TwinMOS Booming

802.11b
Wireless Router

User's Manual

TwinMOS®

Contents

PACKAGE CONTENTS

Unpack your ***Booming AP Router*** kit and verify that all items are present.

- ***Booming*** Wireless Router
- User's Manual (on CD)
- Power Adapter (7.5V/1.1A)
- Antenna

If any of the items described appear to be damaged or missing, please contact your reseller.

INTRODUCTION

Thank you for purchasing the Wireless Router. The Wireless Router is an ideal broadband sharing solution for SOHO and home networks, featuring a wireless LAN function that reduces the necessity of connecting stations via a wired LAN.

The Wireless Router manages all IP address assignments by DHCP, relieving users of the necessity of manually configuring clients for inter-client communication and access to the Internet. A built-in firewall provides extra security from malicious attack.

The intuitive Web browser interface enables users to configure all aspects of the router, including making LAN, WAN, and WLAN settings, making access restrictions, setting administrative and user passwords.

This ***Booming Wireless Router*** supports following features：

- Compatible with IEEE 802.11b Direct Sequence high data rate specifications.
- Supports high-speed wireless connections up to 11 Mbps
- Easy setup through a Web browser on any operating system that supports TCP/IP.
- 10 Mbps WAN port connection to xDSL/Cable modem.
- Four 10/100 Mbps Ethernet switch ports.
- DHCP for dynamic IP configuration, and DNS for domain name mapping.
- 64/128-bit Wired Equivalent Privacy (WEP) data encryption.
- Web-based firmware upgrade

Description of Hardware

Front Panel

The front panel provides LED's for device status. Refer to the following table for the meaning of each feature.

LED	State	Color	Meaning
Power	On	Green	The device is receiving power.
	Off	—	The device is not receiving power.
WLAN Link	On	Green	Indicates that the device is connected to WLAN.
WLAN Tx/Rx	On	Red	Indicates WLAN status.
	Blinking	Red	Indicates WLAN traffic.
10/100	On	Red	Indicates link speed(10/100 Mbps)
Act	On	Green	Link is established.
	On	Flashing Green	Packet transmit or receive activity.
	Off	—	No link activity.

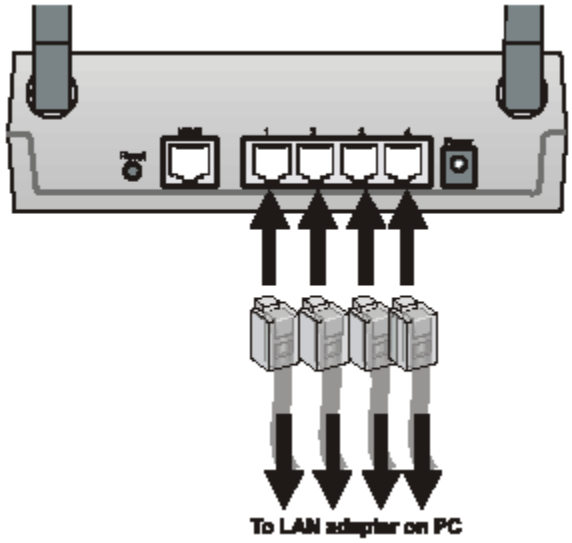
Rear Panel

Item	Description
LAN ports	The four RJ-45 Ethernet ports allow you to con-nect client PCs or LAN hubs to the Wireless Router.
WAN port	WAN port (RJ-45). Connect your Cable modem, xDSL modem, or an Ethernet router to this port.
Power port	Connect the included power adapter to this inlet. **Warning:** The included power adapter is DC 7.5V/1.1A. Using the wrong type of power adapter may cause damage.
Antenna	Two antennas provide wireless LAN functionality and ensure optimal signal strength.
Reset button(Side)	Use this button to reset the power and restore the default factory settings by pressing this button for five seconds.

Basic Installation Procedure

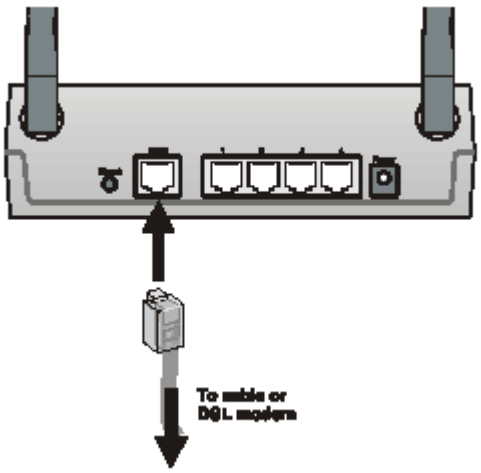
Connecting the Router to the LAN

You can connect the WLAN 11b Router to your PC, a hub, or a switch. Run the Ethernet cable from one of the LAN ports on the rear of the WLAN 11b Router to your computer's network adapter or to another network device. You can also connect the WLAN 11b Router to your PC or to a client adapter via radio signals. Position one antenna on the back of the WLAN 11b Router into the desired positions.



Connecting the Router to the WAN

Prepare an Ethernet cable for connecting the WLAN 11b Router to a Cable/xDSL modem or Ethernet router.

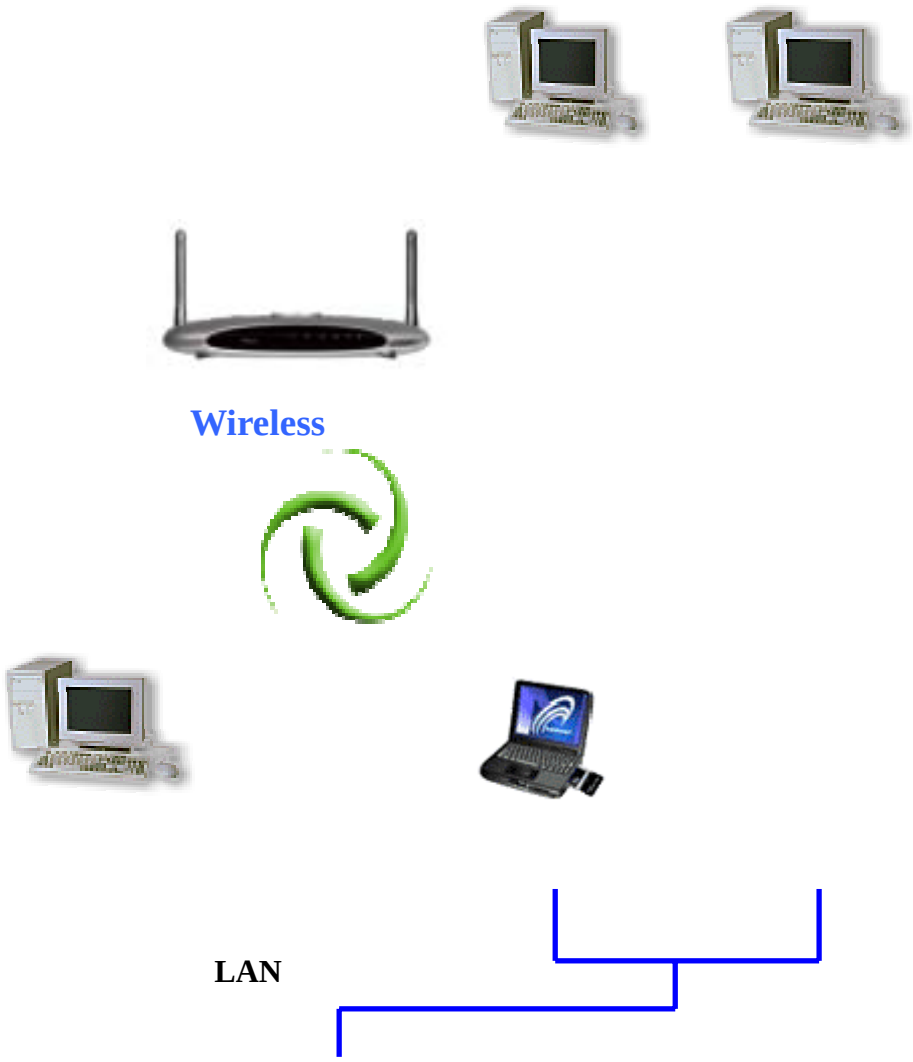


Power On

Connect the power adapter to the WLAN 11b Router.

SOHO/Home Networking

Office Networking



CONNECTING THE AP ROUTER

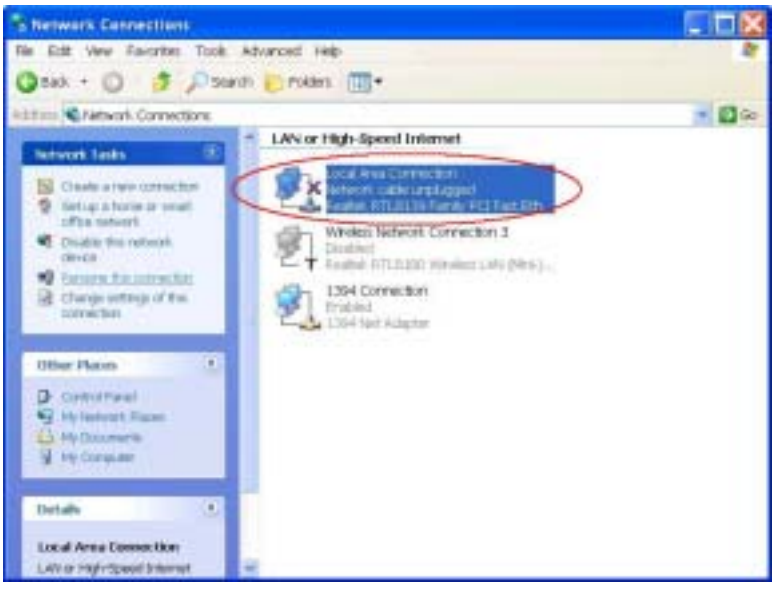
Follow the procedure below to connect the AP Router.

LAN connecting

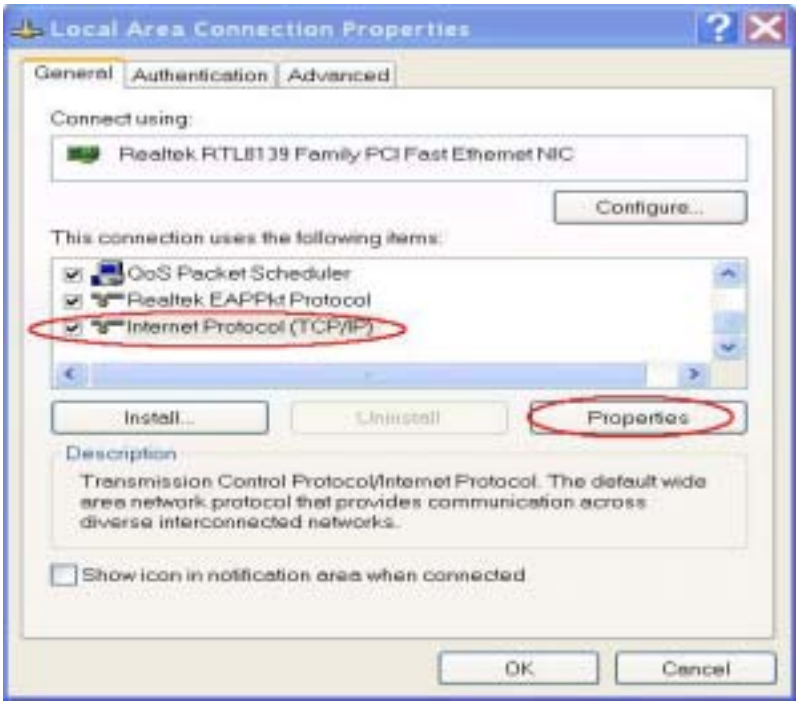
- **Plug a Ethernet cable into a free LAN port at the rear of the router. Plug the other end of the cable into the RJ-45 port on your computer.**
- **Turn on power supply for AP Router.**
- **Setting TCP/IP to work with the AP Router.**
  - **Windows XP**

1. Click **Start**, **Settings**, then click **Control Panel**. The Control Panel opens:

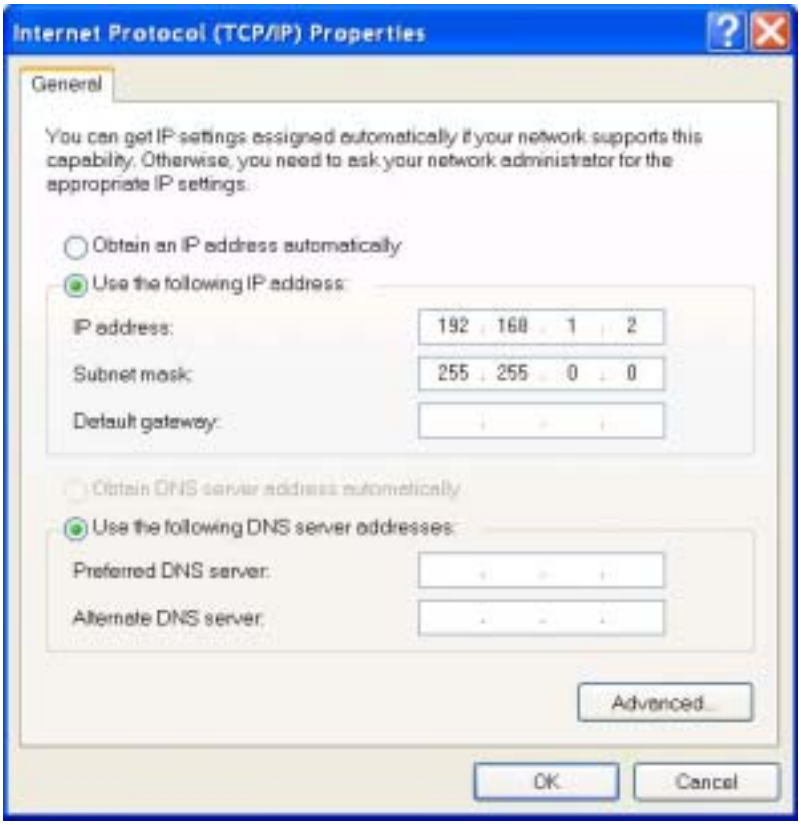
2. Right-click the **Network** icon and select Open to open the Network Connections dialog:



3.Right- click the appropriate LAN connection and click Properties to open the properties dialog for the connection:



4. Check the box next to Internet Protocol (TCP/IP) and click Properties:



5.Assign a IP address, follow these steps:

a. In the TCP/IP Properties dialog box, click the radio button next to **Use the following IP address**:

b. Enter an IP address in the IP field. In the example shown, IP addresses is ***192.168.1.X***(Where X means 2-253)

c. Type a Subnet Mask value is **255.255.0.0.**

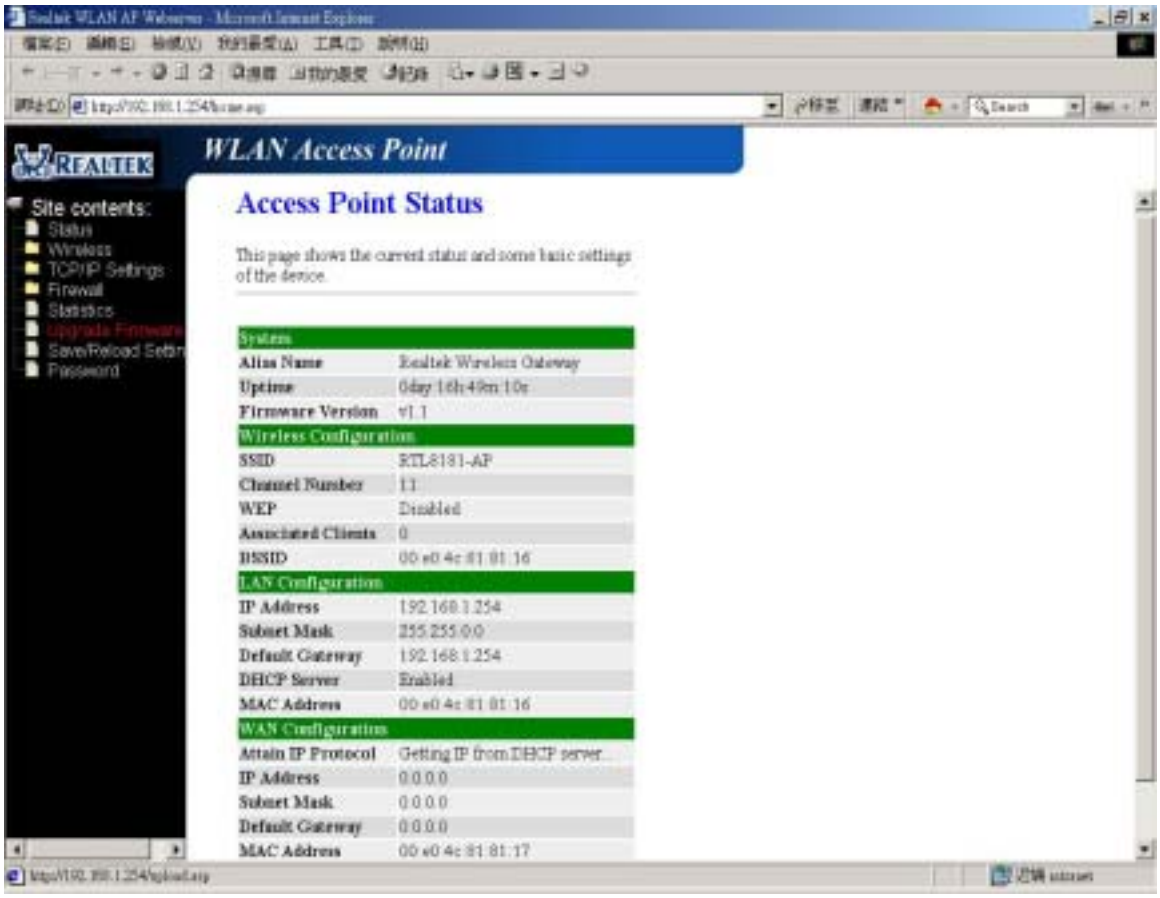
d. Type the router's IP address in the "Default gateway" field.

e. Check the radio button next to "Use the following DNS server addresses" and type the ISP do-main name server IP address.

f. Click **OK**. You are returned to the Network configuration dialog box.

6. Click **OK** to apply the settings and exit the Network configuration dialog box.

- **Open your Web browser and type the router IP address in the address bar. The Router default IP address is *192.168.1.254.***



Wireless connecting

- **Turn on power supply for AP Router.**
- **Insert 802.11b wireless LAN card to your PC.**
- **Setup your wireless utility. The SSID is "RTL8181-AP",WEP off, Infrastructure mode.**
- **Setting TCP/IP to work with the AP Router.**
- **Open your Web browser and type the router IP address in the address bar. The Router default IP address is *192.168.1.254*.**

WEB MANAGEMENT SETTINGS

Before using the Web browser interface, be sure you have set up your computer's network configuration. Refer to page 7.

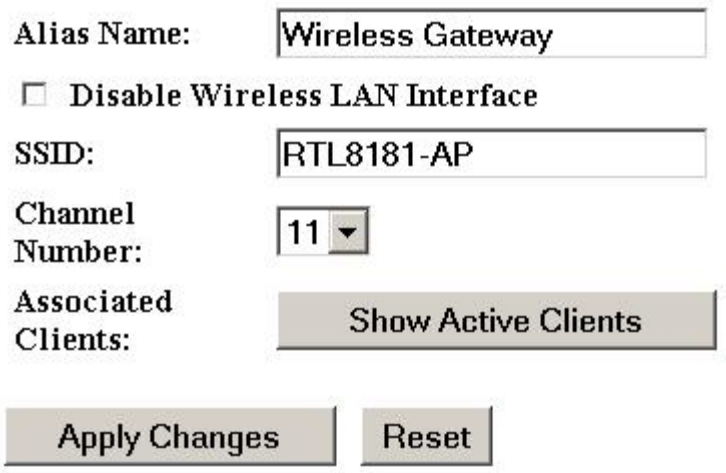
Access Point Status Page

This page shows the current status and some basic settings of the device.

System	
Alias Name	Realtek Wireless Gateway
Uptime	0day:23h:44m:56s
Firmware Version	v1.1
Wireless Configuration	
SSID	RTL8181-AP
Channel Number	11
WEP	Disabled
Associated Clients	0
BSSID	00:e0:4c:81:81:16
LAN Configuration	
IP Address	192.168.1.254
Subnet Mask	255.255.0.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:e0:4c:81:81:16
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:81:17

Wireless--Basic Settings Page

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.



- **Disable Wireless LAN Interface**

When the setting is checked, the RF signal of the device will be disabled.

- **SSID**

The name of the wireless network. This name cannot be longer than 32 characters. The default value is "RTL8181-AP.

- **Channel Number**

A transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the router.

- **Associated Clients**

Click "Show Active Clients" button to launch the Active Wireless Client Table. This table shows the MAC address, transmission, receipt packet counters and encrypted status for each associated wireless client.

- **Apply Changes**

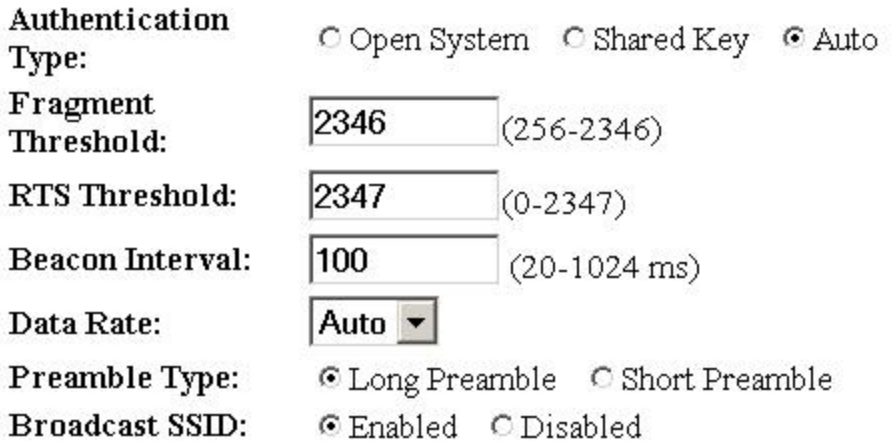
Click "Apply" button to save and implement the new settings.

- **Reset**

Click "Reset" button to reload default settings.

Wireless—Advanced Settings Page

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



- **Authentication Type**

This setting has to be consistent with the wireless devices which the adapter intends to connect.

・**Open System –** No authentication is needed among the wireless devices.

・**Shared Key –** Only wirelss devices using a shared key (WEP Key) are allowed to connecting each other. Setup the same key as the wireless devices which the adapter intends to connect.

・**Auto –** Auto switch the authentication algorithm depending on the wireless devices which the adapter is connecting to.

- **Fragment Threshold**

The value defines the maximum size of packets, any packet size larger than the value will be fragmented. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2346 bytes. Minor change is recommended.

- **RTS Threshold**

Minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the WLAN. Select a setting within a range of 0 to 2347 bytes. Minor change is recommended

- **Beacon Interval**

This value specifies the duration between beacon packets (milliseconds). The beacon packets include the Router's information and are broadcasted to the WLAN network periodly.

- **Data Rate**

Auto - When it is enabled, the device will choose the most suitable transmission rate automatically.

- **Preamble Type**

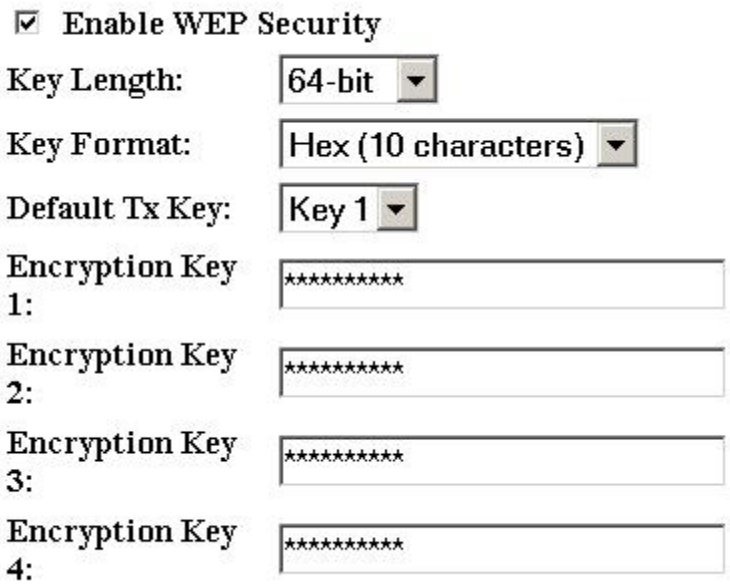
Select either a short preamble or long preamble. Select a short preamble for WLANs with high network traffic; select a long preamble when the network traffic is low.

- **Broadcast SSID**

Enables and disables a Service Set Identifier broadcast. When enabled, the SSID of the router is sent to wireless enabled devices on the LAN. Set the router's SSID in the Basic screen.

Wireless—Security Page

This page allows you setup the WEP security. Turn on WEP by using Encryption Keys could prevent any unauthorized access to your wireless network.



- **Key Length**

You may select the 64-bit or 128-bit to encrypt transmitted data. Larger key length will provide higher level of security, but the throughput will be lower.

- **Default Tx Key**

Select one of the keys (1~4) as the encryption key.

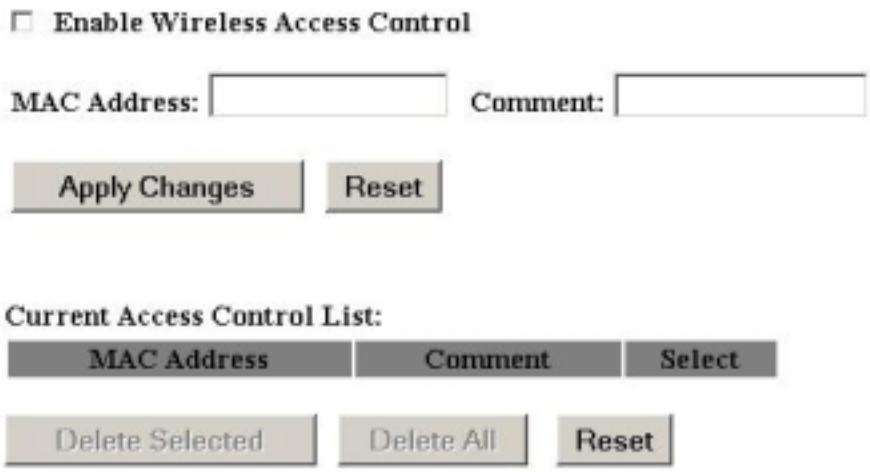
- **Encryption Key1~Key4**

The keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below.

- **64-bit** – Input 10 digit Hex values (in the “A-F”, “a-f” and “0-9”range) as the encryption keys. For example: “0123456aef“.
- **128-bit** – Input 26 digit Hex values (in the “A-F”, “a-f” and “0-9” range) as the encryption keys. For example:“01234567890123456789abcdef“.

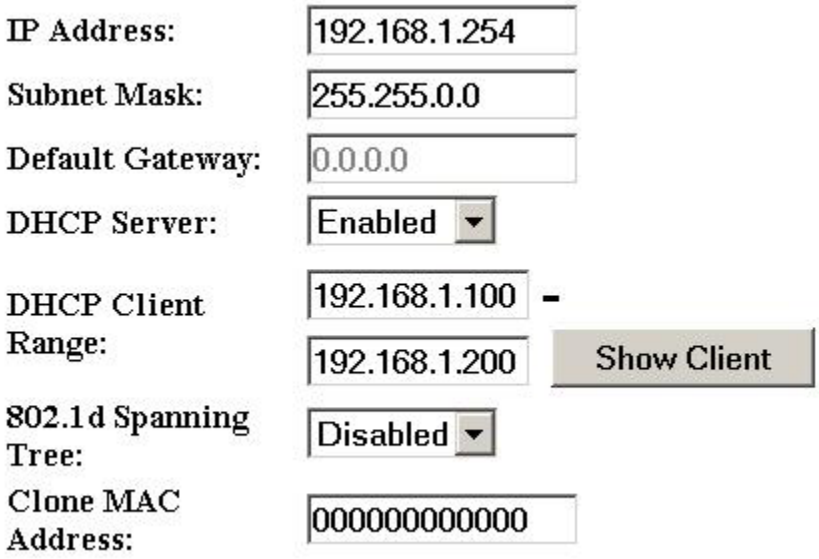
Wireless—Access Control Page

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries



TCP/IP Settings—LAN Interface Page

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..



- **IP Address**

This is the IP address of the router. The default IP address is 192.168.1.254.

- **Subnet Mask**

Type the subnet mask for the router in the text box. The default subnet mask is 255.255.0.0

- **Default Gateway**

Allows administrator to use the Default Gateway address, assign a specific Gateway address, or block clients from Gateway notification.

- **DHCP Server**

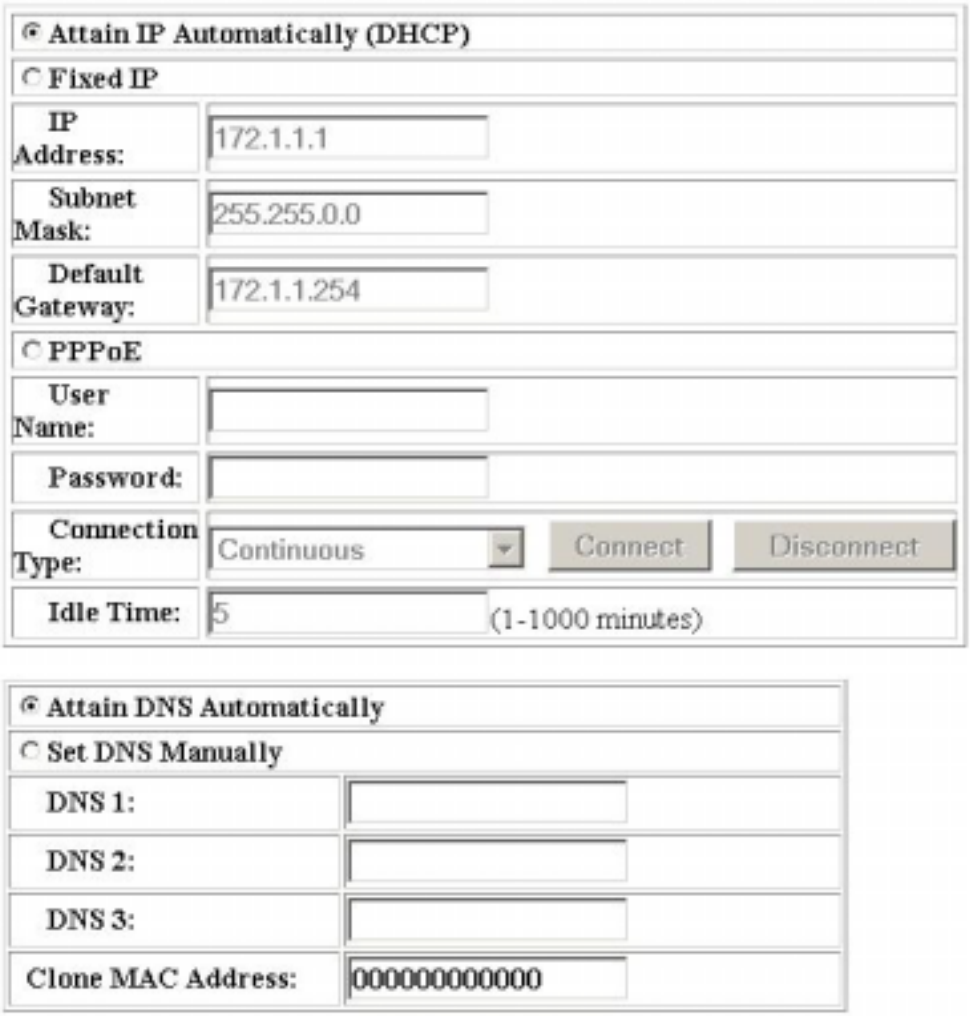
Enables the DHCP server to allow the router to automatically assign IP addresses to devices connecting to the LAN. DHCP is enabled by default. All DHCP client computers are listed in the table at the bottom of the screen, providing the host name, IP address, and MAC address of the client.

- **DHCP Client Range**

Sets the beginning address and range of addresses to be assigned by the Router's DHCP server function. Select up to 253 consecutive addresses (nodes).The IPs to be excluded from the range specification should be entered in the specified field.

TCP/IP Settings—WAN Interface Page

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the setting for IP address, PPPoE, DNS, etc..



When using DHCP Fixed IP, enter the following information in the fields (some information is provided by your ISP):

- **IP Address**

Select whether you want to specify an IP address manually, or want DHCP to obtain an IP address automatically. When *Specify IP* is selected, type the IP address, subnet mask, and default gateway in the text boxes. Your ISP will provide you with this information.

When using PPPoE, enter the following information in the fields (some information is provided by your ISP)

- **User Name**

Type your PPPoE user name.

- **Password**

Type your PPPoE password.

- **Connection Type**

· **Continuous** – Connects immeditely after setting and never disconnects.

· **Connect on Demand** - Reconnects when the Disconnect time elapses.

· **Manual** - Disables Automatic Connection. Connects to Internet using the "**Connect"** button on the settings page.

- **Idle Time Out**

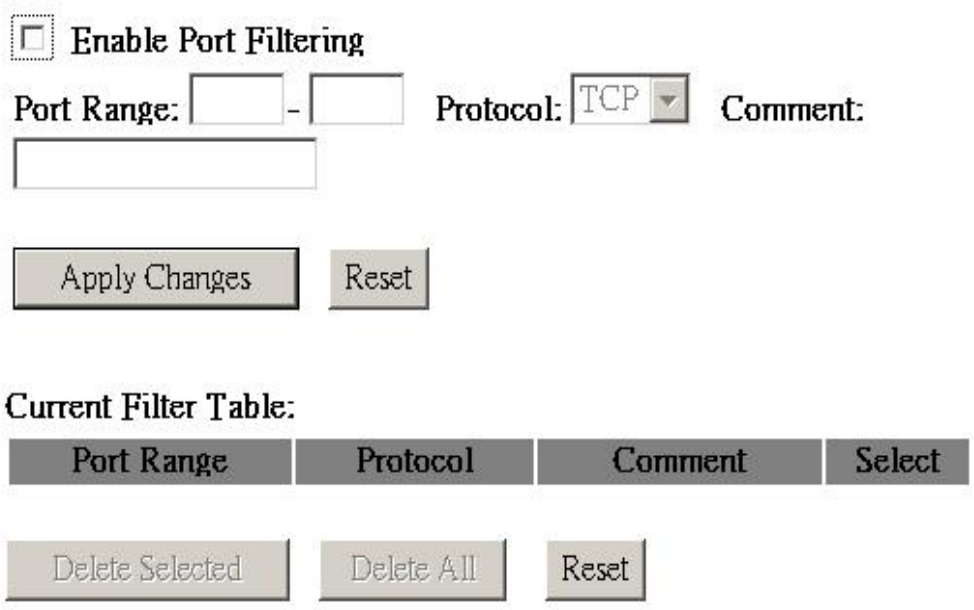
Specify the time that will elapse before the router times out of a connection.

- **Set DNS Manual**

Type up to three DNS numbers in the text boxes. Your ISP will provide you with this information.

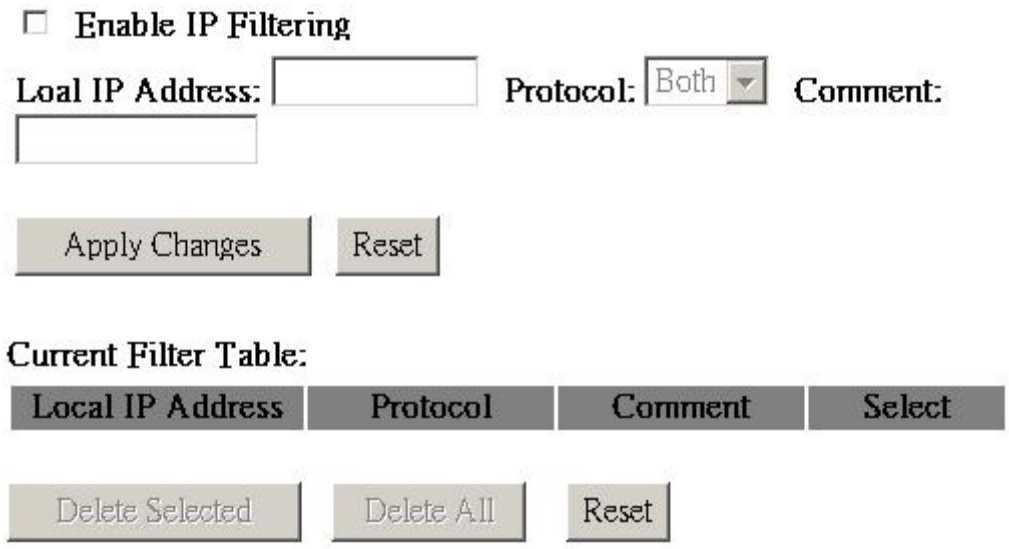
Firewall—Port Filtering Page

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



Firewall—IP Filtering Page

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

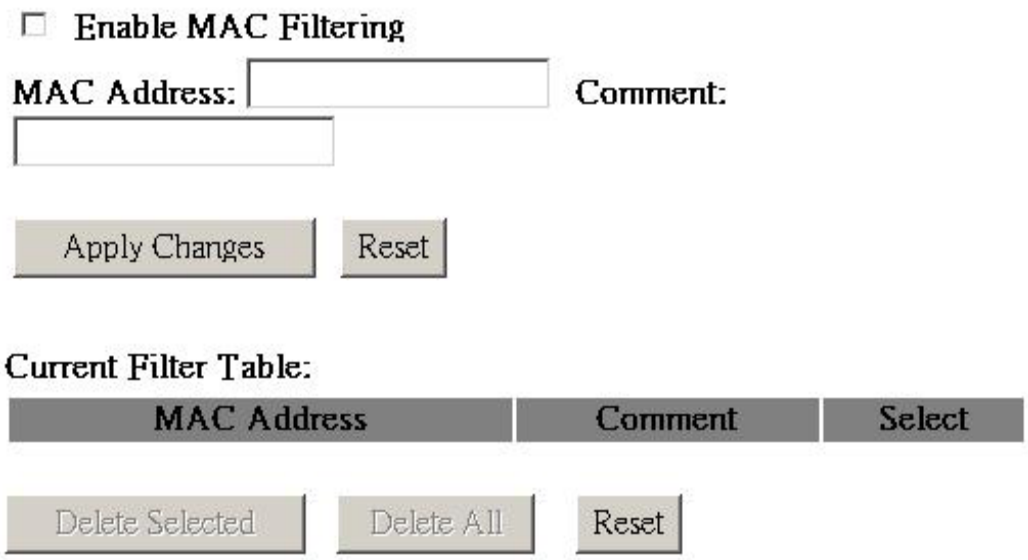


- **Enable IP Filtering**

  Click to enable or disable the IP address filter.

Firewall—MAC Filtering Page

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

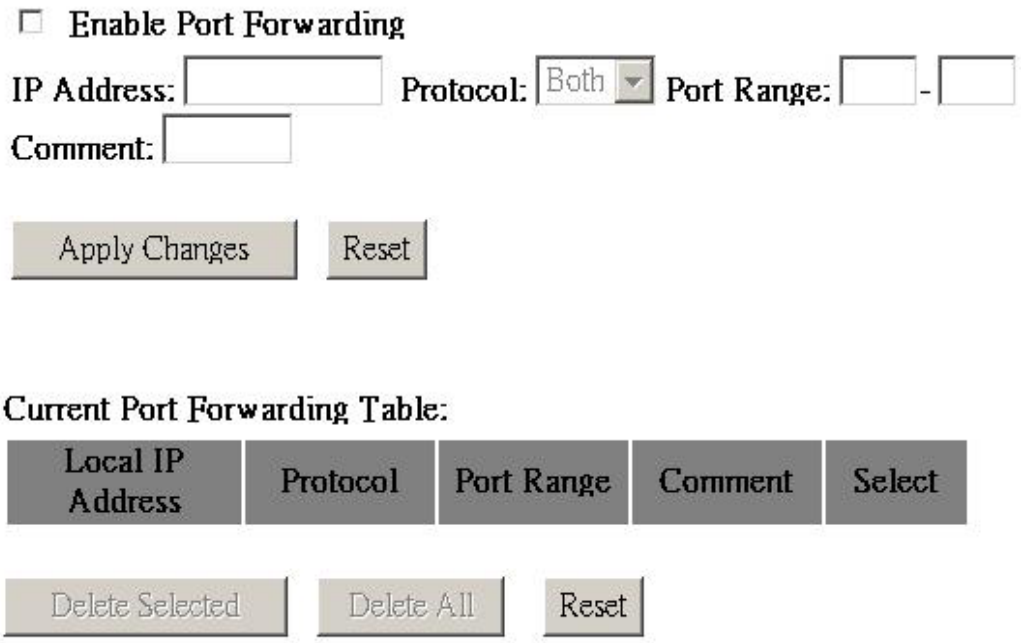


- **MAC Address**

Type the MAC address of the user's network interface.

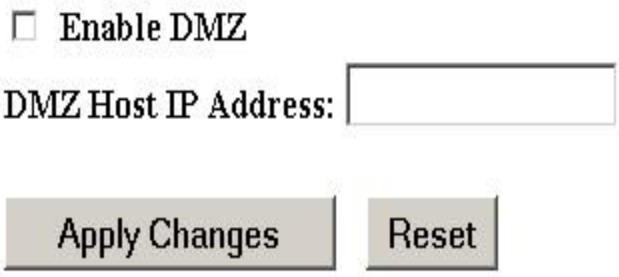
Firewall—Port Forwarding Page

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.



Firewall—DMZ Page

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



- **DMZ Host IP Address**

Type a host IP address for the DMZ. The computer with this IP address acts as a DMZ host with unlimited Internet access.

Statistics Page

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	*Sent Packets*	375892
	Received Packets	79
Ethernet LAN	*Sent Packets*	2562
	Received Packets	3732695
Ethernet WAN	*Sent Packets*	465
	Received Packets	0

Refresh

Upgrade Firmware Page

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Follow these instructions:

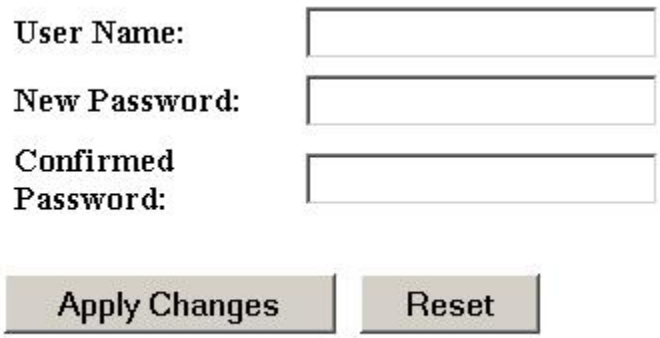
1. Download the latest firmware from the manufacturer's Web site, and save it to your disk.
2. Click *Browse* and go to the location of the downloaded firmware file.
3. Select the file and click Upload to update the firmware to the latest release.

Save/Reload Setting Page

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Password Page

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.



- **User name** –Type your name to the text
- **New Password** - Type new password.
- **Confirmed Password** - Reenter the new password for confirmation.

TROUBLESHOOTING

Symptom : Power LED off

Resolution:

Connect the power adapter to your AP Router and plug it into the power outlet.

Note: Only use the power adapter provided with your AP Router. Using any other adapter may damage your AP Router.

Symptom : Can not setting AP through web browser

Resolution:

- The Ethernet cable(RJ45) must plug to LAN port of AP Router.
- Check that the IP address in the URL field is correct.
- Check your host PC IP address. If the IP address of AP Router is 192.168.1.254 then your IP of host PC must set 192.168.1.1~253.

Symptom : Forgot IP address

Resolution:

If you forgot the IP address of AP Router you can press reset button to restore the default factory settings by pressing this button for five seconds. The default IP is 192.168.1.254.

Symptom : Can not setting AP Router from a wireless card

Resolution:

- Make sure that the Mode, SSID, Channel and encryption settings are set the same on each wireless adapter.
- Make sure that your computer is within range and free from any strong electrical devices that may cause interference.
- Check your IP Address to make sure that it is compatible with the Wireless Router.

Symptom : Can not connect to ISP

Resolution:

- Make sure that your DSL or Cable modem is running correctly and connected to the WAN port of the Broadband Router.
- Make sure that the right connection type is used in the web configuration.
- Make sure that the username and password used in the connection type is correct.
- Some ISP's do not care if you share your broadband connection among multiple users.
- Other ISP's will explicitly restrict this type of activity in your service contract. It is important that you

verify that you are in accordance with your service agreement before sharing Internet access.

Glossary

10BaseT or 100BaseTx: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 10 is 10 Mbps and 100 is 100 Mbps.

802.1x: The standard for wireless LAN authentication used between an AP and a client. 802.1x with EAP will initiate key handling.

Ad-Hoc Network: The wireless network based on a peer-to-peer communications session. Also referred to as AdHoc.

Access Point : Access points are way stations in a wireless LAN that are connected to an Ethernet hub or server. Users can roam within the range of access points and their wireless device connections are passed from one access point to the next.

Authentication: Authentication refers to the verification of a transmitted message's integrity.

DMZ: DMZ (DeMilitarized Zone) is a part of an network that is located between a secure LAN and an insecure WAN. DMZs provide a way for some clients to have unrestricted access to the Internet.

DHCP: DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manu-ally assign permanent IP addresses.

DSSS (Direct Sequence Spread Spectrum): Method of spreading a wireless signal into wide frequency bandwidth.

DTE (Data Terminal Equipment): Device that controls data flowing to and from a computer.

Dynamic IP Address: An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

DNS (Domain Name System): System used to map readable machine names into IP addresses

DTIM:DTIM (Delivery Traffic Indication Message) provides client stations with information on the next opportunity to monitor for broadcast or multicast messages.

Filter: Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.

Firewall: Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization’s public Web

server separate from the internal LAN.

Firmware: Programming inserted into programmable read-only memory, thus becoming a permanent part of a computing device.

Fragmentation: Refers to the breaking up of data packets during transmis-sion.

Gateway: Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.

Half-duplex: To transmit on the same channel in both directions, one direction at a time.

Host Name: The name given to a computer or client station that acts as a source for information on the network.

ISP: An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.

LAN(Local Area Network): A group of computers and peripheral devices connected to share resources.

MAC(Medium Access Control) Address: A unique number that distinguishes network cards.

MTU: MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages lar-ger than the MTU are divided into smaller packets.

NAT: NAT (Network Address Translation - also known as IP mas-querading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

PPPoE: PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.

PoE (Power over Ethernet): A mechanism to send DC power to a device using a CAT5 Ethernet cable.

Preamble: Preamble refers to the length of a CRC (Cyclic Redundancy Check) block that monitors communications between roam-ing wireless enabled devices and access points.

Protocol: A standard way of exchanging information between computers.

RADIUS (Remote Authentication Dial In User Service): A server that issues authentication key to clients.

RAM (Random Access Memory): Non-permanent memory.

RIP: RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

Router: Device that can connect individual LANs and remote sites to a server.

Roaming: The ability to use a wireless device while moving from one access point to another without losing the connection.

RTS: RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to trans-mit data.

Server: Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.

SMTP: SMTP (Simple Mail Transfer Protocol) is the standard Inter-net e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.

SNMP: SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol. SNMP hard-ware or software components transmit network device activity data to the workstation used to oversee the network.

Static IP Address: A permanent IP address is assigned to a node in a TCP/IP network. Also known as global IP.

STP (Shielded Twisted Pair): Twisted Pair cable wrapped in a metal sheath to provide extra protection from external interfering signals.

Subnet Mask: Subnet Masks (SUBNETwork masks) are used by IP proto-col to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP ad-dress to determine whether to accept or reject the packet.

SSID: SSID (Service Set Identifier) is a security measure used in WLANs. The SSID is a unique identifier attached to packets sent over WLANs. This identifier emulates a password when a wireless device attempts communication on the WLAN. Because an SSID distinguishes WLANS from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID.

TCP/IP: TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in real-time video and audio transmission).

TFTP (Trivial File Transfer Protocol): Simple form of FTP (File Transfer Protocol), which Uses UDP (User Datagram Protocol), rather than TCP/IP for data transport and provides no security features.

TKIP (Temporal Key Integrity Protocol): An encryption method replacing WEP.TKIP uses random IV and frequent key exchanges.

UDP (User Datagram Protocol): A communication method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network. UDP is used as an alternative to TCP/IP.

Uplink: Link to the next level up in a communication hierarchy.

UTP (Unshielded Twisted Pair) cable: Two or more unshielded wires twisted together to form a cable.

Virtual Servers: Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

WEP (Wired Equivalent Privacy): An encryption method based on 64 or 128bit algorithm.

Web Browser: A software program that allows viewing of web pages.

WAN: WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (con-trasted with a LAN, which covers a small area such as a company building).

WLAN: WLANs (Wireless LANs) are local area networks that use wireless communications for transmitting data. Transmis-sions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are con-nected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and ob-jects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

VPN (Virtual Private Network): A security method to connect remote LAN users to a corporate LAN system.

TECHNICAL SPECIFICATIONS

Networking Characteristics

Compatibility	● IEEE 802.11 Standard for WLAN (DSSS) ● IEEE 802.3 10Base-T Ethernet ● Internal Wi-Fi certified by TwinMOS
Ports	RJ-45, 10Base-T Ethernet Port WAN X-II 10/100
Operating Modes	Access Point Wireless Bridge ▪ Point to Point ▪ Point to Multipoint Client AP
Network Protocol	TCP/IP, IPX/SPX, NetBEUI, ARP,SNMP DHCP,NDIS3,NDIS4

RF Characteristics

Power Input	DC 7.5 – 12V, 1A Use External Power Supply
Frequency Range	2.400-2.4835 GHz, Direct Sequence Spread Spectrum (DSSS)
Operating Channels	● 1-11 United States (FCC) ● 1-11 Canada (DOC) ● 1-14 Japan (MKK) ● 1-13 Europe (Except Spain and France) (ETSI)
Modulation Technique	● 11 Mbps: CCK ● 5.5 Mbps: CCK ● 2 Mbps: DQPSK ● 1 Mbps: DBPSK
Spreading	11-chip Barker Sequence
Transmit Power	15 dBm @ Nominal Temp Range
Receive Sensitivity	Nominal Temp Range：11 Mbps 10^{-5} BER @ -83 dBm, minimum
Security	64/128-bit WEP Encryption
Antenna	Two Antenna with Diversity and AGC At least 2 dBi Gain
Operating Range	Open Space：100 ~ 300m; Indoor: 30m ~ 100m The transmission speed varies in the surrounding environment.
EMC Certification	FCC Class B part 15B, 15C; R&TTE

FCC CAUTION

NOTE

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection. This equipment generates, uses and can radiated radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Shielded interface cables must be used in order to comply with emission limits.

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits 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 20cm (8 inches) during normal operation