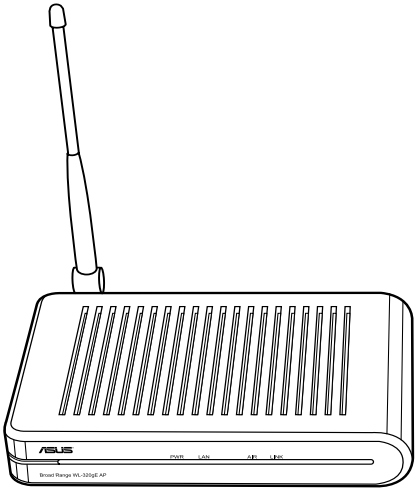
802.11g Access Point
WL-320gE
(For 802.11g and 802.11b Wireless Clients)



User's Manual

Copyright Information

E4466
Third Edition
February 2009

ASUS Contact information

ASUSTeK COMPUTER INC. (Asia Pacific)

Address	15 Li-Te Road, Peitou, Taipei, Taiwan 11259
Website	www.asus.com.tw

Technical Support

Telephone	+886228943447
Support Fax	+886228907698
Software download	support.asus.com*

ASUS COMPUTER INTERNATIONAL (America)

Address	800 Corporate Way, Fremont, CA 94539, USA
Telephone	+15029550883
Fax	+15029338713
Website	usa.asus.com
Software download	support.asus.com*

ASUS COMPUTER GmbH (Germany and Austria)

Address	Harkort Str. 25, D40880 Ratingen, Germany
Telephone	+49210295990
Fax	+492102959911
Online contact	www.asus.com.de/sales

Technical Support

Telephone	+49210295990
Fax	+492102959911
Online support	www.asus.com.de/support
Website	www.asus.com.de/news

* Available on this site is an online Technical Inquiry Form that you can fill out to contact technical support.

Table of Contents

About this user guide

Notational conventions

- Acronyms are defined the first time they appear in the text.
- The ASUS WL-320gE is referred to as the “ASUS 802.11g WLAN AP”.

Typographical conventions

- **Boldface** type text is used for items you select from menus and dropdown lists, and commands you type when prompted by the program. These items could either be enclosed in < > (open and close brackets) or " " (open & close quotations). **Boldface** type text is also used for emphasis.

Symbols

This document uses the following icons to call your attention to specific instructions or explanations.

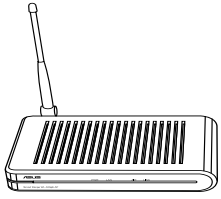
Note: Provides clarification or non-essential information on the current topic.

Warning: Provides messages of high importance, including messages relating to personal safety or system integrity.

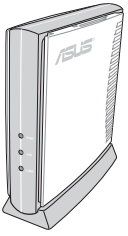
The ASUS Wireless Family

The ASUS Wireless family contains several wireless network solutions for 802.11g & 802.11b wireless local area networks.

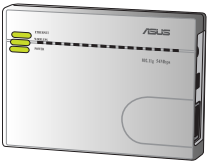
Access Point or Client



The **ASUS WL320gE Wireless Access Point** incorporates 802.11g OFDM technology designs, which provides the fastest IEEE 802.11g wireless transmission at 54Mbps and is compatible with existing IEEE 802.11b devices.

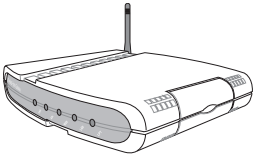


The **ASUS WLAN 802.11g Access Point (WL-300g)** creates a wireless network using the IEEE 802.11g and 802.11b wireless standards.

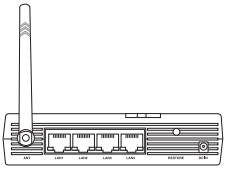


The **ASUS 3 in 1 Pocket Access Point (WL-330g)** creates a wireless network using the IEEE 802.11g/b wireless standards.

Access Point & Router

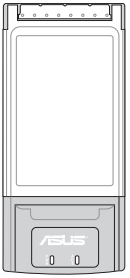


The **ASUS WLAN Gateway (WL-500g)** creates a wireless network using the IEEE 802.11g/b wireless standards and allows sharing of a single Internet connection.



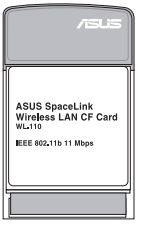
The **ASUS WLAN 802.11g Pocket Router (WL-530g)** creates a wireless network using the IEEE 802.11g and 802.11b wireless standards and allows sharing of a single Internet connection.

PCMCIA Client



The **ASUS WLAN PC Card (WL-107g)** is a wireless LAN adapter that fits into the PCMCIA Type II slot in a Notebook PC and creates a wireless network using the IEEE 802.11g/b wireless standards.

Compact Flash (CF) Client

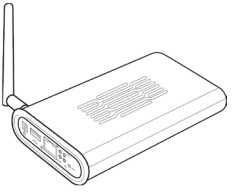


The **ASUS 802.11b Wireless CF Card (WL-110)** is an IEEE 802.11b wireless LAN adapter that fits into a Compact Flash Type II slot in a Portable Digital Assistant (PDA).

PCI Client

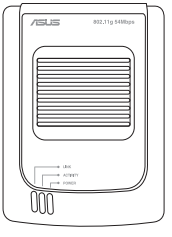
The **ASUS WLAN PCI Card (WL-138g)** is a wireless LAN adapter that fits into the standard PCI slot in a desktop PC and creates a wireless network using the IEEE 802.11g/b wireless standards.

Access Point & File Server



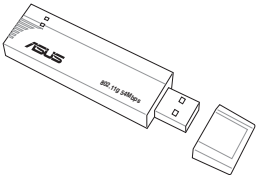
The **ASUS WLAN 802.11g Access Point (WL-HDD)** creates a wireless network using the IEEE 802.11g and 802.11b wireless standards. It also serves as a file server (wireless network attached storage).

USB Access Point or Client



The **ASUS USB Wireless LAN Adapter (WL-160g)** creates a wireless network using the IEEE 802.11g/b wireless standards and connects to any computer via the USB 2.0 slot.

USB Client



The **ASUS USB Wireless LAN Adapter (WL-167g)** creates a wireless network using the IEEE 802.11g/b wireless standards and connects to any computer via the USB2.0 slot.

The illustrations are not to scale.

1. Introduction

1.1 Welcome!

Thank you for purchasing the ASUS WL320gE Wireless Access Point!

The ASUS WL320gE Wireless Access Point incorporates 802.11g OFDM technology designs, which provides fastest IEEE 802.11g wireless transmission at 54Mbps and is compatibile with existing IEEE 802.11b devices. With its Afterburner technology, its performance is greatly enhanced compared to the standard IEEE 802.11g devices. The packets are protected by WiFi Protected Access version 2.0 (WPA2), a wireless security protocol.

1.2 Package contents

Check the following items in your WL-320gE package.

- WL-320gE WLAN Access Point x1
- Quick Start Guide x1
- Power adapter x1 (5 Volts DC, 1 Amp)
- Support CD x1 (utilities and user's manual)
- RJ-45 Ethernet cable x1 (straight-through)
- Bracket for ceiling mounting x1
- Bracket for office partition mounting x1
- Sticker for wall mounting alignment x1

If any of items is damaged or missing, contact your retailer.

1.3 Technical Specifications

HARDWARE	
Ethernet interface	RJ45 for 10/100 BaseT with auto cross-over function (MDI/MDI-X)
Antenna	1 x external dipole antenna with Reverse-SMA antenna connector, 1 X internal Inverted-F PCB antenna (TBD)
Output power	24dBm in b mode and 20dBm in g mode with 1.5dB tolerance
Power adapter	AC Input: 100V~240V(50~60HZ) DC Output: 5V with max. 2 A current
Reset button	Using a pen or a paper clip, press for over five seconds to restore the AP to its factory default settings.
LED	Power, Ethernet, Wireless Activities, and Wireless LED Association
	Wireless Association behavior: • On: associated (AP mode), or associates with an AP (EA mode or URE is enabled, RSSI>= -65dBm) • Flashing: (EA mode or URE is enabled) < -89 dBm On: 200 ms, Off: 1000 ms >= -89 dBm < -83 dBm On: 200 ms, Off: 800 ms >= -83 dbm < -77 dBm On: 200 ms, Off: 600 ms >= -77 dBm < -71 dBm On: 200 ms, Off: 400 ms >= -71 dBm < -65 dBm On: 200 ms, Off: 200 ms • Off: not associated (AP mode), or associates with no APs (EA mode)
Size	185 mm x 205 mm x 36 mm (LxWxH). Size excludes the external antenna
Weight	500g (excluding power supply)
Operating Frequency	2.4 - 2.5 GHz
Spreading	Direct Sequence Spread Spectrum
Modulation	OFDM, CCK, DQPSK, DBSPK
Emissions	ETS; CE Mark; FCC Part 15
Data rate	802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps 802.11b: 1, 2, 5.5, 11Mbps
Operation channels	11 for N. America, 14 Japan, 13 Europe (ETSI)
Range	3 (non-overlapping)

(continued on the next page)

SOFTWARE	
Management	Access point mode Ethernet adapter cable Gateway mode WDS URE DHCP server, DHCP client Device statistic Noise level, noise level on other channel, signal level of current AP, list of other APs and log of last 10 association attempts Smart Wizard web-based administration Guest SSID (only in Gateway mode) Bandwidth management UPnP Internet Gateway Device (only in Gateway mode) Network management a. Save/restore configurations b. MAC address cloning c. Upgrade firmware via web browser d. Remote firmware upgrade: enable management by operator e. SNMP version 2.0 f. Network initiated throughput test: supports ncttcp server embedded; this will enable mesh network to initiate uplink and downlink throughput tests
Security	**Firewall:** • NAT and SPI **Filtering:** • Port, IP address, protocol and URL Keyword **Logging:** • Device statistic (TBD) **Encryption:** • 64/128-bit WEP • WPA/WPA2, WPA-TKIP/AES, WPA-PSK **Authentication:** • MAC address, 802.1x RADIUS (TLS, TTLS, PEAP)
Utilities	**Device Discovery:** Allows you to search for WL-300g/WL-320g/WL-500g/WL-600/WL700g in your network and allows you to configure the WL-320gE through its web interface. **Firmware Restoration:** Restores the firmware that failed during its firmware upgrading process.

1.4 Wireless Performance

This section provides you with information on how to improve the performance of an ASUS WLAN network.

1.4.1 Site Topography

For optimal performance, locate wireless mobile clients and the ASUS APs away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment. Signal loss can occur when metal, concrete, walls or floors block transmission. Locate the ASUS APs in open areas or add the ASUS APs as needed to improve coverage.

Microwave ovens operate in the same frequency band as the ASUS AP . If you use a microwave within range of the ASUS AP, you may notice network performance degradation. But both your microwave and your the ASUS AP continue to function.

1.4.2 Range

Every environment is unique with different obstacles, barriers, or materials. Hence, it is difficult to determine the exact range that will be achieved without testing. Some guidelines have been developed so users can estimate the rage, but there are no hard and fast specifications.

Radio signals may reflect off of some obstacles or be absorbed by others depending on their construction. For example, with two 802.11b radios, you may achieve up to 1000' in open space outdoors where there are no obstacles between the two devices. The same two units may only achieve up to 300' of range when used indoors.

By default, the ASUS AP will automatically adjust the data rate to maintain a usable radio connection. A client that is close to the ASUS AP may operate at a higher speed while a client that is on the fringe of coverage may operate at a lower speed. As mentioned earlier, you can configure the data rates that the ASUS AP will use. If you limit the range of data rates available to the ASUS AP, you may reduce the effective wireless range of the WLAN coverage.

1.4.3 Site Surveys

A site survey, a utility provided with the ASUS WLAN cards, analyzes the installation environment and provides you with recommendations for the device and its placement. The optimum placement differ depending on the ASUS AP design and specifications.

1.4.4 Roaming Between ASUS APs

If there are multiple ASUS APs on the network, then a wireless mobile client may seamlessly roam from one ASUS AP to another.

Each ASUS AP creates its own wireless cell or coverage area, which is also known as the Basic Service Set (BSS). Any wireless mobile client can communicate with a particular ASUS AP if it is within the ASUS AP's coverage area.

If the cells of multiple ASUS APs overlap, then the wireless mobile client may switch from one ASUS AP to another as it travels throughout the facility. During the hand-off from one ASUS AP to another, the wireless mobile client maintains an uninterrupted connection to the network. This is known as "roaming."

Multiple ASUS APs connected to a common Ethernet network form an Extended Service Set (ESS). All members of an Extended Service Set are configured with an ID, known as the SSID or ESSID. Wireless mobile clients must be configured with the same SSID as the ASUS APs on the network. A client can only roam between ASUS APs that share the same SSID.

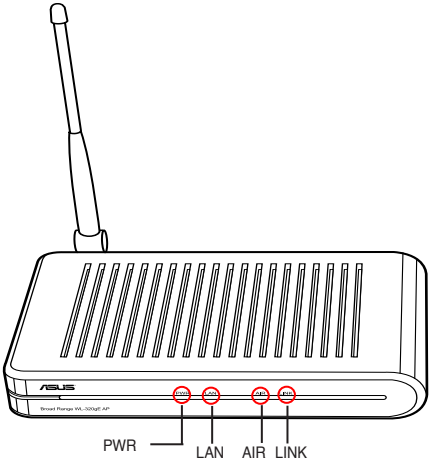
1.4.5 Roaming Guidelines

- An ASUS WLAN Card can only roam between APs of the same type.
- All ASUS APs must have the same SSID.
- All computers with ASUS WLAN Cards must have the same SSID as the Access Points that they will roam between.
- If WEP encryption is enabled, then all ASUS APs and client adapters must use the same encryption level and WEP Key to communicate.
- The ASUS APs' cells must overlap to ensure that there are no gaps in coverage and to ensure that the roaming client will always have a connection available.
- ASUS APs that use the same channel should be installed as far away from each other as possible to reduce potential interference.
- It is strongly recommended that you perform a site survey using the utility provided with the ASUS WLAN Card to determine the best location for each ASUS AP in the facility.

1.5 Getting to Know the WL-320gE

1.5.1 Front panel features

The ASUS WL-320gE Access Point includes LED indicators which show the system, LAN, wireless network, and link status.



PWR (Power)

OFF: No power or performing boot sequence

ON: System ready

Blinking: Firmware upgrade failed

LAN (Local Area Network)

OFF: No power

ON: Has physical connection to an Ethernet network

Blinking: Transmitting or receiving data (through Ethernet cable)

AIR (Wireless Network)

OFF: No power

ON: Wireless function ready

Blinking: Transmitting or receiving data (wireless)

LINK (Link Status)

OFF: No power

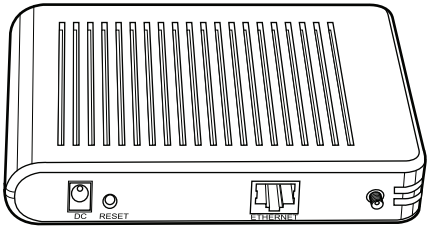
ON: Has physical connection to an Ethernet network

Blinking: Transmitting or receiving data (through Ethernet cable)

Operation Mode	AP/Repeater/Bridge/ Gateway	Client
Off	Client not associated	Not associated to AP
On	Client associated	Associated to AP with strong signal
Blinking slowly	--	Associated to AP with better signal
Blinking slowly	--	Associated to AP with weak signal

1.5.2 Rear panel features

The rear panel contains the Ethernet, the DC port, and the Reset button.



Label	Description
ETHERNET	The Ethernet port connects to an Ethernet device such as to a switch or to a router.
RESET	Using a pen or a paper clip, press the Reset button to restore to factory default settings.
DC	The DC port connects to the power adapter.

2. Installation

This chapter describes the installation procedure for the ASUS 802.11g AP and includes a description of the LEDs found on the unit.

2.1 Installation Procedure

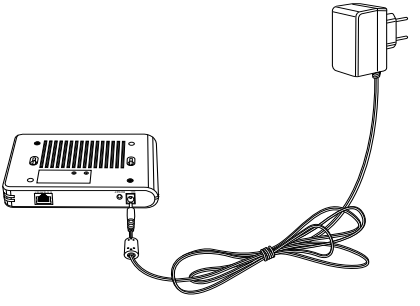
Follow these steps to install the ASUS 802.11g WLAN AP.

1. Determine the best location for the ASUS 802.11g WLAN AP. Keep in mind the following considerations:

- The length of the Ethernet cable that connects the Access Point to the network must not exceed 100 meters.
- For standard placement, try to place the Access Point on a flat, sturdy surface as far from the ground as possible, such as on top of a desk or bookcase, keeping clear of metal obstructions and away from direct sunlight.
- For external antenna mounting, install the external antennas so that they are clear of obstructions. Refer to the documentation that came with the antennas for mounting and installation instructions.
- Try to centrally locate the Access Point or its antennas so that it will provide coverage to all of the wireless mobile devices in the area.
- Use only the power supply that came with this unit. Other power supplies may fit but the voltage and power may not be compatible.

Note: The ASUS AP 802.11g AP should be operated at least 20 centimeters from any person. This is necessary to ensure that the product is operated in accordance with the RF Guidelines for Human Exposure which have been adopted by the Federal Communications Commission.

2. Place the Access Point in the desired location. Wall mounting is also possible for the Access Point. Refer to the section **Wall Mounting Option** on the next page for details.
3. Attach one end of an RJ-45 Ethernet cable to the Access Point and attach the other end to the RJ-45 10Base-T port of a network hub, switch, router, or patch panel (possibly on a wall).
4. Attach one end of the bundled AC power adapter to the back of the ASUS 802.11g AP and the other end to a power outlet.



Note: Use only the power adapter included in the product package. Using another power supply may damage the Access Point.

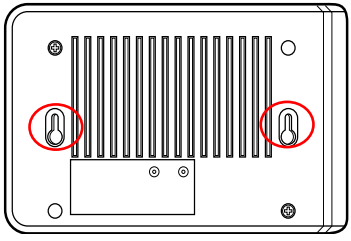
The Power LED on the front of the Access Point will light up when the unit is powered ON. In addition, the green Link LED will turn ON to indicate that the Access Point has a physical Ethernet network connection.

2.2 Wall Mounting Option

The ASUS WL-320gE Access Point is designed to sit on a raised flat surface like a file cabinet or a bookshelf. The unit may also be converted for mounting to a wall or ceiling.

Follow these steps to mount the ASUS 802.11g WLAN AP to a wall:

1. Look on the underside for the two mounting hooks.
2. Mark two upper holes in a flat surface.
3. Tighten two screws until only 1/4" is showing.
4. Latch the hooks of the ASUS WL-320gE onto the screws.



Note: Readjust the screws if you cannot latch the Access Point onto the screws or if it is too loose.

3. Software Configuration

3.1 Configuring the ASUS 802.11g AP

The ASUS 802.11g AP meets various working scenarios with proper configurations. You may need to change the ASUS AP's default settings so as to meet the requirements in your environment.

Configuring the ASUS 802.11g AP through a web browser. You need a Notebook PC or desktop PC connected to the ASUS 802.11g AP (either directly or through a hub) and running a web browser as a configuration terminal. The connection can be wired or wireless. For the wireless connection, you need an IEEE 802.11g/b compatible device, such as an ASUS WLAN Card, installed in your Notebook PC. You should also disable WEP and set the SSID to "default" for your wireless LAN device.

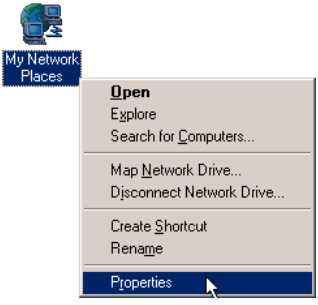
To access the ASUS 802.11g AP, you must have the correct TCP/IP settings on your wired or wireless clients. Ensure that the clients' IP addresses are within the same subnet as the ASUS 802.11g AP.

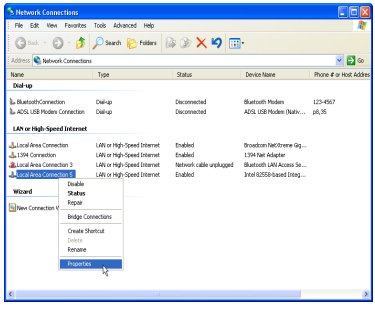
Note: Changing TCP/IP settings may require rebooting your PC. When rebooting, the ASUS 802.11g AP should be switched ON and in the ready state.

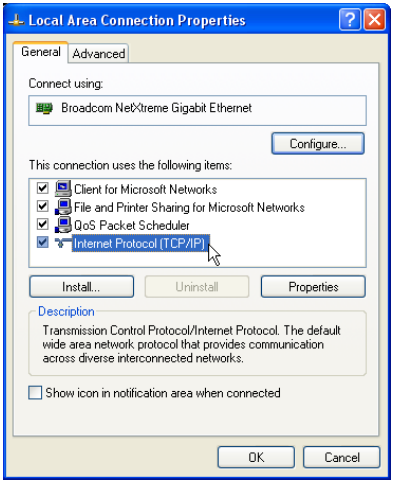
Settings up an IP address manually

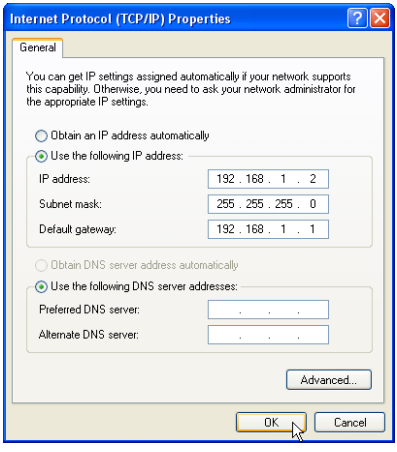
If you want to manually assign an IP address to a client, we recommended that you use the following settings:

- IP address 192.168.1.xxx (xxx can be any number between 2 and 254 that is not used by another device)
- Subnet Mask 255.255.255.0 (same as the ASUS 802.11g AP)
- Gateway 192.168.1.1 (this is the ASUS 802.11g AP IP address)
- DNS 192.168.1.1 (ASUS 802.11g AP IP address or your own).



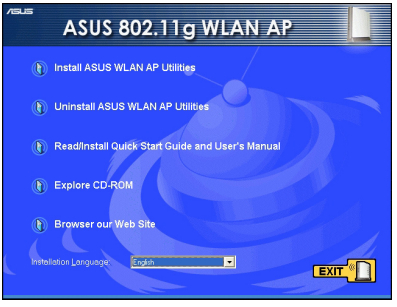




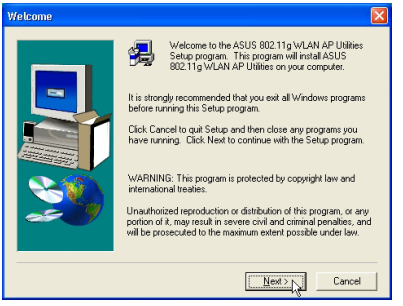


3.1.1 Installing the ASUS WLAN Utilities

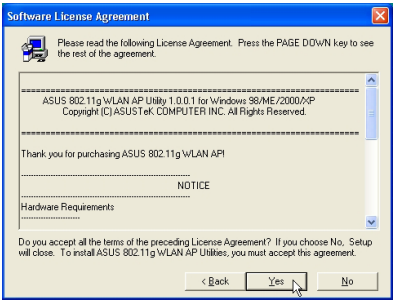
The support CD contains the utilities for configuring the ASUS 802.11g AP. To install the ASUS WLAN utilities in Microsoft® Windows OS, insert the support CD in the optical drive. If Autorun is disabled, run **setup.exe** from the root directory of the support CD.



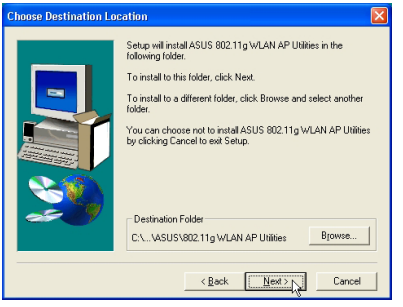
(1) Click **Install...Utilities.**



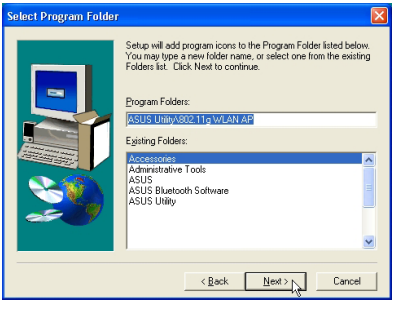
(2) Click **Next**.



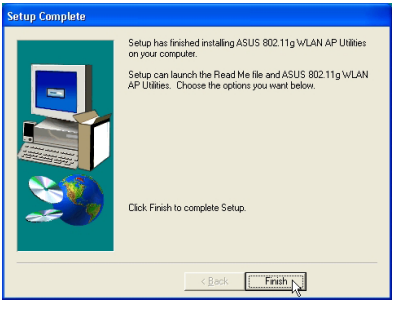
(3) Click **Yes** after reading the license agreement.



(4) Click **Next** to accept the default destination folder or click **Browse** to specify another path.



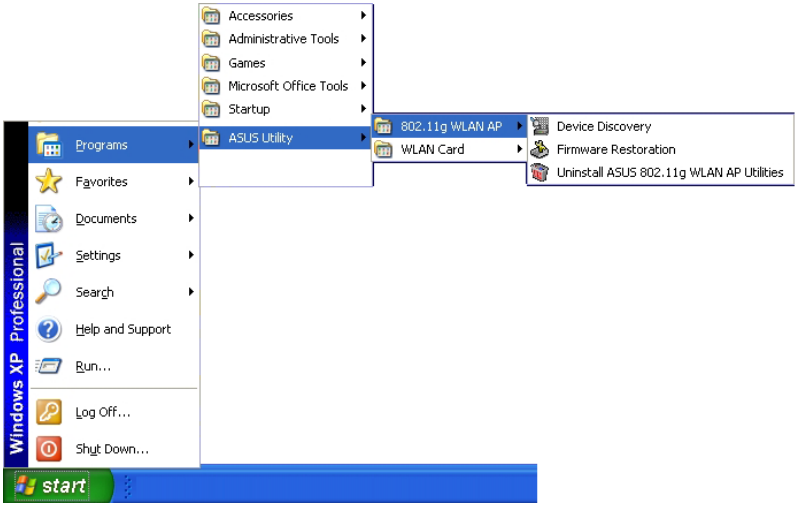
(5) Click **Next** to accept the default program folder or enter another name.



(6) Click **Finish** when setup is complete.

3.2 ASUS WLAN Utilities

After installation, you can launch the utilities through the Start menu.



3.3 Connecting to the WLAN Web Manager

Wired Ethernet Connection

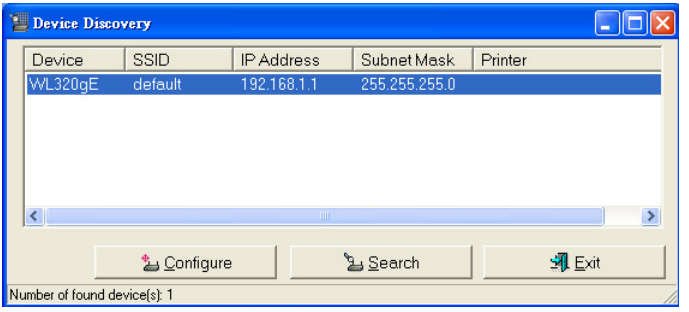
Besides using a network hub, you can also use an Ethernet cable to connect the ASUS 802.11g AP to your computer. The ASUS 802.11g AP has auto-crossover function, so use either a straight-through or crossover cable for wired connection.

Wireless Connection

Use a wireless adapter to connect your computer with the ASUS 802.11g AP. Ensure that the TCP/IP settings are set correctly.

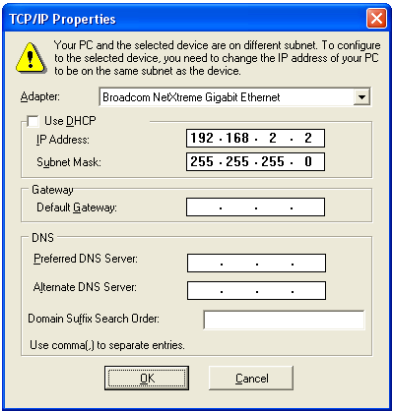
3.4 Device Discovery

Device Discovery is an ASUS WLAN utility that detects an ASUS wireless device, and enables you to configure the device.



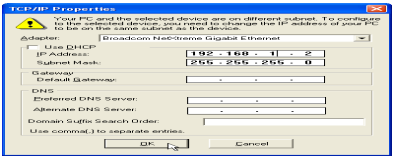
Manually Entering the Address

Launch the web browser on your computer and enter the IP address of the ASUS 802.11g AP : **http://192.168.1.1**



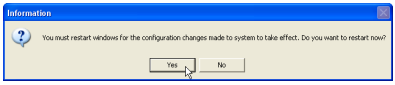
(This is the wrong setting.)

If your computer's IP is not on the same subnet as the ASUS 802.11g AP (192.168.1.X), you will be asked to change it. The IP address can be any number from 2 to 254 that is not used by another device. Gateway is not required.



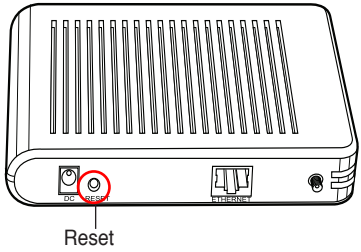
(This is the correct setting.)

Note: You can also change your TCP/IP settings through Windows network properties.



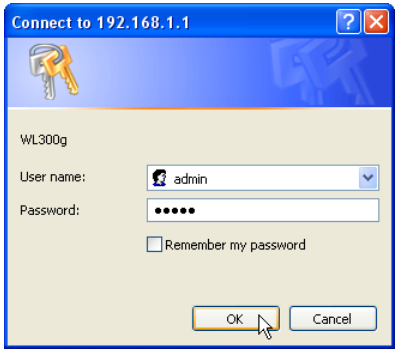
Click **Yes** to restart the Windows® OS for the configuration changes to take effect.

Note: If you cannot find any the ASUS 802.11g APs due to a problem in the IP settings, press the button for over five seconds to restore the system to its factory default settings.



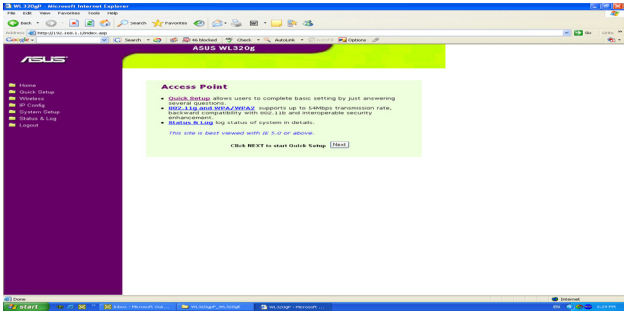
User Name and Password

Once connected, you are asked for the User name and Password in order to log in. The factory default values are "**admin**" and "**admin**".



Home Page

After logging in, the ASUS 802.11g AP home page is displayed. The default pages will be for the Access Point mode. Router and Home Gateway modes are described later in this manual.



3.5 Access Point Mode

In “Access Point” mode, the ASUS 802.11g AP operates as a MAC layer learning bridge and forward packets between wireless mobile clients and the Ethernet network.

In “Access Point” mode, the wireless LAN generally consists of one or more 802.11g/b Access Points and one or more wireless mobile clients that have an 802.11g/b adapter installed.

The ASUS 802.11g AP maintains a table of MAC addresses, which are located either on the Ethernet network or on the radio network, and monitors the source address of packets it receives. For example, if the ASUS 802.11g AP receives a packet over its radio, it creates an entry in its table for the node that sent the packet and labels the entry as a member of the radio network. The ASUS 802.11g AP removes an entry from the table after five minutes of inactivity.

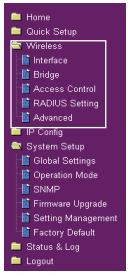
When the ASUS 802.11g AP receives a packet from the Ethernet network, it compares the packet’s destination address with the node addresses in its table. If the packet’s destination address is not in the table or if is listed in the table as a member of the radio network, the ASUS 802.11g AP will forward the packet to the wireless mobile clients. If the packet’s destination address is listed in the table as a member of the Ethernet network, the ASUS 802.11g AP will not forward the packet to the wireless mobile clients. The ASUS 802.11g AP applies the same principles to determine if a packet received over its radio should be forwarded to the Ethernet network.

The ASUS 802.11g AP forwards all broadcast packets to wireless mobile clients. Given this, the ASUS 802.11g AP can only support a limited amount of network traffic. We recommend that you only use the ASUS 802.11g AP on networks that contain less than 512 nodes.

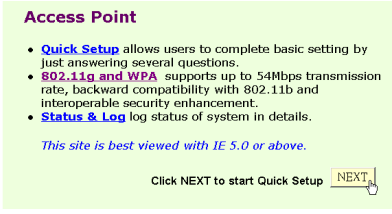
The number of wireless mobile clients that can be supported by the ASUS 802.11g AP depends on the amount of information that each client exchanges in the network. Hence, the number of clients that can be supported by one ASUS 802.11g AP will vary based on the applications in use and how frequently network information is accessed.

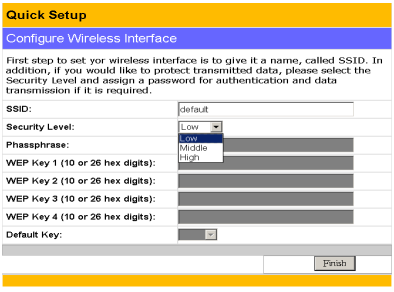
3.6 Quick Setup

Click **Next** to enter the Quick Setup page. Follow the instructions to set up the ASUS 802.11g AP. Tips are given when you move your cursor over each item.



3.6.1 Configure Wireless Interface





To configure your wireless interface:

1. Assign an SSID, which is a unique name for your wireless AP.
2. From the dropdown list, select the Security Level for your wireless AP.

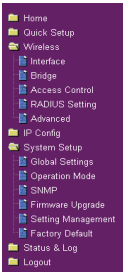
*Medium: Select this option to allow client with the same WEP keys to access this AP and transmit data with 64-bit or 128-bit WEP encryption.

*High: Select this option to allow clients with the same WPA pre-shared keys to connect to this AP and transmit data with TKIP encryption.

3. Click **Finish** when done.

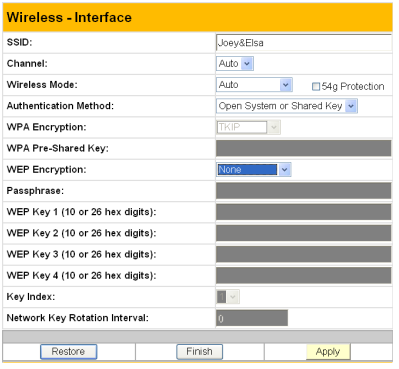
If you would like to perform other settings, click an item on the menu to reveal a submenu. Follow the instructions to set up the ASUS 802.11g AP. Tips are given when you move your cursor over each item.

3.7 Wireless



Click an item on the menu to reveal a submenu. Follow the instructions to set up the ASUS 802.11g AP. Tips are displayed when you move your cursor over an item.

3.7.1 Interface



SSID

The Service Set Idenfifier (SSID), a unique identifier that contains up to 32 ASCII characters, differentiates WLANs from each other. The SSID is also referred to as the “ESSID” or “Extended Service Set ID.” You can use the default SSID and radio channel unless more than one ASUS 802.11g AP is deployed in the same area. In that case, you should use a different SSID and radio channel for each ASUS 802.11g AP. All ASUS Wireless APs/Routers and ASUS 802.11g/802.11b WLAN client adapters must have the same SSID to allow a wireless mobile client to roam. By default, the SSID is set to “default”.

Channel

The 802.11g and 802.11b specifications supports up to 14 overlapping channels for radio communication. To minimize interference, configure each ASUS 802.11g AP to be non-overlapping. Select "Auto" from the Channel dropdown list to enable the system to select a clear channel during boot up as your operating channel.

Ensure that ASUS 802.11g APs sharing the same channel (or channels which are close in number) are as far away from each other as possible, based on the results of your site survey of the facility. Obtain the site survey utility on the ASUS 802.11g AP support CD.

Wireless Mode

Select any of these options from the dropdown list to set up the 802.11g interface mode:

*Auto: Select this option to allow 802.11g and 802.11b clients to connect to the ASUS 802.11g AP.

*54g Only: Select this option to maximize performance, but this option prevents 802.11b clients from connecting to the ASUS 802.11g AP.

If "54 Protection" checkbox is ticked, G-Mode protection of 11g traffic is automatically enabled in the presence of 11b traffic.

Authentication Method

This field enables you to set different authentication methods which determine different encryption schemes. The relationship between Authentication Method, WPA Encryption, WPA Pre-Shared Key, WEP Encryption, Passphrase, and WEP Keys is listed in the following table. If all your clients support WPA, using "WPA-PSK" is recommended for better security.

Authentication Method	WPA / WEP Encryption	WPA Pre-Shared Key Passphrase	WEP Key 1–4
Open or shared key	None WEP (64 bits) WEP (128 bits)	Not required 1–64 characters 1–64 characters	Not required 10 hex 26 hex
Shared key	WEP (64 bits) WEP (128 bits)	1–64 characters 1–64 characters	10 hex 26 hex
WPA–PSK	TKIP only AES only	8–63 characters 8–63 characters	Not required Not required
WPA	TKIP only AES only	Not required Not required	Not required Not required
Radius with 802.1x	Auto WEP (64 bits) WEP (128 bits)	Not required 1–64 characters 1–64 characters	Not required 10 hex 26 hex

WPA Encryption

When “WPA-PSK” authentication method is used, the newly proposed TKIP (Temporal Key Integrity Protocol) or AES encryption schemes are applied.

WPA Pre-Shared Key

When you select “TKIP” or “AES” as the WPA Encyption, this field is used as a password to begin the encryption process. Key in a password with 8 to 63 characters.

WEP Encryption

When you select “Open or Shared Key”, “Shared Key”, or “Radius with 802.11x” authentication methods are selected, traditional WEP encryption is applied.

NOTE: When “WPA” or “WPA-PSK” authentication methods are selected, you still can set WEP encryption for those clients that do not support WPA/WPA-PSK. Please note that Key Index for WEP key is limited to 2 or 3 when both WPA and WEP encryption are supported at the same time.

64/128-bit versus 40/104-bit

The following section explains low-level (64-bit) and high-level (128-bit) WEP Encryption schemes:

64-bit WEP Encryption

64-bit WEP and 40-bit WEP refer to the same encryption level and can interoperate in a wireless network. This level of WEP encryption uses a 40-bit (10 Hex character) encryption scheme as a secret key, which is set by the user, and a 24-bit “Initialization Vector” scheme, which is not under user control.

Together these two schemes make a 64-bit (40 + 24) encryption scheme. Some vendors refer to this level of WEP as 40-bit and others refer to this as 64-bit. ASUS WLAN products use the term 64-bit when referring to this lower level of encryption.

128-bit WEP Encryption

104-bit WEP and 128-bit WEP refer to the same encryption level and can interoperate on a wireless network. This level of WEP encryption uses a 104-bit (26 Hex character) encryption scheme as a secret key which is set by the user, and a 24-bit “Initialization Vector”, which is not under user control.

Together these two schemes make a 128-bit (104 + 24) encryption scheme. Some vendors refer to this level of WEP as 104-bit and others refer to this as 128-bit. ASUS WLAN products use the term 128-bit when referring to this higher level of encryption.

Passphrase

Selecting "WEP-64bits" or "WEP-128bits" in the Encryption field generates four WEP keys automatically. A combination of up to 64 letters, numbers, or symbols is required. Alternatively, leave this field blank and type in four WEP keys manually.

WEP-64bit key: 10 hexadecimal digits (0~9, a~f, and A~F)
WEP-128bit key: 26 hexadecimal digits (0~9, a~f, and A~F)

Note: The ASUS WLAN family of products uses the same algorithm to generate WEP keys, eliminating the need for users to remember passwords and to maintain compatibility between products. However, using this method to generate WEP keys is not as secure as manual assignment.

WEP Key

You can set a maximum of four WEP keys. A WEP key is either 10 or 26 hexadecimal digits (0~9, a~f, and A~F) based on whether you select 64bits or 128bits in the WEP pull-down menu. The ASUS 802.11g AP and ALL of its wireless clients MUST have at least the same default key.

Key Index

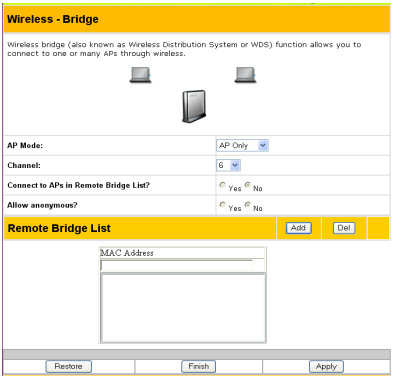
The Default Key field lets you specify which of the four encryption keys you use to transmit data on your wireless LAN. As long as the ASUS 802.11g AP or wireless mobile client with which you are communicating has the same key in the same position, you can use any of the keys as the default key. If the ASUS 802.11g AP and ALL of its wireless clients use the same four WEP keys, select "key rotation" to maximize security. Otherwise, choose one key in common as the default key.

Network Rotation Key Interval

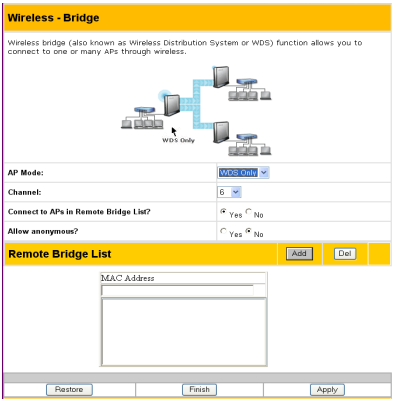
This field specifies the time interval (in seconds) after which a WPA group key is changed. Enter '0' (zero) to indicate that a periodic key-change is not required.

3.7.2 Bridge

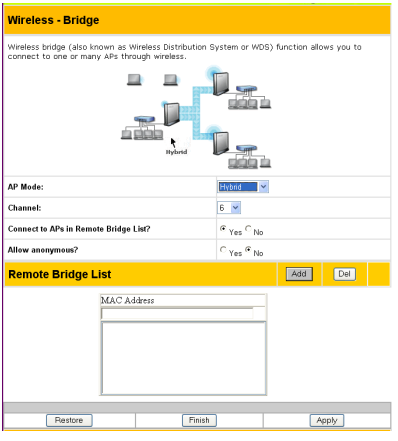
AP Only



WDS Only



Hybrid



Wireless bridge (also known as Wireless Distribution System or WDS) allows you to connect to one or many Access Points.

Access Point

AP Mode configures the ASUS 802.11g AP for a specific purpose. By default, the ASUS 802.11g AP is set to serve as an “Access Point” where a wireless mobile client can connect wirelessly to a wired Ethernet network.

WDS Only

With WDS, the ASUS 802.11g AP can only communicate with other Access Points.

Hybrid

Hybrid allows you to use the ASUS 802.11g AP both as an access point and as a wireless bridge.

Channel

Both Access Points in Wireless Bridge mode must be set to the same channel.

Connect to APs in Remote Bridge List (Yes/No)

Select **Yes** to connect to access points in the remote bridge list.

Allow anonymous? (Yes/No)

Select Yes to allow users without accounts to connect.

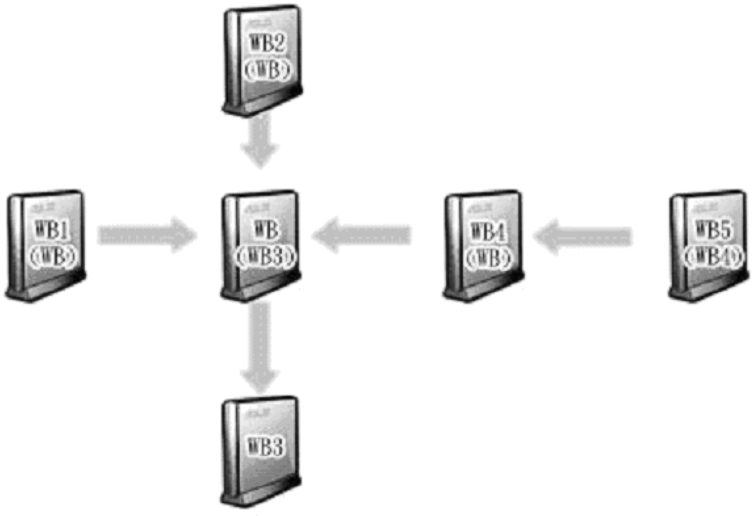
Note: If “Connect to APs in Remote Bridge List” and “Allow Anonymous” are both set to “No”, it means that this AP will not connect with other APs and therefore the AP mode setting will return to “AP Only”.

Remote Bridge List

MAC Address

Enter the MAC address of the target ASUS 802.11g AP in order to designate which ASUS 802.11g AP will be the partner for this ASUS 802.11g AP.

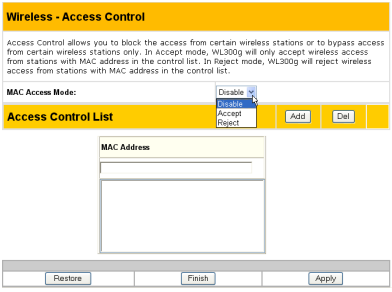
You can setup your wireless environment as shown in this figure:



Note: The content in braces "( )" is the MAC address in the Remote Bridge List of the AP. For example, WB1 have the MAC address of WB in its Remote Bridge List.

In this case, there are six ASUS 802.11g APs and they are linked as wireless bridges. Take one of them, named WB, as an example. WB is not in "AP Only" mode and "Connect to APs in Remote Bridge List" is set as "Yes", so it can connect to WB3. Meanwhile, "Allow anonymous" is set as "Yes" or "Allow anonymous" is set as "No" but it has the MAC addresses of WB1, WB2, and WB4 in the "Remote Bridge List", so it can be connected by WB1, WB2, and WB4.

3.7.3 Access Control



Items in the dropdown list:

Disable (no info required)

Accept (need to input information)

Reject (need to input information)

For better security, you can select to “Accept” or “Reject” wireless clients that connect to the ASUS 802.11g AP.

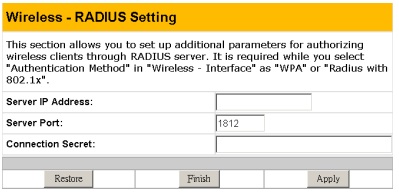
Selecting “Disable” allows all wireless clients to connect to the ASUS 802.11g AP.

Adding a MAC Address

To add a MAC address, key in the MAC address with 12 hexadecimal characters into the “MAC Address” field and click the **Add** button. The new MAC address is listed in the control list below. You can only enter a maximum of 31 MAC addresses into this page.

Note: Click the “Finish” button to save your new settings and restart the ASUS 802.11g AP or click “Save” and restart later.

3.7.4 RADIUS Setting



When you select “WPA” or “Radius with 802.1x” as the authentication method in the **Wireless > Interface** page, the Radius Setting page allows you to set up additional parameters for the Radius Server.

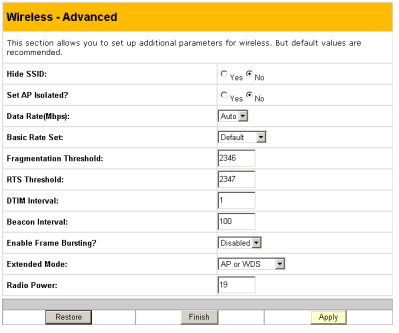
Server IP Address - This field specifies the IP address of the RADIUS server to use for 802.1X wireless authentication and dynamic WEP key derivation.

Server Port - This field specifies the UDP port number used by the RADIUS server.

Connection Secret - This field specifies the password used to initialize a RADIUS connection.

Note: Click “Finish” to save your new settings and restart the ASUS 802.11g AP or click “Save” and restart later.

3.7.5 Advanced



This section allows you to set up additional parameters for the wireless router function. We recommend that you use the default values for all items in this window.

Hide SSID - By default, your ASUS 802.11g AP's SSID is hidden, which allows all wireless clients to connect to your AP. If you select "Yes", your ASUS 802.11g AP will not show in site surveys by wireless mobile clients and they will have to manually enter your ASUS 802.11g AP's SSID. If you want to restrict access to "your" ASUS 802.11g AP , this is a simple way to do it but for security reasons, do not forget to change the SSID to something other than "default".

Set AP Isolated - Select "Yes" to prevent wireless clients from communicating with each other.

Data Rate (Mbps) - This field allows you to specify the transmission rate. Select "Auto" to maximize performance versus distance.

Basic Rate Set - This field indicates the basic rates that wireless clients must support. Use "1 & 2 Mbps" only when backward compatibility is needed for some older wireless LAN cards with a maximum bit rate of 2Mbps.

Fragmentation Threshold (256-2346) – Fragmentation is used to divide 802.11 frames into smaller pieces (fragments) that are sent separately to the destination. Enable fragmentation by setting a specific packet size threshold. If there is an excessive number of collisions on the WLAN, experiment with different fragmentation values to increase the reliability of frame transmissions. The default value (2346) is recommended for normal use.

RTS Threshold (0-2347) – The RTS/CTS (Request to Send/Clear to Send) function is used to minimize collisions among wireless stations. When RTS/CTS is enabled, the router refrains from sending a data frame until another RTS/CTS handshake is completed. Enable RTS/CTS by setting a specific packet size threshold. The default value (2347) is recommended.

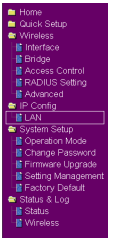
DTIM Interval (1-255) – DTIM (Delivery Traffic Indication Message) is a wireless message used to inform clients in Power Saving Mode when the system should wake up to receive broadcast and multicast messages. Type the time interval in which the system will broadcast a DTIM for clients in Power Saving Mode. The default value (3) is recommended

Beacon Interval (1-65535) – This field indicates the time interval in milliseconds that a system broadcast packet, or beacon, is sent to synchronize the wireless network. The default value (100 milliseconds) is recommended.

Enable Frame Bursting? – This field allows you to enable frame-bursting mode to improve performance with wireless clients that also support frame-bursting.

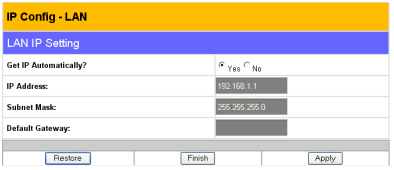
Enable Radio – Radio Power can be set between 1 to 84 but the default value is recommended.

3.8 IP Config



Click this item on the menu to reveal a submenu. Follow the instructions to set up the ASUS 802.11g AP. Tips are given when you move your cursor over each item.

LAN



Yes (no info required)

No (need to input information)

Click **Apply** or **Finish** if you make any changes.

Get IP Automatically

Select Yes (default) or No to get IP address automatically from a DHCP server.

Yes

This parameter determines if the ASUS 802.11g AP will send out a DHCP request during bootup. If you have a DHCP server on the network, set this option so that the ASUS 802.11g AP can receive an automatic IP address assignment.

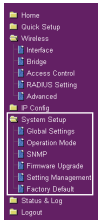
If you have a DHCP (Dynamic Host Configuration Protocol) server on the network, then the DHCP server will automatically assign the ASUS 802.11g AP an IP address when the ASUS 802.11g AP is powered up. To determine what IP address has been assigned to the ASUS 802.11g AP, review the IP address on the “Status” page available on the “Main Menu”.

No

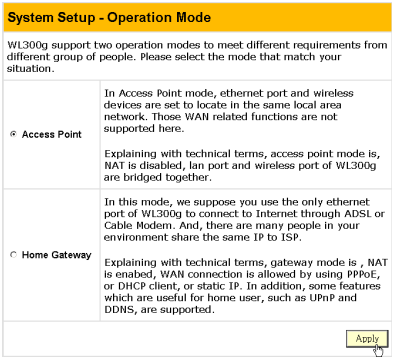
The ASUS 802.11g AP also accepts a static IP address. You may manually configure the IP address and subnet mask on the “IP Config” page. Enter an IP address and a subnet mask in the field provided to assign the ASUS 802.11g AP a static IP address. If you do not know your Gateway setting, leave the field blank (not 0.0.0.0).

3.9 System Setup

Click this item on the menu to reveal a submenu. Follow the instructions to set up the ASUS 802.11g AP. Tips are given when you move your cursor over each item.



3.9.1 Operation Mode



The ASUS 802.11g AP supports two operation modes to meet different requirements. Please select the mode that matches your networking requirements.

Home Gateway

In this mode, an Ethernet cable is used for Internet connection and many clients in the network share the same IP address.

In this mode, NAT is enabled, WAN connection is allowed via PPPoE, DHCP, or manually assigning an IP address. In this mode, UPnP and DDNS functions are supported.

Access Point

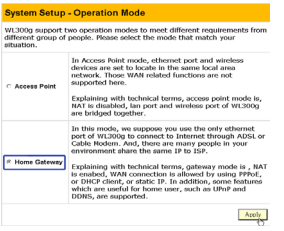
In this mode, the ASUS 802.11g AP and wireless clients are located in the same local area network, and WAN functions are not supported.

In this mode, NAT is disabled, one WAN port and four LAN ports are bridged together.

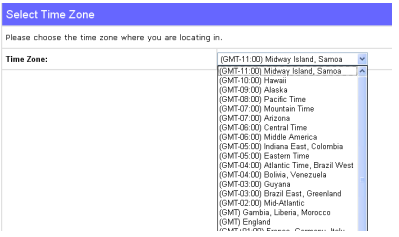
By default, ASUS 802.11g AP operates in Access Mode.

3.9.1.1 Home Gateway Mode

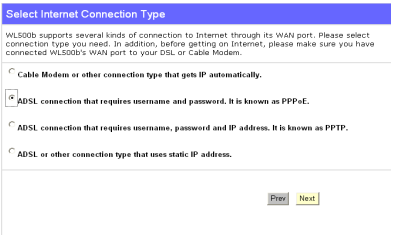
Home Gateway Mode is the default operation mode of the ASUS 802.11g AP. For more details about this mode, refer to section **3.9 System Setup** in this user manual.



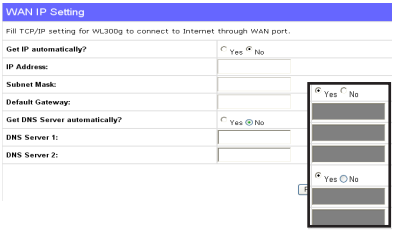
Quick Setup in Home Gateway Mode



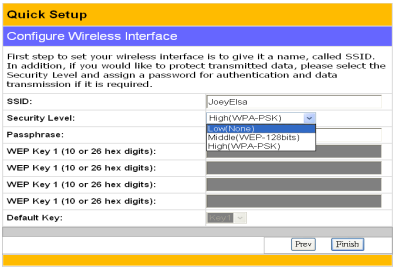
Select your time zone or the closest region. Click **Next** to continue.

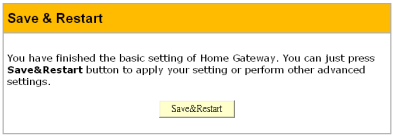


Select the connection type. Click **Next** to continue.



Select “No” to enter the information manually. “Yes” will disable the field. Click **Next** to continue.





To set up your wireless interface, you must first give it an SSID (Service Set Identifier). 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. Since an SSID distinguishes WLANs from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID.

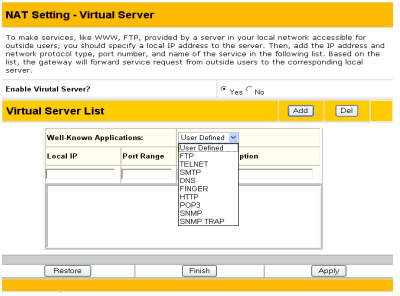
If you want to protect transmitted data, select a middle or high Security Level.

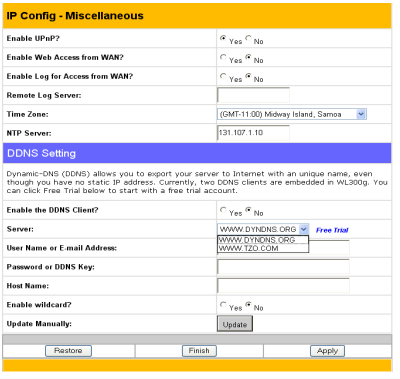
Medium: Only allows those clients with the same WEP key to connect to this access point and to transmit data using 64-bit WEP or 128-bit WEP encryption.

High: Only allows those clients with the same WPA pre-shared key to connect to this access point and to transmit data using TKIP encryption.

Click **Finish** to continue. You are prompted to save the settings. Click **Save&Restart** to save the settings to the ASUS 802.11g AP and enable the new settings.

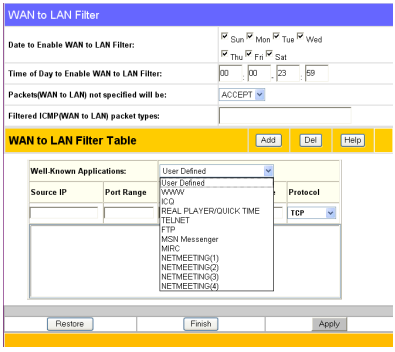
Virtual Server and Dynamic-DNS (DDNS)

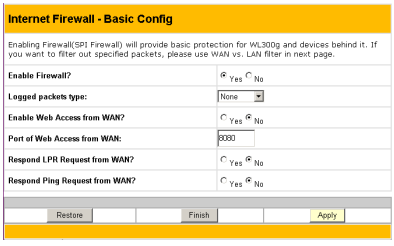




Virtual Server allows you to make LAN services, such as WWW or FTP, accessible to other users outside the network. DDNS allows you to export host names to the Internet through a DDNS service provider. Each time your ASUS 802.11g AP connect to the Internet and get an IP address from an ISP, this function will update your IP address to the DDNS service provider automatically, so that any Internet can access your servers through a pre-defined name registered in a DDNS service provider.

Note: Currently, clients connected to DynDNS or TZO are embedded in ASUS 802.11g AP. You can click Free Trial link on any DDNS service provider in the dropdown list to start with a free trial account.



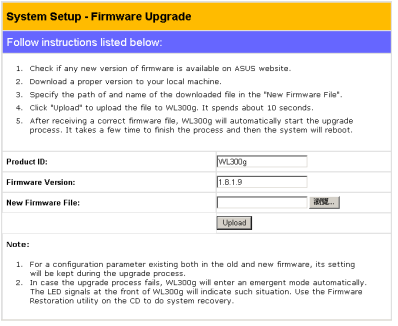


Internet Firewall

LAN & WAN filter allows you to block specified packets between LAN and WAN in a pre-defined time interval. URL filter allows you to block specific URL access from your local network.

Note: The only Ethernet port in ASUS 802.11g AP is used for WAN connection in “Gateway” mode. If you still want to configure ASUS 802.11g AP through Ethernet port, please remember to enable “Web Access from WAN” in “Internet Firewall - Basic Config”.

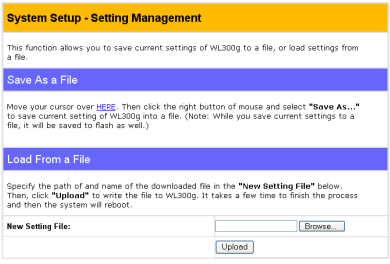
3.9.2 Firmware Upgrade



This page allows you to upgrade your ASUS 802.11g AP's firmware. You can check the ASUS website at www.asus.com for the latest firmware updates.

Note: The firmware upgrade takes approximately 60 to 90 seconds. When the firmware upgrade is completed, you will be directed to the home page.

3.9.3 Setting Management



This function allows you to save current settings to a file, or load settings from a file.

Save As a File

Right-click on the **HERE** link and select **Save As...** to save the current settings into a file.

Note: When current settings are saved to a file, it will be saved to flash as well.

Load From a File

In the **New Setting File** field, click **Browse** to locate the file, and click **Upload** to load the file. It takes a few time to finish the process and then then system will reboot.

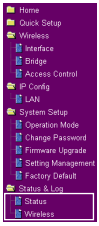
3.9.4 Factory Default

Restoring to the factory default settings

* On the Factory Default page, click **Restore** to clear the system from its current settings and restore it to its factory default settings.

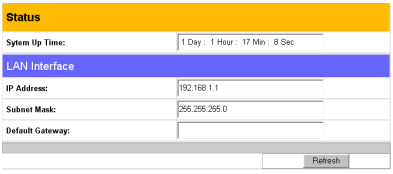
* Use a pen or a paper clip to press the Reset button, located at the back of the ASUS 802.11g AP, for over five seconds until the AP's power LED starts blinking.

3.10 Status & Log

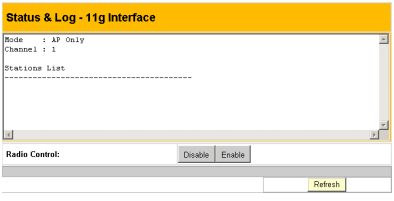


Click this item on the menu to reveal a submenu. Follow the instructions to set up the ASUS 802.11g AP. Tips are given when you move your cursor over each item.

3.10.1 Status



3.10.2 Wireless

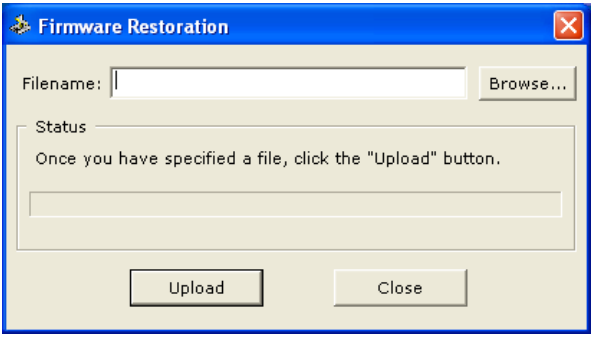


System Up Time

Shows how long the ASUS 802.11g AP has been running since the last bootup.

3.11 Firmware Restoration

Firmware Restoration is a utility that searches for an ASUS 802.11g AP that failed during its firmware upgrading process, then restores or re-uploads the firmware that you specify. The process takes about three to four minutes.



Note: This is not a firmware upgrade utility and cannot be used on a working ASUS 802.11g AP . Normal firmware upgrades must be done through the web interface.

Using a Hub

If you encounter problems uploading a firmware using a network hub, try connecting your computer directly to either a 10Base-T or 10Base-TX LAN (Ethernet) port.

4. Troubleshooting

This troubleshooting guide provides solutions to some common problems that you may encounter while intalling or using the ASUS 802.11g AP. These problems require simple troubleshooting that you can perform by yourself. Contact the ASUS Technical Support if you encounter problems not mentioned in this chapter.

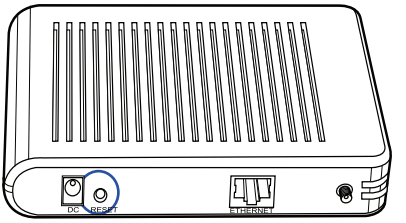
The ASUS 802.11g AP does not power up.

- Check that all cables are properly connected.
- Check if the ASUS 802.11g AP is plugged to the correct power rating.

The client cannot establish a wired connection with the ASUS 802.11g AP.

- Ensure that there are no duplicate IP addresses in the network. Turn off the ASUS 802.11g AP and plug its IP address. Ensure that no other device responds to that address.
- Check that all cables are properly connected and working properly.
- Check that all the devices, such as hub, switch or computer, that the ASUS 802.11g AP is connected to support 10/100Mbps speed.

The ASUS 802.11g AP is not accessible.



If the ASUS 802.11g AP is not accessible, restore it to its factory default settings. Use a pen or paper clip to press the Reset button at the rear panel for over five seconds. The power LED lights up when the AP is successfully restored to its factory default settings.

The following settings are the factory default settings of the ASUS 802.11g AP.

Name	Default Value
Wireless - Interface	
SSID	default
Channel	6
Encryption (WEP)	None
Broadcast SSID	No
Wireless - Bridge	
AP Mode	Access Point Only
Wireless - Access Control	
MAC Access Mode	Disabled
IP Config - LAN	
IP Address	192.168.1.1
Get IP Address Automatically	Yes
Subnet Mask	255.255.255.0
Gateway	(blank)
System Setup - Password	
Operation Mode	Access Point
User Name	admin
Password	admin

My ASUS WLAN Card will not associate with the ASUS AP.

Follow these steps:

1. Ensure that your WLAN Card has the same specifications as the WLAN Access Point.
2. Move the devices closer together. The ASUS WLAN Card may be out of range of the ASUS AP.
3. Ensure that the ASUS AP and ASUS WLAN Card have the same SSID.
4. If encryption is enabled, ensure that both the ASUS AP and the ASUS WLAN Card have the same encryption settings.
5. Ensure that the ASUS AP's Air and Link LEDs are solid green.
6. Ensure that the MAC address of your ASUS WLAN card is in the "Accept" list in your Access Control List. For more details, refer to the section **3.7.3 Access Control in this user manual**.
7. Ensure that your ASUS 802.11g AP is set to Access Point mode.
8. Ensure that both the ASUS AP and the ASUS WLAN card have the same preamble mode.

The throughput seems slow.

- To achieve maximum throughput, verify that your antennas are well-placed, not behind metal, and do not have too many obstacles between them. If you move the client closer to the ASUS AP and throughput increases, you may want to consider adding a second ASUS AP and implementing roaming.
- Check antenna, connectors and cable connections.
- Verify network traffic does not exceed 37% of bandwidth.
- Ensure that the wired network does not exceed ten broadcast messages per second.
- Verify wired network topology and configuration.

The Device Discovery utility cannot find the ASUS AP.

Ensure that your client or computer and the ASUS AP have the same subnet. The default subnet of the ASUS AP is 192.168.1.1

How do I upgrade the ASUS AP's firmware?

Refer to the section **3.9.2 Firmware Upgrade on this user manual**.

5. Appendix

Operating frequency range

The DSSS PHY shall operate in the frequency range of 2.4 GHz to 2.4835 GHz as allocated by regulatory bodies in the USA and Europe or in the 2.471 GHz to 2.497 GHz frequency band as allocated by regulatory authority in Japan.

Number of operating channels

The channel center frequencies and CH ID numbers shall be as shown below. The FCC (US), IC (Canada), and ETSI (Europe) specify operation from 2.4 GHz to 2.4835 GHz. For Japan, operation is specified as 2.471 GHz to 2.497 GHz. France allows operation from 2.4465 GHz to 2.4835 GHz, and Spain allows operation from 2.445 GHz to 2.475 GHz. For each supported regulatory domain, all channels marked with “Yes” shall be supported.

In a multiple cell network topology, overlapping and/or adjacent cells using different channels can operate simultaneously without interference if the distance between the center frequencies is at least 30 MHz. Channel 14 shall be designated specifically for operation in Japan.

Glossary

Access Point (AP)

An networking device that seamlessly connects wired and wireless networks. Access Points combined with a distributed system support the creation of multiple radio cells that enable roaming throughout a facility.

Ad Hoc

A wireless network composed solely of stations within mutual communication range of each other (no Access Point).

AES(Advance Encryption Standard)

AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES. This encryption key protocol is applied in 802.1i standard to improve WLAN security. AES will require new hardware, in contrast with TKIP that can be used on existing wireless devices.

Basic Service Area (BSS)

A set of stations controlled by a single coordination function.

Broadband

A type of data transmission in which a single medium (such as cable) carries several channels of data at once.

Channel

An instance of medium use for the purpose of passing protocol data units that may be used simultaneously, in the same volume of space, with other instances of medium use (on other channels) by other instances of the same physical layer, with an acceptably low frame error ratio due to mutual interference.

Client

A client is the desktop or mobile PC that is connected to your network.

COFDM (for 802.11a or 802.11g)

Signal power alone is not enough to maintain 802.11b-like distances in an 802.11a/g environment. To compensate, a new physical-layer encoding technology was designed that departs from the traditional direct-sequence technology being deployed today. This technology is called COFDM (coded OFDM). COFDM was developed specifically for indoor wireless use and offers performance much superior to that of spread-spectrum solutions. COFDM works by breaking one high-speed data carrier into several lower-speed subcarriers, which are then transmitted in parallel. Each high-speed carrier is 20 MHz wide and is broken up into 52 subchannels, each approximately 300 KHz wide. COFDM uses 48 of these subchannels for data, while the remaining four are used for error correction. COFDM delivers higher data rates and a high degree of multipath reflection recovery, thanks to its encoding scheme and error correction.

Each subchannel in the COFDM implementation is about 300 KHz wide. At the low

end of the speed gradient, BPSK (binary phase shift keying) is used to encode 125 Kbps of data per channel, resulting in a 6,000-Kbps, or 6 Mbps, data rate. Using quadrature phase shift keying, you can double the amount of data encoded to 250 Kbps per channel, yielding a 12-Mbps data rate. And by using 16-level quadrature amplitude modulation encoding 4 bits per hertz, you can achieve a data rate of 24 Mbps. The 802.11a/g standard specifies that all 802.11a/g-compliant products must support these basic data rates. The standard also lets the vendor extend the modulation scheme beyond 24 Mbps. Remember, the more bits per cycle (hertz) that are encoded, the more susceptible the signal will be to interference and fading, and ultimately, the shorter the range, unless power output is increased.

Device Name

Also known as DHCP client ID or network name. Sometimes provided by an ISP when using DHCP to assign addresses.

DHCP (Dynamic Host Configuration Protocol)

This protocol allows a computer (or many computers on your network) to be automatically assigned a single IP address from a DHCP server.

DNS Server Address (Domain Name System)

DNS allows Internet host computers to have a domain name and one or more IP addresses. A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a user enters a domain name into the Internet browser, the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL Modem (Digital Subscriber Line)

A DSL modem uses your existing phone lines to transmit data at high speeds.

Direct-Sequence Spread Spectrum (for 802.11b)

Spread spectrum (broadband) uses a narrowband signal to spread the transmission over a segment of the radio frequency band or spectrum. Direct-sequence is a spread spectrum technique where the transmitted signal is spread over a particular frequency range.

Direct-sequence systems communicate by continuously transmitting a redundant pattern of bits called a chipping sequence. Each bit of transmitted data is mapped into chips and rearranged into a pseudorandom spreading code to form the chipping sequence. The chipping sequence is combined with a transmitted data stream to produce the output signal.

Wireless mobile clients receiving a direct-sequence transmission use the spreading code to map the chips within the chipping sequence back into bits to recreate the original data transmitted by the wireless device. Intercepting and decoding a direct-sequence transmission requires a predefined algorithm to associate the spreading code used by the transmitting wireless device to the receiving wireless mobile client.

This algorithm is established by IEEE 802.11b specifications. The bit redundancy within the chipping sequence enables the receiving wireless mobile client to recreate the original data pattern, even if bits in the chipping sequence are corrupted by interference. The ratio of chips per bit is called the spreading ratio. A high spreading ratio increases the resistance of the signal to interference. A low spreading ratio increases the bandwidth available to the user. The wireless device uses a constant chip rate of 11Mchips/s for all data rates, but uses different modulation schemes to encode more bits per chip at the higher data rates. The wireless device is capable of an 11 Mbps data transmission rate, but the coverage area is less than a 1 or 2 Mbps wireless device since coverage area decreases as bandwidth increases.

Encryption

This provides wireless data transmissions with a level of security.

Extended Service Set (ESS)

A set of one or more interconnected basic service set (BSSs) and integrated local area networks (LANs) can be configured as an Extended Service Set.

ESSID (Extended Service Set Identifier)

You must have the same ESSID entered into the gateway and each of its wireless clients. The ESSID is a unique identifier for your wireless network.

Ethernet

The most widely used LAN access method, which is defined by the IEEE 802.3 standard. Ethernet is normally a shared media LAN meaning all devices on the network segment share total bandwidth. Ethernet networks operate at 10Mbps using CSMA/CD to run over 10-BaseT cables.

Firewall

A firewall determines which information passes in and out of a network. NAT can create a natural firewall by hiding a local network's IP addresses from the Internet. A Firewall prevents anyone outside of your network from accessing your computer and possibly damaging or viewing your files.

Gateway

A network point that manages all the data traffic of your network, as well as to the Internet and connects one network to another.

IEEE

The Institute of Electrical and Electronics Engineers. The IEEE sets standards for networking, including Ethernet LANs. IEEE standards ensure interoperability between systems of the same type.

IEEE 802.11

IEEE 802.xx is a set of specifications for LANs from the Institute of Electrical

and Electronic Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Infrared. 802.11 specifies a carrier sense media access control and physical layer specifications for 1 and 2 Mbps wireless LANs.

IEEE 802.11a (54Mbits/sec)

Compared with 802.11b: The 802.11b standard was designed to operate in the 2.4-GHz ISM (Industrial, Scientific and Medical) band using direct-sequence spread-spectrum technology. The 802.11a standard, on the other hand, was designed to operate in the more recently allocated 5-GHz UNII (Unlicensed National Information Infrastructure) band. And unlike 802.11b, the 802.11a standard departs from the traditional spread-spectrum technology, instead using a frequency division multiplexing scheme that's intended to be friendlier to office environments.

The 802.11a standard, which supports data rates of up to 54 Mbps, is the Fast Ethernet analog to 802.11b, which supports data rates of up to 11 Mbps. Like Ethernet and Fast Ethernet, 802.11b and 802.11a use an identical MAC (Media Access Control). However, while Fast Ethernet uses the same physical-layer encoding scheme as Ethernet (only faster), 802.11a uses an entirely different encoding scheme, called OFDM (orthogonal frequency division multiplexing).

The 802.11b spectrum is plagued by saturation from wireless phones, microwave ovens and other emerging wireless technologies, such as Bluetooth. In contrast, 802.11a spectrum is relatively free of interference.

The 802.11a standard gains some of its performance from the higher frequencies at which it operates. The laws of information theory tie frequency, radiated power and distance together in an inverse relationship. Thus, moving up to the 5-GHz spectrum from 2.4 GHz will lead to shorter distances, given the same radiated power and encoding scheme.

Compared with 802.11g: 802.11a is a standard for access points and radio NICs that is ahead of 802.11g in the market by about six months. 802.11a operates in the 5GHz frequency band with twelve separate non-overlapping channels. As a result, you can have up to twelve access points set to different channels in the same area without them interfering with each other. This makes access point channel assignment much easier and significantly increases the throughput the wireless LAN can deliver within a given area. In addition, RF interference is much less likely because of the less-crowded 5 GHz band.

IEEE 802.11b (11Mbits/sec)

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) adopted the 802.11 standard for wireless devices operating in the 2.4 GHz frequency band. This standard includes provisions for three radio technologies: direct sequence spread spectrum, frequency hopping spread spectrum, and infrared. Devices that comply with the 802.11 standard operate at a data rate of either 1 or 2 Mbps.

In 1999, the IEEE created the 802.11b standard. 802.11b is essentially identical to the 802.11 standard except 802.11b provides for data rates of up to 11 Mbps for direct sequence spread spectrum devices. Under 802.11b, direct sequence devices can operate at 11 Mbps, 5.5 Mbps, 2 Mbps, or 1 Mbps. This provides interoperability with existing 802.11 direct sequence devices that operate only at 2 Mbps.

Direct sequence spread spectrum devices spread a radio signal over a range of frequencies. The IEEE 802.11b specification allocates the 2.4 GHz frequency band into 14 overlapping operating Channels. Each Channel corresponds to a different set of frequencies.

IEEE 802.11g

802.11g is a proposed (to be finalized) new extension to 802.11b (used in majority of wireless LANs today) that broadens 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. 802.11g allows backward compatibility with 802.11b devices but only at 11 Mbps or lower, depending on the range and presence of obstructions.

Infrastructure

A wireless network centered about an access point. In this environment, the access point not only provides communication with the wired network but also mediates wireless network traffic in the immediate neighborhood.

IP (Internet Protocol)

The TCP/IP standard protocol that defines the IP datagram as the unit of information passed across an Internet and provides the basis for connectionless packet delivery service. IP includes the ICMP control and error message protocol as an integral part. It provides the functional equivalent of ISO OSI Network Services.

IP Address

An IP address is a 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

ISM Bands (Industrial, Scientific, and Medicine Bands)

Radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 902 MHz, 2.400 GHz, and 5.7 GHz.

ISP (Internet Service Provider)

An organization that provides access to the Internet. Small ISPs provide service via modem and ISDN while the larger ones also offer private line hookups (T1, fractional T1, etc.).

LAN (Local Area Network)

A communications network that serves users within a defined geographical area. The benefits include the sharing of Internet access, files and equipment like printers and storage devices. Special network cabling (10 Base-T) is often used to connect the PCs together.

MAC Address (Media Access Control)

A MAC address is the hardware address of a device connected to a network.

NAT (Network Address Translation)

NAT masks a local network's group of IP addresses from the external network, allowing a local network of computers to share a single ISP account. This process allows all of the computers on your home network to use one IP address. This will enable access to the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

NIC (Network Interface Card)

A network adapter inserted into a computer so that the computer can be connected to a network. It is responsible for converting data from stored in the computer to the form transmitted or received.

Packet

A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

PCMCIA (Personal Computer Memory Card International Association)

The Personal Computer Memory Card International Association (PCMCIA), develops standards for PC cards, formerly known as PCMCIA cards. These cards are available in three types, and are about the same length and width as credit cards. However, the different width of the cards ranges in thickness from 3.3 mm (Type I) to 5.0 mm (Type II) to 10.5 mm (Type III). These cards can be used for various functions, including memory storage, land line modems and wireless modems.

PPP (Point-to-Point Protocol)

PPP is a protocol for communication between computers using a serial interface, typically a personal computer connected by phone line to a server.

PPPoE (Point-to-Point Protocol over Ethernet)

Point-to-Point Protocol is a method of secure data transmission. PPP using Ethernet to connect to an ISP.

Radio Frequency (RF) Terms: GHz, MHz, Hz

The international unit for measuring frequency is Hertz (Hz), equivalent to the older unit of cycles per second. One megahertz (MHz) is one million Hertz. One gigahertz (GHz) is one billion Hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55-1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and wireless 802.11 LANs operate at 2.4 GHz.

RIP (Routing Information Protocol)

Routing Information Protocol(RIP1) is defined as a means by which routing equipment can find the best path for transmitting data packets from one network to another. Upgrades have been made to the RIP1 protocol, resulting in Routing Information Protocol Version 2 (RIP2). RIP2 was developed to cover some of the inefficiencies of RIP1.

Metric: RIP metric is a value of distance for the network. Usually RIP increments the metric when the network information is received. Redistributed routes' default metric offset is set to 1. These rules can be used to change the metric offset only for the matched networks specified or excluded in the Route Metric Offset table. But the metric offset of other networks is still set to 1.

SSID (Service Set ID)

SSID is a group name shared by every member of a wireless network. Only client PCs with the same SSID are allowed to establish a connection.

Station

Any device containing IEEE 802.11 wireless medium access conformity.

Subnet Mask

A subnet mask is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network.

TCP (Transmission Control Protocol)

The standard transport level protocol that provides the full duplex, stream service on which many application protocols depend. TCP allows a process or one machine to send a stream of data to a process on another. Software implementing TCP usually resides in the operating system and uses the IP to transmit information across the network.

TKIP (Temporal Key Integrity Protocol)

TKIP is used in WPA to replace WEP with a new encryption algorithm that is stronger than the WEP algorithm but that uses the calculation facilities present on existing wireless devices to perform encryption operations.

WAN (Wide Area Network)

A system of LANs, connected together. A network that connects computers located in separate areas, (i.e., different buildings, cities, countries). The Internet is a wide area network.

WECA (Wireless Ethernet Compatibility Alliance)

An industry group that certifies cross-vender interoperability and compatibility of IEEE 802.11b wireless networking products and to promote that standard for enterprise, small business, and home environments.

WEP (Wired Equivalent Privacy)

The IEEE 802.11b standard specifies an optional encryption feature, known as Wired Equivalent Privacy or WEP, that is designed to provide a wireless LAN with a security level equal to what is found on a wired Ethernet network. WEP encrypts the data portion of each packet exchanged on the 802.11b network using either a 64-bit or 128-bit encryption algorithm. In addition, WEP is also used in conjunction with the optional Shared Key Authentication algorithm to prevent unauthorized devices from associating with an 802.11b network.

WLAN (Wireless Local Area Network)

This is a group of computers and other devices connected wirelessly in a small area. A wireless network is referred to as LAN or WLAN.

WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access is a specification, which offsets encryption and authentication improvements that are stronger than the Wireless Encryption Protocol (WEP), which it is meant to replace.

WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key)

WPA-PSK is a special mode of WPA for home environment without a Remote Authentication Dial-In User Service (RADIUS). It is required to enter a password into their access point or home wireless gateway and each clients that is on the wireless network to keeps out eavesdroppers and other unauthorized users by requiring all devices to have the matching password.

6. Safety Information

Federal Communications Commission

This device complies with FCC Rules Part 15. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this 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.

WARNING! The use of a shielded-type power cord is required in order to meet FCC emission limits and to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used. Use only shielded cables to connect I/O devices to this equipment. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Reprinted from the Code of Federal Regulations #47, part 15.193, 1993. Washington DC: Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office.

FCC Radio Frequency Interference Requirements

MPE Statement: Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal.

This device is restricted to INDOOR USE due to its operation in the 5.15 to 5.25GHz frequency range. FCC requires this product to be used indoors for the frequency range 5.15 to 5.25GHz to reduce the potential for harmful interference to co-channel of the Mobile Satellite Systems.

High power radars are allocated as primary user of the 5.25 to 5.35GHz and 5.65 to 5.85GHz bands. These radar stations can cause interference with and / or damage this device.

FCC RF Exposure Guidelines (Access Points)

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247(b)(4) addressing RF Exposure from radio frequency devices. The radiation output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation – as a mobile or portable device but use in a body-worn way is strictly prohibit. When using this device, a certain separation distance between antenna and nearby persons has to be kept to ensure RF exposure compliance. In order to comply with the RF exposure limits established in the ANSI C95.1 standards, Access Point equipment should be installed and operated with minimum distance **[20cm]** between the radiator and your body. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

CAUTION: Any changes or modifications not expressly approved in this manual could void your authorization to use this device.

FCC RF Exposure Guidelines (Wireless Cards)

This device has been tested for compliance with FCC RF Exposure (SAR) limits in typical portable configurations.

In order to comply with SAR limits established in the ANSI C95.1 standards, it is recommended when using a WLAN Card adapter that the integrated antenna is positioned more than **[2.5cm]** from your body or nearby persons during extended periods of operation. If the antenna is positioned less than **[2.5cm]** from the user, it is recommended that the user limit the exposure time.

Canadian Department of Communications

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Operation Channel for Different Domains

N. America	2.412-2.462 GHz	Ch01 through CH11
Japan	2.412-2.484 GHz	Ch01 through Ch14
Europe ETSI	2.412-2.472 GHz	Ch01 through Ch13
France	2.457-2.472 GHz	Ch10 through Ch13

France Restricted Frequency Band

Some areas of France have a restricted frequency band. The worst case maximum authorized power indoors is:

- 10mW for the entire 2.4 GHz band (2400 MHz–2483.5 MHz)
- 100mW for frequencies between 2446.5 MHz and 2483.5 MHz

NOTE: Channels 10 through 13 inclusive operate in the band 2446.6 MHz to 2483.5 MHz.

There are few possibilities for outdoor use: On private property or on the private property of public persons, use is subject to a preliminary authorization procedure by the Ministry of Defense, with maximum authorized power of 100mW in the 2446.5–2483.5 MHz band. Use outdoors on public property is not permitted.

In the departments listed below, for the entire 2.4 GHz band:

- Maximum authorized power indoors is 100mW
- Maximum authorized power outdoors is 10mW

Departments in which the use of the 2400–2483.5 MHz band is permitted with an EIRP of less than 100mW indoors and less than 10mW outdoors:

01 Ain Orientales	36 Indre	66 Pyrénées
02 Aisne	37 Indre et Loire	67 Bas Rhin
03 Allier	41 Loir et Cher	68 Haut Rhin
05 Hautes Alpes	42 Loire	70 Haute Saône
08 Ardennes	45 Loiret	71 Saône et Loire
09 Ariège	50 Manche	75 Paris
11 Aude	55 Meuse	82 Tarn et Garonne
12 Aveyron	58 Nièvre	84 Vaucluse
16 Charente	59 Nord	88 Vosges
24 Dordogne	60 Oise	89 Yonne
25 Doubs	61 Orne	90 Territoire de Belfort
26 Drôme	63 Puy du Dôme	94 Val de Marne
32 Gers	64 Pyrénées Atlantique	

This requirement is likely to change over time, allowing you to use your wireless LAN card in more areas within France. Please check with ART for the latest information (www.art-telecom.fr)

NOTE: Your ASUS WLAN Card transmits less than 100mW, but more than 10mW.

Licensing Information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License.

Please see The GNU General Public License for the exact terms and conditions of this license.

Specially, the following parts of this product are subject to the GNU GPL:

- The Linux operating system kernel
- The iptables packet filter and NAT software
- The busybox swiss army knife of embedded linux
- The zebra routing daemon implementation
- The udhcpd DHCP client/server implementation
- The pptp-linux PPTP client implementation
- The rp-pppoe PPPoE client implementation
- The pppd PPP daemon implementtion
- The dproxy DNS proxy implementation
- The bridge-utils package

All listed software packages are copyright by their respective authors. Please see the source code for detailed information.

Availability of source code

ASUSTek COMPUTER Inc. has eposed the full source code of the GPL licensed software, including any scripts to control compilation and installation of the object code. All future firmware updates will also be accompanied with their respective source code. For more information on how ou can obtain our open source code, please visit our web site.

The GNU General Public License

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, he GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any ther program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to reedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can chnge the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restritions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that ou have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gies you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by soeone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by sftware patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's ree use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any proram or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means eitherthe Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitaton in the term “modification”.) Each licensee is addressed as “you”.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the otput from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copis of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and o the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchang for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all ofthese conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or s derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started unning for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute th program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License,

and its terms, d not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissons for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to xercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storageor distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provded that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to bedistributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowe only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modificationsto it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a spcial exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that omponent itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of te source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to cop, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as sch parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibite by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifing the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these trms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgmentor allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the coditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license ould not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   I any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this sectin to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public licens practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute softare through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restrictd in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permtted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public Licens from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of his License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number f this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permision. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our fre software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATEDIN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TH ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRTING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO SE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OFTHE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS