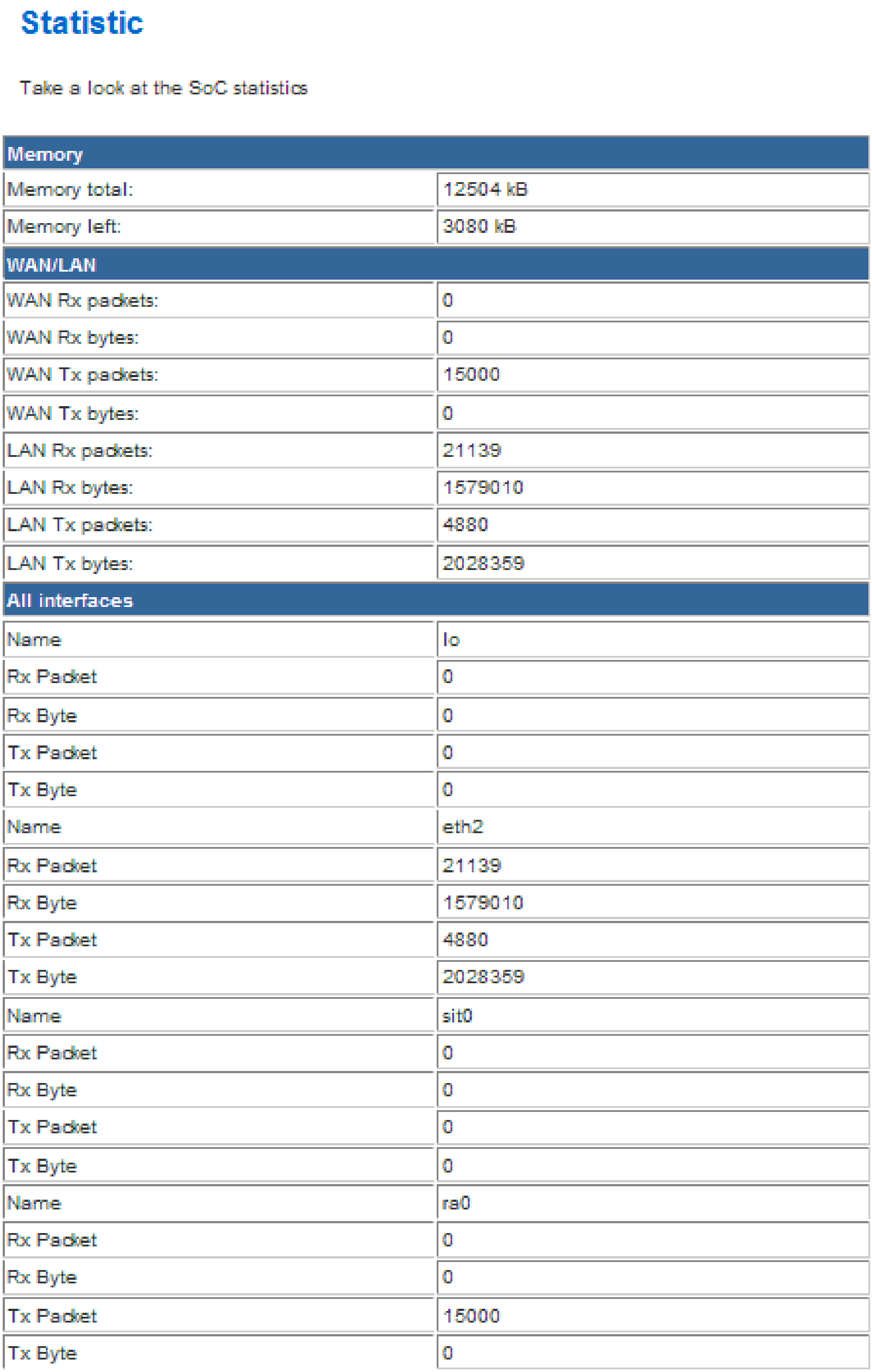
Access Point Status

Let's take a look at the status of SoC Platform.

System Info	
SDK Version	3.2.0.0 (Aug 24 2009)
System Up Time	1 hour, 53 mins, 22 secs
System Platform	RT2880 with IC+ PHY
Operation Mode	WISP Mode
Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	192.168.1.5
Secondary Domain Name Server	168.95.1.1
MAC Address	00:30:4F:28:80:20
Local Network	
Local IP Address	10.10.10.254
Local Netmask	255.255.255.0
MAC Address	00:30:4F:28:80:21

4.7.5 Statistics

In this section, you can look at the statistics of this wireless 11n Router, such as Memory statistics, WAN/LAN's Rx & Tx packets, and all interface statistics…etc



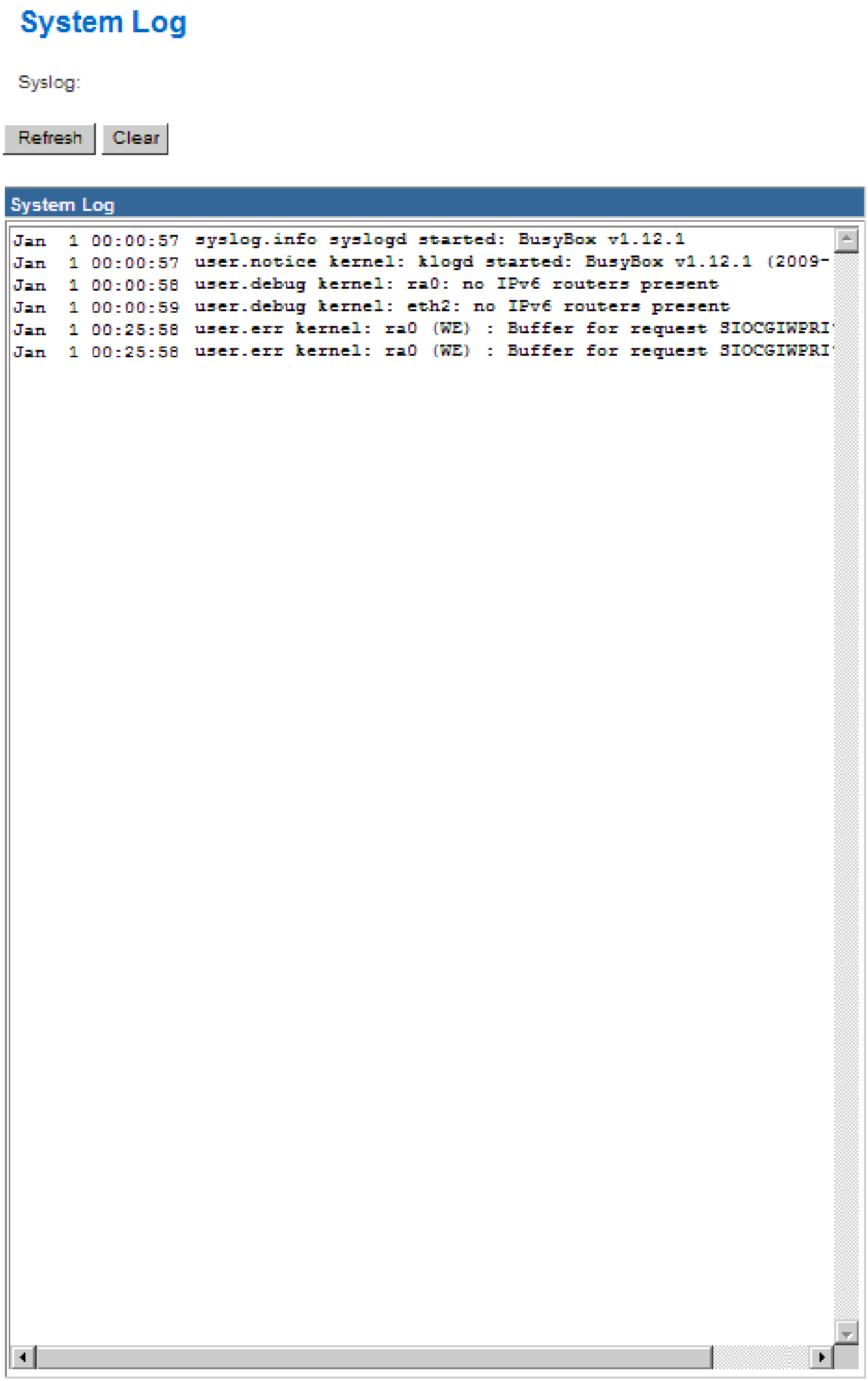
Statistic

Take a look at the SoC statistics

Memory	
Memory total:	12504 kB
Memory left:	3080 kB
WAN/LAN	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	15000
WAN Tx bytes:	0
LAN Rx packets:	21139
LAN Rx bytes:	1579010
LAN Tx packets:	4880
LAN Tx bytes:	2028359
All interfaces	
Name	lo
Rx Packet	0
Rx Byte	0
Tx Packet	0
Tx Byte	0
Name	eth2
Rx Packet	21139
Rx Byte	1579010
Tx Packet	4880
Tx Byte	2028359
Name	sit0
Rx Packet	0
Rx Byte	0
Tx Packet	0
Tx Byte	0
Name	ra0
Rx Packet	0
Rx Byte	0
Tx Packet	15000
Tx Byte	0

4.7.6 System Log

This 802.11n Router supports sending system log (sending UDP packets and keeping log messages in Log Server. Click Refresh on Administration, below screen will prompt for System Log information



```
Jan  1 00:00:57 syslog.info syslogd started: BusyBox v1.12.1
Jan  1 00:00:57 user.notice kernel: klogd started: BusyBox v1.12.1 (2009-
Jan  1 00:00:58 user.debug kernel: ra0: no IPv6 routers present
Jan  1 00:00:59 user.debug kernel: eth2: no IPv6 routers present
Jan  1 00:25:58 user.err kernel: ra0 (WE) : Buffer for request SIOCGIWPRI
Jan  1 00:25:58 user.err kernel: ra0 (WE) : Buffer for request SIOCGIWPRI
```

APPENDIX A. GLOSSARY

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

Adapter - This is a device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

CTS (**C**lear **T**o **S**end) - A signal sent by a wireless device, signifying that it is ready to receive data.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

Download - To receive a file transmitted over a network.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A message included in data packets that can increase wireless efficiency.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firmware - The programming code that runs a networking device.

Fragmentation -Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) - An independent institute that develops networking standards.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Node - A network junction or connection point, typically a computer or work station.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (**R**equest **T**o **S**end) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

Upgrade - To replace existing software or firmware with a newer version.

WEP (**W**ired **E**quivalent **P**rivacy) - An optional cryptographic confidentiality algorithm specified by IEEE 802.11 that may be used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy confidentiality.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

APPENDIX B. TROUBLESHOOTING

This part provides solutions to problems usually encountered during the installation and operation of the WNAP-7200.

The bridges can't successfully associate with each other:

- To make sure the cables is connected properly.
- To check the WNAP-7200 adapter's LED is on or not.
- To check the both Frequency settings are on the same channel or not.
- To check the data rate is matched with one and another through the statistic RSSI display or the advance setting inside the Frequency setting.
- To make sure you use the same encryption key on the both sides or during the bridge link.
- To check the Antenna is aligned appropriately before the Bridge's association.

If you experience the poor performance (high packet loss rate) during the bridge link, it is better for to check the following items:

- To check the range is still inside the Antenna range limitation or not.
- To make sure the Antenna is aligned properly again.
- To make sure if there is no any obstruction in the middle of Line-of-Sight (LOS).
- To be sure there is no radio transmitter too close to the bridge s' Antennas and relocated the Antennas if you have some around.
- To check if you use too close frequency channels to cause the poor link and to set another channel.
- To ping one and another IP address to make sure it will reply or not.

If all recovery measures fail, the bridge still couldn't function properly and take this action as what we recommend:

- Do not open the bridge box by yourself.
- Contact the technical support experts for the troubleshooting.
- If you do open the bridge, you will lose the manufacture warranty.

If Technical Support assistance is required, please prepare the following information ready before you contact us:

- A list of the product hardware (including revision levels), and a brief description of the network structure.
- Details of recent configuration changes, if applicable.

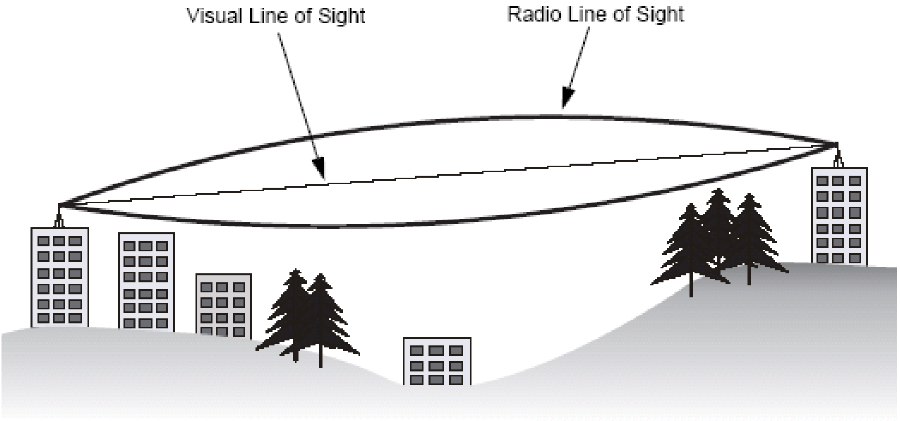
If it appears that more in-depth support is required, have the following information on hand before seeking assistance:

- What you were doing when the error occurred.
- What error messages you saw.
- Whether the problem can be reproduced.
- The serial number of the product.
- The firmware version and the debug information.

APPENDIX C. RF LOS (LINE-OF-SIGHT)

For the wireless communication, the Line-of-Sight (LOS) will be the major issue over building up the wireless link. This evaluated procedure is to reduce the obstructions and to avoid the multiple-path signal degrading the communication quality.
The first requirement is the Line-of-Sight (LOS) between the both sides' Antennas. The radio line-of-sight concept is the area along the radio linking path through which is the bulk of the radio signal power travels. The area is known as the first Fresnel Zone of the radio link. For the radio link, it should avoid to be affected by obstacles in this path, including the ground within 60% of the first Fresnel Zone.

The following figure illustrates the concept of a good radio line-of-sight.



If there is any obstacle in the radio path, it may still be a radio link but the quality and the signal strength will be affected. Ensuring the maximum clearance from objects on a path is important to locate the antennas and the height. For the long-distance links, the radio signals might be lost partially due to the non-LOS issue.

As we setup the radio path for the wireless bridge link, it needs to consider these factors:

- ◆ Avoid any partial line-of-sight between the antennas.
- ◆ Be aware of trees that may be near the path or obstruct the path.
- ◆ Make sure there is enough clearance from buildings and there is no any building or construction blocking the path.
- ◆ Check the land topology between the antennas using topographical maps, aerial photos, or even satellite image data.
- ◆ Avoid a path that may have the temporary blockage due to the moving objects, such as cars, trains, or aircrafts.

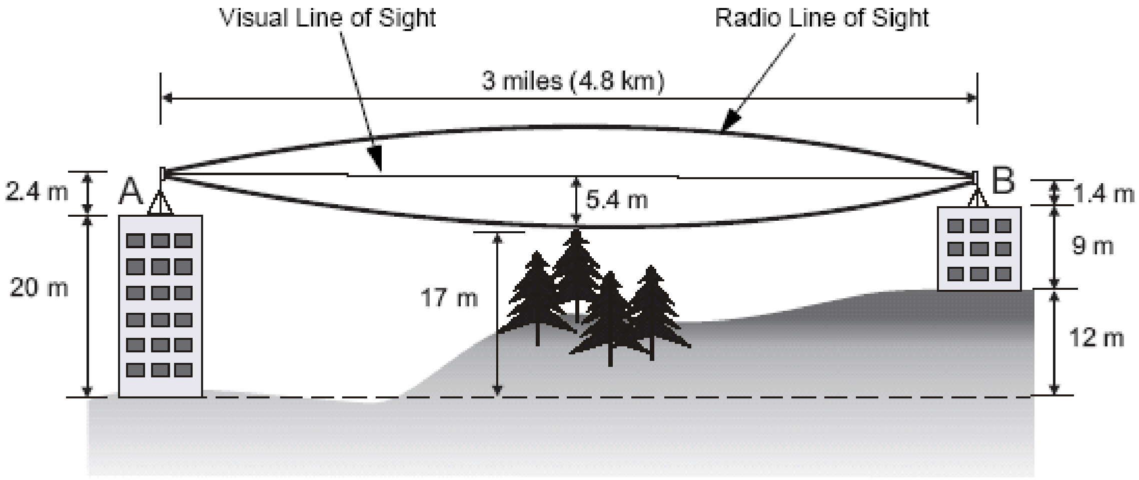
Note:

For the wireless link less than 500 m, the IEEE 802.11a radio signal will tolerate some obstacles in the path and may not even require a visual line of sight between the antennas.

APPENDIX D. ANTENNA HEIGHT

The reliable wireless linkage usually depends on the both sides' antennas for a clear radio line of sight. The minimum height is up to the link distance, obstacles that may be in the path, topology of the terrain, and the curvature of the earth (for links over 2 miles). For the long-distance links, the mast or the pole may need to be constructed to attain the minimum required height. The following table is for you to estimate the required minimum clearance above the ground or path obstruction.

Total link distance	Max clearance for 60% of first Fresnel zone at 5.8GHz	Approximate clearance for earth curvature	Total clearance required at mid-point of link
0.25 mile (402 m)	4.5 ft (1.4 m)	0	4.5 ft (1.4 m)
0.5 mile (805 m)	6.4 ft (1.95 m)	0	6.4 ft (1.95 m)
1 mile (1.6 km)	9 ft (2.7 m)	0	9 ft (2.7 m)
2 mile (3.2 km)	12.7 ft (3.9 m)	1 ft (0.3 m)	13.7 ft (4.2 m)
3 mile (4.8 km)	15.6 ft (4.8 m)	2 ft (0.6 m)	17.6 ft (5.4 m)
4 mile (6.4 km)	18 ft (5.5 m)	3 ft (0.9 m)	21 ft (6.4 m)



For example, the wireless link between the building A and the building B is located three miles (4.8 km) away. There is a tree-covered hill in the mid-way. From the table above, it can be seen that for a three-mile link and the object clearance required at the mid-point is 5.4 m (17.6 ft). The tree-covered hill height is at an elevation of 17 m (56 ft), so the antennas linkage on both sides needs to be at least 22.4 m (73 ft) high. The building A is six stories high or 20 m (66 ft), so the mast or pole with 2.4 m (7.9 ft) must be constructed on its roof to meet the required antenna height. The building B is only three stories high or 9 m (30 ft) but it is located at an elevation that is 12 m (39 ft) higher than the building A. A mast or pole is required to mount an antenna at the required height 1.4 m (4.6ft) on the roof of building B.

PLANET
Networking & Communication

EC Declaration of Conformity

For the following equipment:

*Type of Product: 802.11a/n Wireless LAN Outdoor CPE AP/Router (18dBi Antenna Built-in)
*Model Number: WNAP-7200

* Produced by:
Manufacturer‘s Name : **Planet Technology Corp.**
Manufacturer‘s Address: 11F, No 96, Min Chuan Road,
Hsin Tien, Taipei, Taiwan, R.O.C.

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to 89/336/EEC, 73/223/EEC, 99/5/EEC R&TTE.
For the evaluation regarding the R&TTE the following standards were applied:

ETSI EN 301 489: V1.5.1	(2008-12)
ETSI EN 301 489-1: V1.8.1	(2008-04)
ETSI EN 301 489-17: V1.3.2	(2008-04)
EN 55022	(2006 + A1: 2007)
IEC 60950-1	(2001)
EN 60950-1	(2001 + A11: 2004)

Responsible for marking this declaration if the:

☒ **Manufacturer** □ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname **Alex Tien**

Position / Title : **Product Manager**

Alex

Taiwan **26th Dec., 2009**
Place *Date* *Legal Signature*