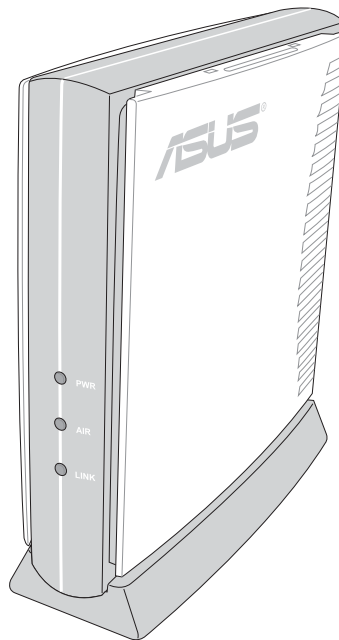




802.11g Access Point

WL-300g

(For 802.11g and 802.11b Wireless Clients)



User's Manual

Copyright Information

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK COMPUTER INC. ("ASUS").

ASUS PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ASUS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE), EVEN IF ASUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification or alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ASUS. ASUS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Copyright © 2003 ASUSTeK COMPUTER INC. All Rights Reserved.

Product Name:	ASUS 802.11g AP (WL-300g)
Manual Revision:	2 E1378
Release Date:	July 2003

ASUSTeK COMPUTER INC. (Asia-Pacific)

Address: 150 Li-Te Road, Peitou, Taipei, Taiwan 112
General Tel: +886-2-2894-3447
General Fax: +886-2-2894-3449
Web Site: www.asus.com.tw

Technical Support

MB/Others (Tel): +886-2-2890-7121 (English)
Notebook (Tel): +886-2-2890-7122 (English)
Desktop/Server (Tel): +886-2-2890-7123 (English)
Support Fax: +886-2-2890-7698

ASUS COMPUTER INTERNATIONAL (America)

Address: 44370 Nobel Drive, Fremont, CA 94538, USA
General Fax: +1-502-933-8713
General Email: tmd1@asus.com
Web Site: usa.asus.com

Technical Support

Support Fax: +1-502-933-8713
General Support: +1-502-995-0883
Notebook Support: +1-510-739-3777 x5110
Support Email: tsd@asus.com

ASUS COMPUTER GmbH (Germany and Austria)

Address: Harkortstr. 25, 40880 Ratingen, BRD, Germany
General Email: sales@asuscom.de (for marketing requests only)
General Fax: +49-2102-9599-31
Web Site: www.asuscom.de

Technical Support

Components: +49-2102-9599-0
Notebook PC: +49-2102-9599-10
Support Fax: +49-2102-9599-11
Support Email: www.asuscom.de/support (for online support)

ASUSTeK COMPUTER (Middle East and North Africa)

Address: P.O. Box 64133, Dubai, U.A.E.
General Tel: +9714-283-1774
General Fax: +9714-283-1775
Web Site: www.ASUSarabia.com

Table of Contents

1. Introduction	7
Overview	7
The ASUS Wireless LAN Family	8
System Requirements	10
Wireless Performance	11
Site Topography	11
Range	11
Site Surveys	11
Roaming Between ASUS APs	12
Roaming Guidelines	12
ASUS 802.11g AP Status Indicators	13
Power Requirements	13
2. Installation	14
Installation Procedure	14
Wall Mounting Option	15
3. Software Configuration	17
Configuring the ASUS 802.11g AP	17
Installing the ASUS WLAN Utilities	19
ASUS WLAN Utilities	20
Connecting to the ASUS WLAN Web Manager	20
Device Discovery	21
User Name and Password	22
Home Page	22
Access Point Mode	23
Quick Setup	24
Configure Wireless Interface	24
Wireless	25
Interface	25
Wireless	31
Bridge	31
Wireless	34
Access Control	34
Wireless	35
RADIUS Setting	35
Wireless	36
Advanced	36
IP Config	37
LAN	37

Table of Contents

Get IP Automatically	37
Yes	37
No	37
System Setup	38
Operation Mode	38
Home Gateway	39
Quick Setup	39
System Setup	43
Change Password	43
System Setup	44
Firmware Upgrade	44
System Setup	45
Setting Management	45
System Setup	46
Factory Default	46
Restoring Factory Default Settings	46
Status & Log	47
Status	47
LAN Interface	47
Wireless	47
Firmware Restoration	48
Using a Hub	48
4. Troubleshooting	49
Common Problems and Solutions	49
Reset to Defaults	50
5. Appendix	53
External Antenna Connector	53
Operating frequency range	54
Number of operating channels	54
DSSS PHY frequency channel plan	54
Glossary	55

6. Safety Information	64
Federal Communications Commission	64
FCC Radio Frequency Interference Requirements	65
FCC RF Exposure Guidelines (Access Points)	65
FCC RF Exposure Guidelines (Wireless Cards)	66
Canadian Department of Communications	66
Operation Channel for Different Domains	66
France Restricted Frequency Band	67
Appendix - GNU General Public License	69
Licensing Information	69
Availability of source code	69
The GNU General Public License	70

1. Introduction

Overview

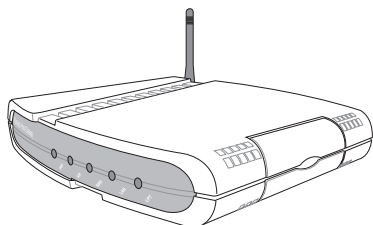
Thank you for purchasing the ASUS 802.11g WLAN AP. The ASUS 802.11g AP is an Access Point designed to be fully compliant with IEEE pre 802.11g and 802.11b standards. 802.11g is a proposed (to be finalized) new extension to 802.11b (used in majority of wireless LANs today) that broadens 802.11b's data 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.

Wireless LANs are complementary extensions to existing wired LANs, offering complete mobility while maintaining continuous network connectivity to both corporate and home Intranets. They add a new level of convenience for LAN users. PC users stay connected to the network anywhere throughout a building without being bound by a LAN wires. This is accomplished through the use of ASUS Access Points. ASUS Access Points with built-in Internet gateway capability, allows your family to share a broadband Modem and one ISP account simultaneously from different rooms without wires! ASUS WLAN products can keep you connected anywhere, any time.

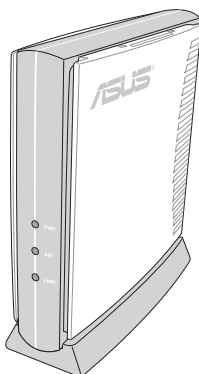
Chapter 1 - Introduction

The ASUS Wireless LAN Family

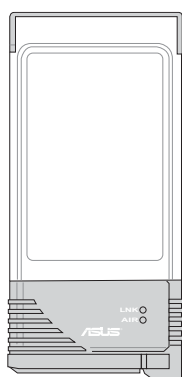
The ASUS Wireless LAN family contains a complete solution for wireless local area networks in the office or at home.



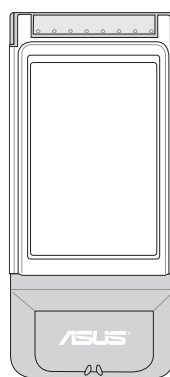
The **ASUS WLAN 802.11b Gateway (WL-500)** creates a wireless network using the IEEE 802.11b wireless standard and allows sharing a single Internet connection.



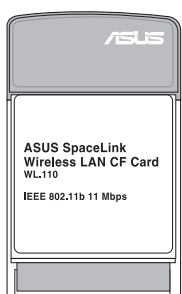
The **ASUS WLAN 802.11b Access Point (WL-300)** creates a wireless network using the IEEE 802.11b wireless standard.



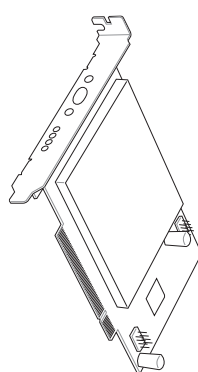
The **ASUS WLAN 802.11b WLAN Card (WL-100)** is a IEEE 802.11b wireless LAN adapter that fits into a PCMCIA Type II slot in a Notebook PC.



The **ASUS WLAN 802.11b/a Cardbus Card (WL-200)** is a dual band (IEEE 802.11a/b) wireless LAN adapter that fits into a Notebook PC's PCMCIA Type II slot with Cardbus support.

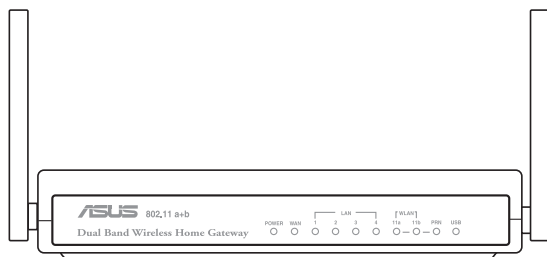


The **ASUS WLAN 802.11b CF Card (WL-110)** is a IEEE 802.11b wireless LAN adapter that fits into a Compact Flash Type II slot in a Portable Digital Assistant (PDA).

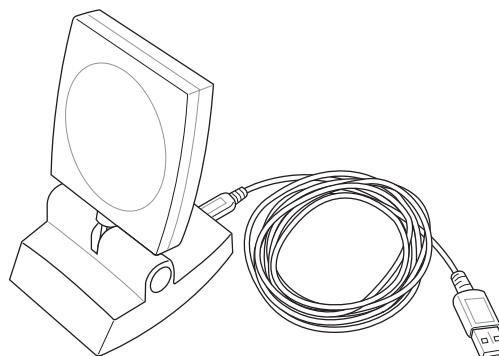


The **ASUS WLAN 802.11b/a PCI Card (WL-230)** is a dual band (IEEE 802.11a/b) wireless PCI card that also supports Bluetooth connections.

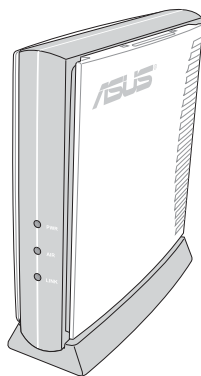
The above illustrations are not to scale.



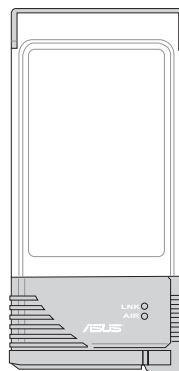
The **ASUS WLAN 802.11b/a Router (WL-600)** creates a wireless network using the IEEE 802.11b and 802.11a wireless standards and allows sharing a single Internet connection.



The **ASUS WLAN 802.11b USB Client (WL-140)** is an IEEE 802.11b wireless USB LAN adapter that connects to any computer's USB port with the benefit of being able to place the antenna above obstructions in order to maximize signal strength.



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



The **ASUS WLAN 802.11g WLAN Card (WL-100g)** is a IEEE pre 802.11g and 802.11b wireless LAN adapter that fits into a PCMCIA Type II slot in a Notebook PC.

The above illustrations are not to scale.

System Requirements

To begin using the ASUS 802.11g WLAN AP, you must have the following minimum requirements:

- An Ethernet (10Base-T or 10/100Base-TX) adapter for wired client
- At least one 802.11g (54Mbps) or one 802.11b (11Mbps) wireless adapter for wireless mobile clients
- TCP/IP and an Internet browser installed

The Product Package

Each ASUS 802.11g AP comes with:

- One ASUS 802.11g WLAN Access Point
- One ASUS 802.11g WLAN Access Point Quick Start Guide
- One power adapter (5 Volts DC, 1 Amp)
- One support CD (utilities and user's manual)
- One RJ-45 Ethernet cable (straight-through)
- One Bracket for ceiling mounting
- One Bracket for office partition mounting
- One Sticker for wall mounting alignment

Wireless Performance

This section provides the user with ideas for how to improve the performance of a ASUS WLAN network.

Site Topography

For optimal performance, locate wireless mobile clients and the ASUS AP s 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 AP s in open areas or add the ASUS AP s as needed to improve coverage.

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

Range

Every environment is unique with different obstacles, barriers, materials, etc. and, therefore, it is difficult to determine the exact range that will be achieved without testing. However, has developed some guidelines to estimate the range that users will see when the product is installed in their facility, 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 two devices have a line of sight, meaning they see each other with no obstacles. However, 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. Therefore, a client that is close to the ASUS AP may operate at higher speeds while a client that is on the fringe of coverage may operate at lower speeds. 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.

Site Surveys

A site survey (utility provided with the ASUS WLAN Cards) analyzes the installation environment and provides users with recommendations for equipment and its placement. The optimum placement differ depending on the ASUS AP design and specifications.

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. This is also known as a 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."

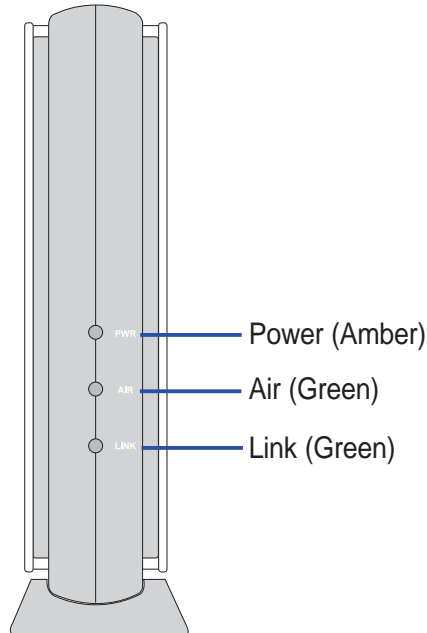
Multiple ASUS APs connected to a common Ethernet network form an Extended Service Set (ESS). All members of an Extended Service Set are configured with an ID, known as the SSID or ESSID. Wireless mobile clients must be configured with the same SSID as the ASUS APs on the network; a client can only roam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

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(s) 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.

ASUS 802.11g AP Status Indicators

There are three LEDs on the front of the ASUS 802.11g WLAN AP, as shown here.



Power LED

OFF: No power or performing boot sequence
ON: System ready
Blinking: Firmware upgrade failed

Air LED

OFF: No power
ON: Wireless function ready
Blinking: Transmitting or receiving data (wireless)

Link LED

OFF: No power
ON: Has physical connection to an Ethernet network
Blinking: Transmitting or receiving data (through Ethernet wire)

Power Requirements

The ASUS 802.11g AP requires power from an external power supply. The ASUS 802.11g AP ships with a UL listed, Class 2 power supply (5V, 1A).

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.

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.

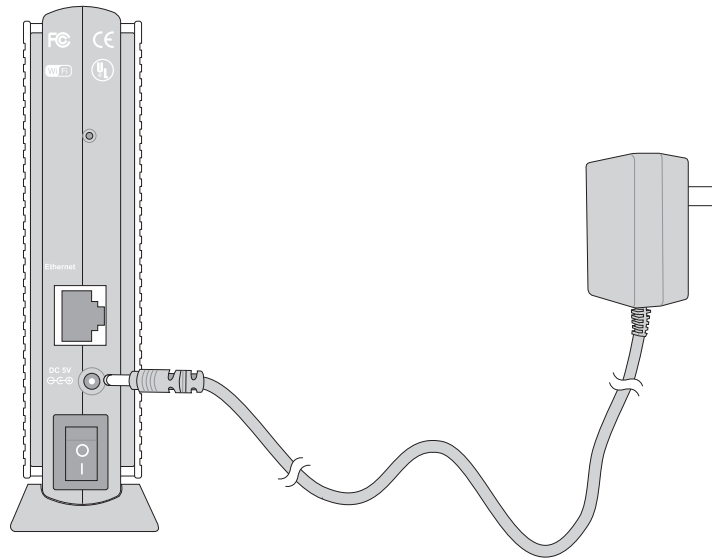


Note: It is the responsibility of the installer and users of the ASUS 802.11g AP to guarantee that the antenna is operated at least 20 centimeters from any person. This is necessary to insure that the product is operated in accordance with the RF Guidelines for Human Exposure which have been adopted 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 entitled “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).

Chapter 2 - Hardware Installation

4. Attach one end of the AC power adapter, included in the product package, to the back of the ASUS 802.11g AP and the other end to a power outlet.



Note: Use the Access Point only with the power adapter supplied 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.

Wall Mounting Option

Out of the box, the ASUS 802.11g AP is designed to sit on a raised flat surface like a file cabinet or book shelf. The unit may also be converted for mounting to a wall or ceiling.

Follow these steps to mount the Access Point to a wall:

1. Remove the base by pressing the tab and sliding the base.
2. Remove the side cover to expose the mounting hooks.
3. Locate the screws provided with the Access Point.
4. Mark two holes in a flat surface using the provided hole template.
5. Tighten the two provided screws until only 1/4" is showing.
6. Latch the Access Point onto the two screws.

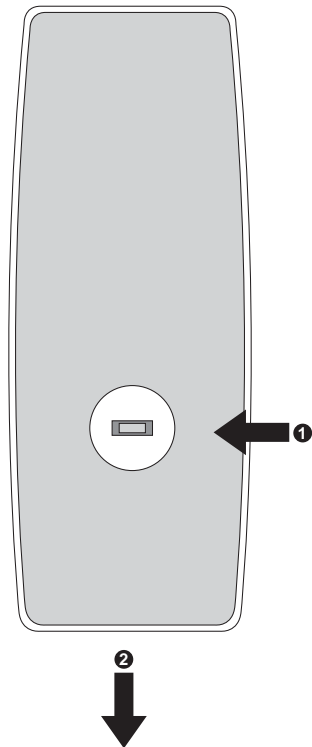


Note: Readjust the screws if you cannot latch the Access Point onto the screws or if it is too loose.

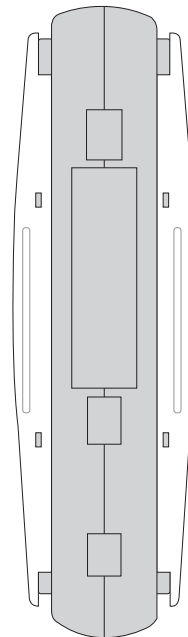
Chapter 2 - Hardware Installation

Step 1

Before:

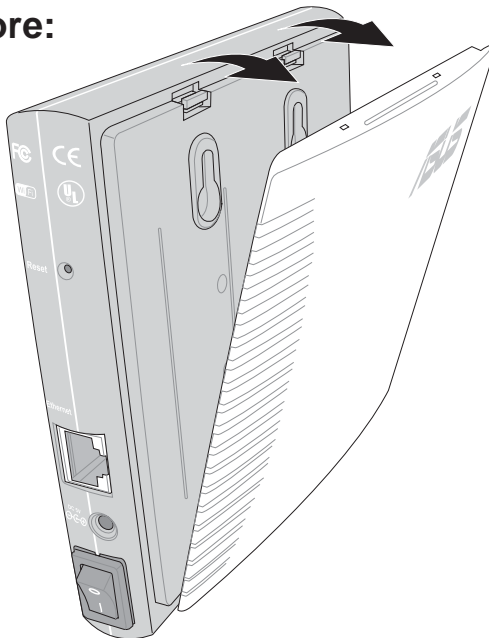


After:

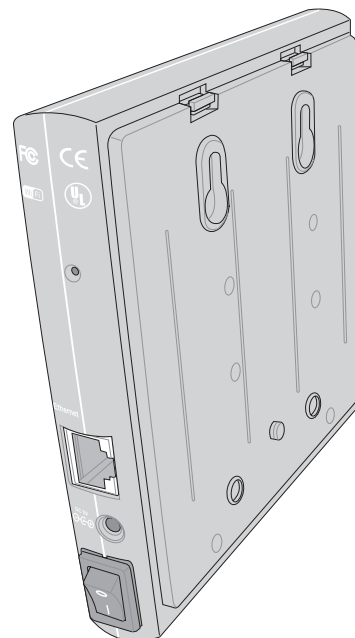


Step 2

Before:



After:



Note: Mounting brackets are provided for you to hang the ASUS 802.11g AP on an office partition or office ceiling.

3. Software Configuration

Configuring the ASUS 802.11g AP

The ASUS 802.11g AP can be configured to meet various usage scenarios. Some of the factory default settings may suit your usage; however, others may need changing. Prior to using the ASUS 802.11g AP, you must check the basic settings to guarantee it will work in your environment.

Configuring the ASUS 802.11g AP is done 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, e.g. ASUS WLAN Card, installed in your Notebook PC. You should also disable WEP and set the SSID to “default” for your wireless LAN device.

If you want to configure the ASUS 802.11g AP or want to access the Internet through the ASUS 802.11g AP, TCP/IP settings must be correct. Normally, the TCP/IP setting should be on the IP subnet of 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.

Chapter 3 - Software Configuration

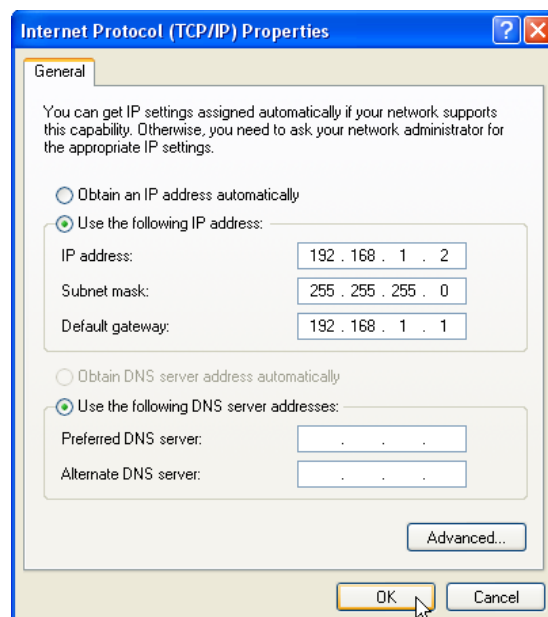
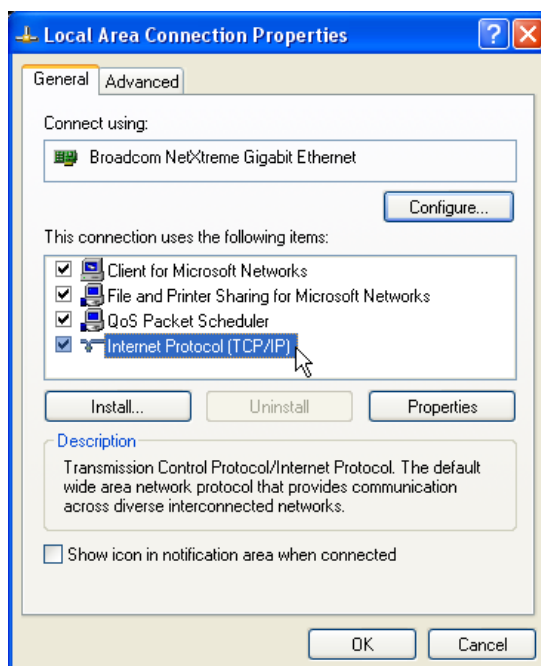
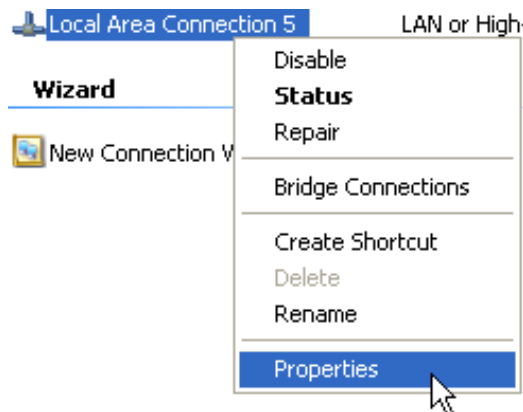
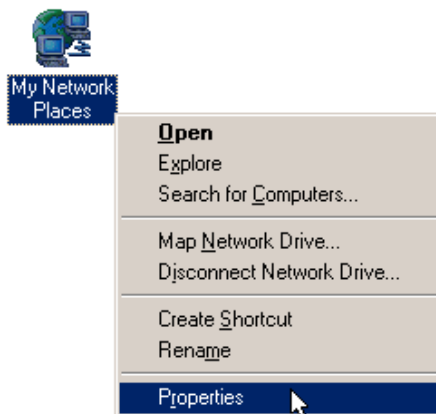
Advanced IP Settings

If you want to set your IP address manually, the following default settings of the ASUS 802.11g AP should be known:

- IP address 192.168.1.1
- Subnet Mask 255.255.255.0.

If you set your computer's IP manually, it needs to be on the same segment. For example:

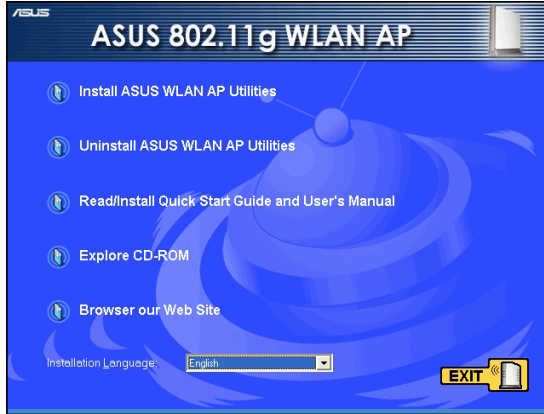
- IP address 192.168.1.xxx (xxx can be any number between 2 and 254 that is not used by another device)
- Subnet Mask 255.255.255.0 (same as the ASUS 802.11g AP)
- Gateway 192.168.1.1 (this is the ASUS 802.11g AP IP address)
- DNS 192.168.1.1 (ASUS 802.11g AP IP address or your own).



Chapter 3 - Software Configuration

Installing the ASUS WLAN Utilities

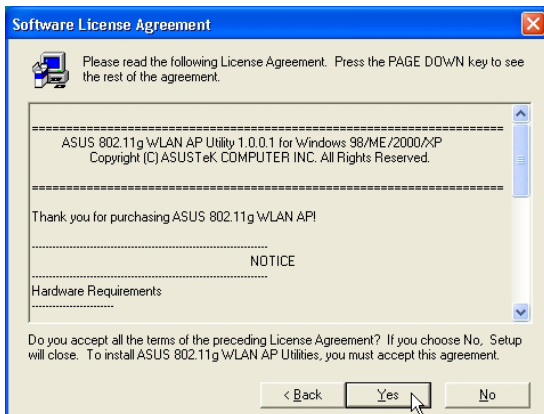
Follow these steps to install the ASUS WLAN Utilities in Microsoft Windows. Insert the support CD. Double-click **setup.exe** (in the root of the support CD) if your autorun has been disabled.



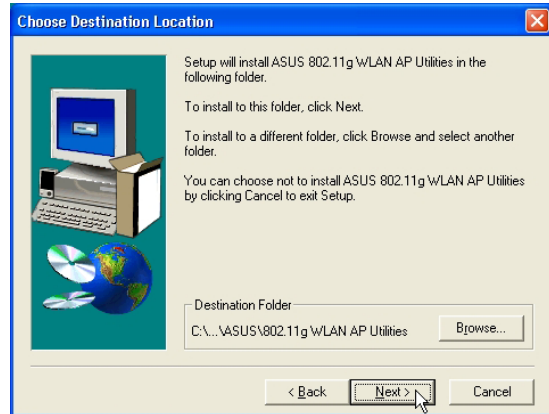
(1) Click **Install...Utilities**.



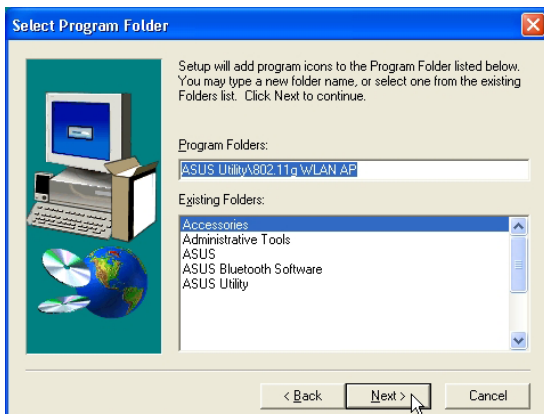
(2) Click **Next** after reading the welcome screen.



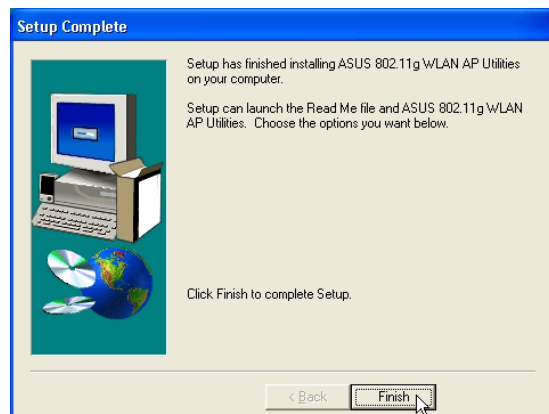
(3) Click **Yes** after reading the license agreement.



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



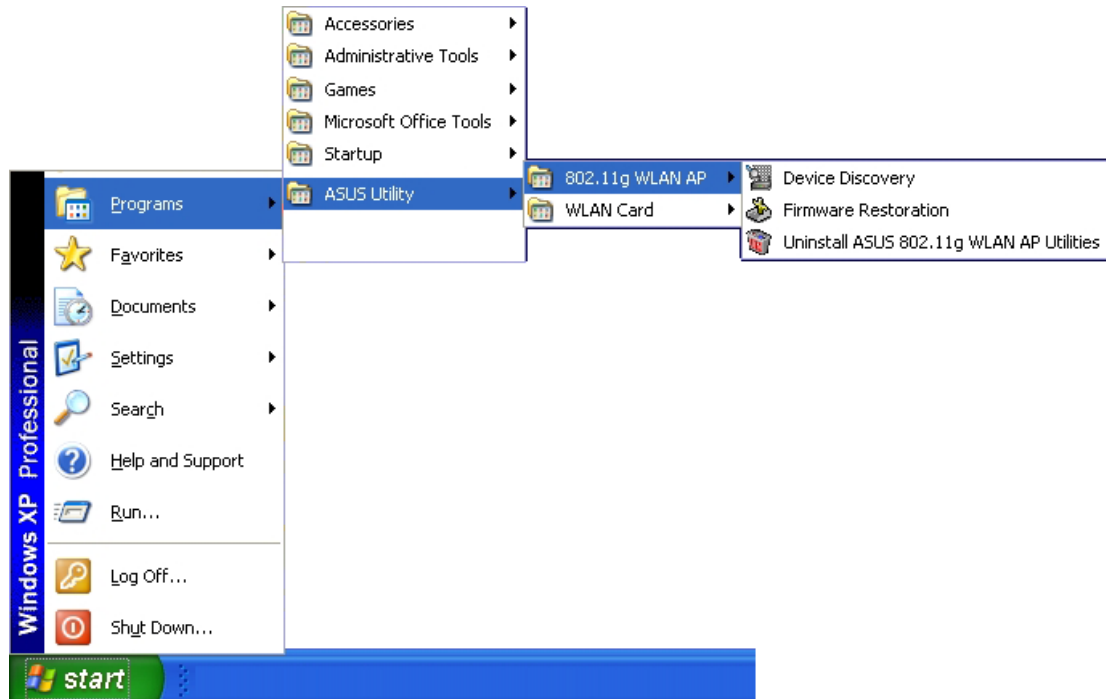
(5) Click **Next** to accept the default program folder or enter another name.



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

ASUS WLAN Utilities

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



Connecting to the ASUS WLAN Web Manager

Wired Ethernet Connection

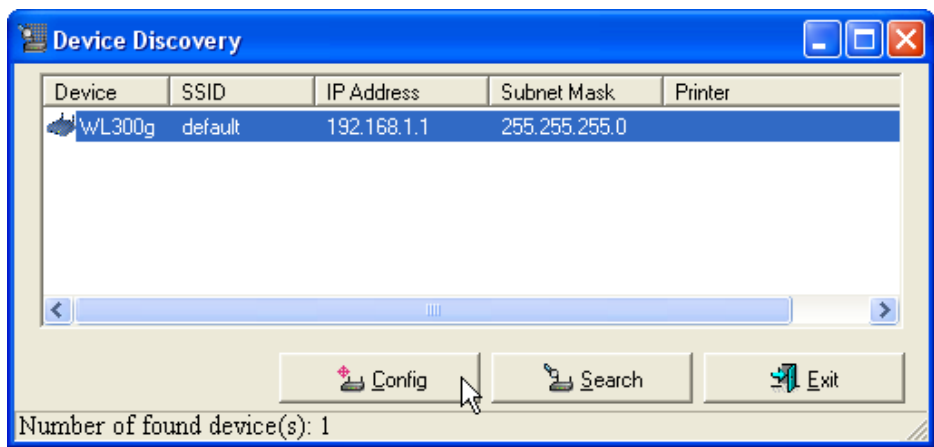
Besides using a network hub, you can also connect a LAN cable from your computer to the ASUS 802.11g AP using either a straight or crossover cable because the ASUS 802.11g AP has auto-crossover capability.

Wireless Connection

If you are using a Notebook PC with a wireless adapter, you can connect to the ASUS WLAN Web Manager without a wired Ethernet connection. Just make sure your TCP/IP settings are set correctly.

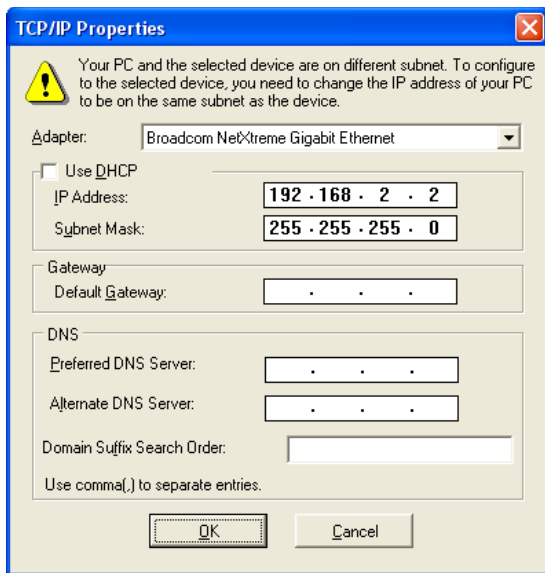
Device Discovery

Run the **ASUS WLAN Device Discovery** from the **Start** menu and click **Config** on the device.



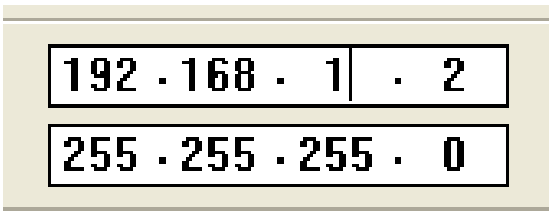
Manually Entering the Address

You can also open your PC's web browser 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.

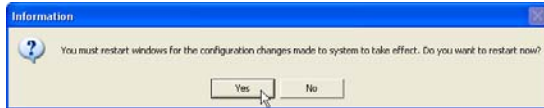


(This is the correct setting.)



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

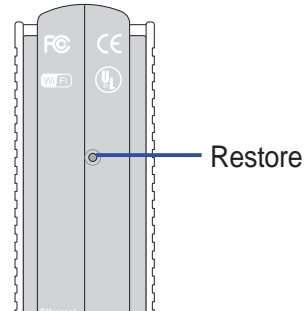
Chapter 3 - Software Configuration



Restart your Windows if you are asked to.



Note: If you cannot find any the ASUS 802.11g APs due to a problem in the IP settings, push and hold the “Restore” button on the ASUS 802.11g AP over five seconds to restore factory default settings.



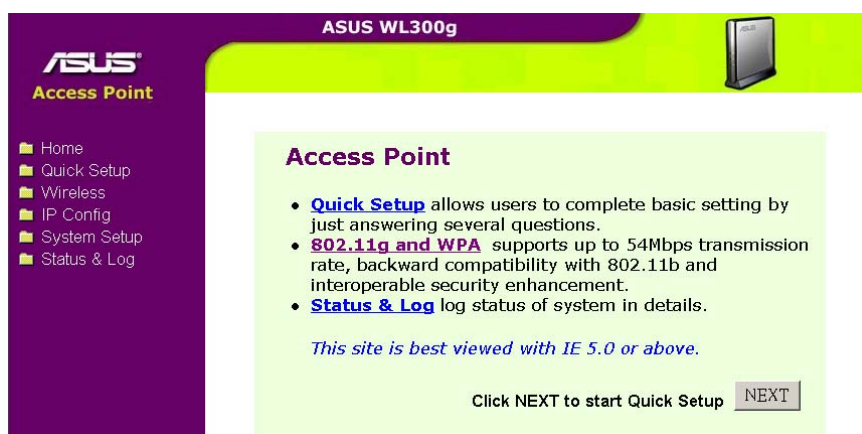
User Name and Password

Once connected, a window will ask for the User name and Password in order to log in. The factory default values are “admin” and “admin”.



Home Page

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



Access Point Mode

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

A wireless LAN that uses the ASUS 802.11g AP in “Access Point” mode 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 it has learned are located either on the Ethernet network or on the radio network by monitoring 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 listed in its table. If the packet’s destination address is not in the table, 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 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.

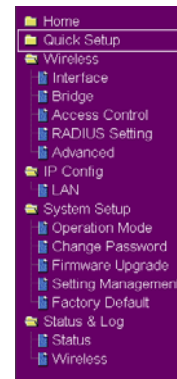
The ASUS 802.11g AP forwards all broadcast packets to wireless mobile clients. Given this, the ASUS 802.11g AP can only support a limited amount of network traffic. It is recommended that you only use the ASUS 802.11g AP on networks that contain less than 512 nodes.

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 with the network. Therefore, 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.

Quick Setup

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

Configure Wireless Interface



Access Point

- **Quick Setup** allows users to complete basic setting by just answering several questions.
- **802.11g and WPA** supports up to 54Mbps transmission rate, backward compatibility with 802.11b and interoperable security enhancement.
- **Status & Log** log status of system in details.

This site is best viewed with IE 5.0 or above.

Click NEXT to start Quick Setup **NEXT**

Quick Setup

Configure Wireless Interface

First step to set your wireless interface is to give it a name, called SSID. In addition, if you would like to protect transmitted data, please select the Security Level and assign a password for authentication and data transmission if it is required.

SSID:	default
Security Level:	Low
Phassphrase:	Low
WEP Key 1 (10 or 26 hex digits):	Middle
WEP Key 2 (10 or 26 hex digits):	High
WEP Key 3 (10 or 26 hex digits):	
WEP Key 4 (10 or 26 hex digits):	
Default Key:	

First step to set your wireless interface is to give it a name, called SSID. In addition, if you would like to protect transmitted data, please select Security Level as middle or high. Selecting Middle allows only those users use the same WEP key connect to this access point and to transmit data with 128 bits WEP encryption. Selecting High allows only those users use the same WPA pre-shared key to connect to this access point and to transmit data with TKIP encryption.

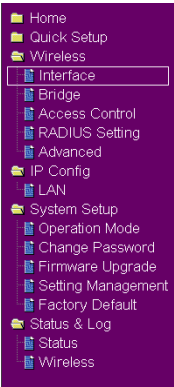
(See next few pages for item descriptions.)

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



Wireless

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



Interface

Wireless - Interface	
SSID:	default
Channel:	Auto
Data Rate(Mbps):	Auto
54g Mode:	Auto <input checked="" type="checkbox"/> 54g Protection
Basic Rate Set:	1, 2, 5.5 & 11 Mbps
Authentication Method:	Open System or Shared Key
Encryption:	None
Passphrase:	
WEP Key 1 (10 or 26 hex digits):	
WEP Key 2 (10 or 26 hex digits):	
WEP Key 3 (10 or 26 hex digits):	
WEP Key 4 (10 or 26 hex digits):	
Default Key:	Key1
WPA Re-key Timer:	0
Block broadcast SSID:	<input type="radio"/> Yes <input checked="" type="radio"/> No
<div>Restore Finish Apply</div>	

SSID

The SSID is an identification string of up to 32 ASCII characters that differentiate one ASUS 802.11g AP or Access Point from other manufacturers. 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 or Access Point is deployed in the same area. In that case, you should use a different SSID and radio channel for each ASUS 802.11g AP or Access Point. All ASUS 802.11g APs and ASUS 802.11g WLAN client adapters must have the same SSID to allow a wireless mobile client to roam between the ASUS 802.11g APs . By default, the SSID is set to “default”.

Chapter 3 - Software Configuration

Channel

IEEE 802.11g and 802.11b devices are direct sequence spread spectrum devices that spread a radio signal over a range of frequencies. The range of frequencies used by a direct sequence device is called a Channel. The 802.11g and 802.11b specification supports up to 14 overlapping Channels for radio communication. To minimize interference, configure each ASUS 802.11g AP to use Non-overlapping. Selecting Auto, system will choose a clear channel during boot up as your operating channel.

Data Rate (Mbps)

This field allows you to specify the transmission rate. Leave on “Auto” to maximize performance versus distance.

54g Mode

This field indicates the 802.11g interface mode. Selecting “Auto” allows 802.11g and 802.11b clients to connect to the ASUS 802.11g AP. Selecting “54g Only” maximizes performance, but prevents 802.11b clients from connecting to the ASUS 802.11g AP. If “54g Protection” is checked, G-Mode protection of 11g traffic is enabled automatically in the presence of 11b traffic.

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.

Authentication Method

This field enables you to set different authentication methods which determine different encryption schemes. The relationship between Authentication Method, Encryption, Pass-phrase and WEP Keys is listed in the following table. If you are not using a RADIUS server in a home environment and all your clients support WPA, using “WPA-PSK” is recommended for better security. Selecting “WPA” or “Radius with 802.1x”, additional settings for the RADIUS server in the “Wireless – Radius” field is required.

Chapter 3 - Software Configuration

Relationship among keys

Authentication Method	Encryption	Passphrase	WEP Key 1~4
Open or Shared Key	None	Not required	Not required
	WEP-64 bits	1~64 characters	10 hex
	WEP-128 bits	1~64 characters	26 hex
Shared Key	WEP-64 bits	1~64 characters	10 hex
	WEP-128 bits	1~64 characters	26 hex
WPA-PSK	TKIP only	8~63 characters	Not required
	AES only*	8~63 characters	Not required
WPA	TKIP only	Not required	Not required
	AES only*	Not required	Not required
Radius with 802.1x	Auto	Not required	Not required
	WEP-64 bits	1~64 characters	10 hex
	WEP-128 bits	1~64 characters	26 hex

Chapter 3 - Software Configuration

Encryption

Using “Open or Shared Key”, “Shared Key” or “Radius with 802.1x” authentication method, traditional WEP encryption is applied. Using “WPA-PSK” or “WPA”, a newly proposed TKIP or AES encryption in WPA is applied.

Enabling WEP can protect your data from eavesdroppers. If you do not need this feature, select “no” to skip the following setting. The ASUS 802.11g AP supports both 64-bit and 128-bit encryption using the Wired Equivalent Privacy (WEP) algorithm. Select the type of encryption you want to use (64 or 128 bit) and configure one to four WEP Keys. The “128-bit” method is more secure than the “64-bit”.

64/128bits versus 40/104bits

You may be confused about configuring WEP encryption, especially when using multiple wireless LAN products from different vendors. There are two levels of WEP Encryption: 64 bits and 128 bits. Firstly, 64 bit WEP and 40 bit WEP are the same encryption method and can interoperate in the wireless network. This lower level of WEP encryption uses a 40 bit (10 Hex character) as a “secret key” (set by user), and a 24 bit “Initialization Vector” (not under user control). This together makes 64 bits (40 + 24). Some vendors refer to this level of WEP as 40 bits and others refer to this as 64 bits. ASUS WLAN products use the term 64 bits when referring to this *lower* level of encryption. Secondly, 104 bit WEP and 128 bit WEP are the same encryption method and can interoperate in the wireless network. This higher level of WEP encryption uses a 104 bit (26 Hex character) as a “secret key” (set by user), and a 24 bit “Initialization Vector” (not under user control). This together makes 128 bits (104 + 24). Some vendors refer to this level of WEP as 104 bits and others refer to this as 128 bits. ASUS WLAN products use the term 128 bits when referring to this *higher* level of encryption.

Phrase

Selecting “TKIP only” or “AES only” in Encryption, this field will be used as a password to kick off the encryption process. A 8~63 characters password is required. Selecting “WEP-64bits” or “WEP-128bits” in Encryption, this field will be used to generate four WEP keys automatically. A WEP key is either 10 or 26 hexadecimal digits (0~9, a~f, and A~F) based on whether you select 64 bit or 128 bit in the WEP pull-down menu. Type a combination of up to 64 letters, numbers, or symbols in the Magic Word

Chapter 3 - Software Configuration

column, then the ASUS 802.11g AP Manager uses an algorithm to generate four WEP keys for encryption. If you want to type in the keys manually, leave this field blank. The ASUS WLAN family of products all uses the same algorithm to generate the keys so that they can all use the same WEP key.



Note: This function eases users from having to remember their passwords and is compatible to ASUS WLAN family of products. But this is not as secure as manual assignment.

WEP Key

At most four keys can be set. A WEP key is either 10 or 26 hexadecimal digits (0~9, a~f, and A~F) based on whether you select 64 bit or 128 bit 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.

Default Key

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.

WPA Re-key Timer

This field specifies the time interval that WPA group key is changed in seconds. 0 means no periodic key-change is required.

Block Broadcast SSID

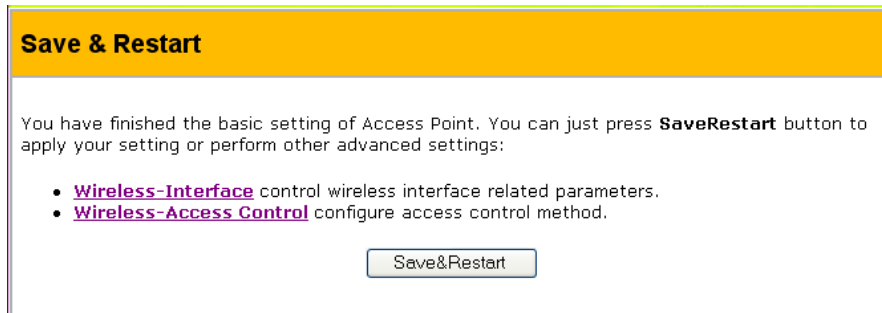
By default, “No” is selected so that wireless mobile users can see your ASUS 802.11g AP’s SSID and join. If “Yes” is selected, your ASUS 802.11g AP will not show in site surveys by wireless mobile clients and they will have to manually enter your ASUS 802.11g AP’s SSID. If you want to restrict access to “your” ASUS 802.11g AP, this is a simple way to do it but for security reasons, don’t forget to change the SSID to something other than “default”.

Chapter 3 - Software Configuration

Save & Restart

When you have finished the basic setting of ASUS 802.11g AP. You can click **Save & Restart** button to apply your setting or perform other advanced settings:

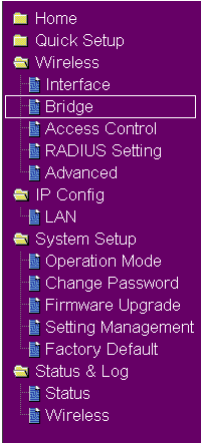
- Wireless - Interface control wireless interface related parameters.
- Wireless - Access Control configure access control method.



Chapter 3 - Software Configuration

Wireless

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



Bridge

AP Mode:	Hybrid
Channel:	AP Only WDS Only Hybrid

AP Only

Wireless - Bridge

Wireless bridge (also known as Wireless Distribution System or WDS) function allows you to connect to one or many APs through wireless.

AP Mode: AP Only

Channel: 6

Connect to APs in Remote Bridge List? ☐ Yes ☒ No

Allow anonymous? ☐ Yes ☒ No

Remote Bridge List

MAC Address

WDS Only

Wireless - Bridge

Wireless bridge (also known as Wireless Distribution System or WDS) function allows you to connect to one or many APs through wireless.

AP Mode: WDS Only

Channel: 6

Connect to APs in Remote Bridge List? ☐ Yes ☒ No

Allow anonymous? ☐ Yes ☒ No

Remote Bridge List

MAC Address

Hybrid

Wireless - Bridge

Wireless bridge (also known as Wireless Distribution System or WDS) function allows you to connect to one or many APs through wireless.

AP Mode: Hybrid

Channel: 6

Connect to APs in Remote Bridge List? ☒ Yes ☐ No

Allow anonymous? ☐ Yes ☒ No

Remote Bridge List

MAC Address

Restore Finish Apply

Chapter 3 - Software Configuration

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.



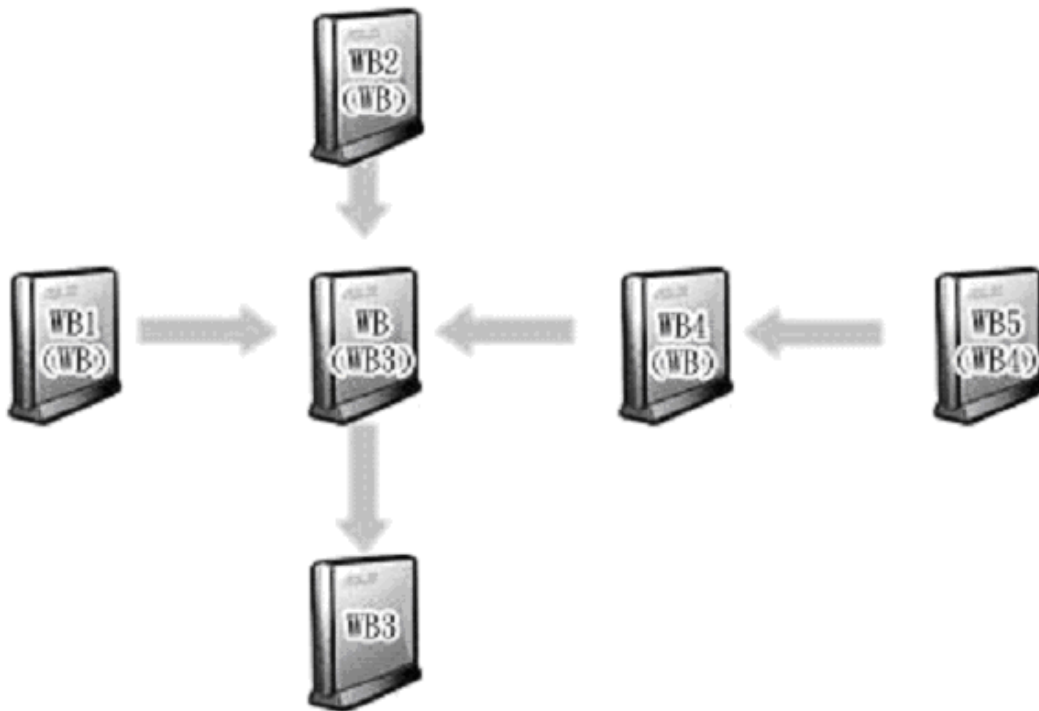
Note: If “Connect to APs in Remote Bridge List” and “Allow Anonymous” are both set to “No”, it means that this AP will not connect with other APs and therefore the AP mode setting will return to “AP Only”.

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:

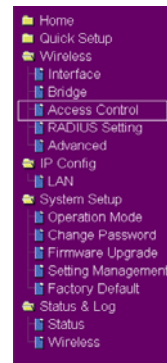


Note: The content in braces “()” is the MAC address in the Remote Bridge List of the AP. For example, WB1 have the MAC address of WB in its Remote Bridge List.

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.

Wireless

Click this item on the menu to reveal a sub menu. Follow the instructions to setup the ASUS wireless router. Tips are given when you move your cursor over each item.



Access Control

Pull down menu items:

Disable (no info required)

Accept (need to input information)

Reject (need to input information)

To add security, the ASUS 802.11g AP has the ability to only associate with or not associate with wireless mobile clients that have their MAC address entered into this page.

The default setting of “Disable” will allow any wireless mobile client to connect. “Accept” will only allow those entered into this page to connect. “Reject” will prevent those entered into this page from connecting.

Adding a MAC Address

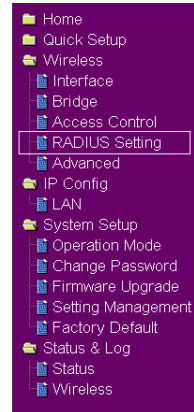
To add a MAC address, enter the 12 hexadecimal characters into the white box next to “MAC Address:” and click the **Add** button. The MAC address will be placed in the control list below. Only a total of 31 MAC addresses can be entered into this page so determine which will be the lesser; those you wish to accept or those you wish to reject and click the appropriate “MAC Access Mode”.



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

Wireless

Click this item on the menu to reveal a sub menu. Follow the instructions to setup the ASUS wireless router. Tips are given when you move your cursor over each item.



RADIUS Setting

Wireless - RADIUS Setting

This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - Interface" as "WPA" or "Radius with 802.1x".

Server IP Address:

Server Port:

Connection Secret:

This section allows you to set up additional parameters for connection with RADIUS Server. It is required while you select "Authentication Method" as "WPA" or "Radius with 802.1x" in "Wireless – Interface".

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.

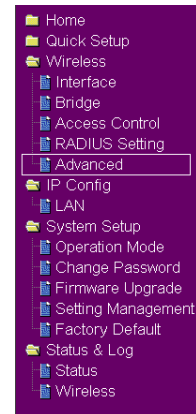
Connection Secret - This field specifies the password used to initialize a RADIUS connection.



Note: Click the "Finish" button to save your new settings and re-start the ASUS 802.11g AP or click "Save" and restart later.

Wireless

Click this item on the menu to reveal a sub menu. Follow the instructions to setup the ASUS wireless router. Tips are given when you move your cursor over each item.



Advanced

Wireless - Advanced	
This section allows you to set up additional parameters for wireless. But default values are recommended.	
Fragmentation Threshold:	2346
RTS Threshold:	2347
DTIM Interval:	3
Beacon Interval:	100
Enable Frame Bursting?	<input checked="" type="radio"/> Yes <input type="radio"/> No
<div>Restore Finish Apply</div>	

This section allows you to set up additional parameters for wireless. But default values are recommended.

Fragmentation Threshold (256~2346) - Fragmentation is used to divide 802.11 frames into smaller pieces (fragments) that are sent separately to the destination. The use of fragmentation can increase the reliability of frame transmissions. This field allows you to enable fragmentation by setting a specific packet size threshold. Default value 2346 is recommended.

RTS Threshold (0~2347) – RTS/CTS(Request to Send/Clear to Send) function is used to minimize collisions among wireless stations. If you enable RTS/CTS, it will refrain from sending a data frame until another RTS/CTS handshake in the air is completed. This field allows you to enable RTS/CTS by setting a specific packet size threshold. Default value 2347 is recommended.

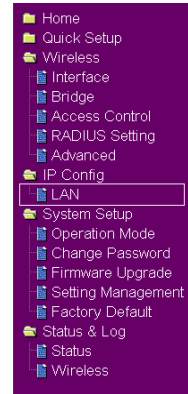
DTIM Interval (1~255) - DTIM(Delivery Traffic Indication Message) is a kind of wireless message used to inform clients in Power Saving Mode when should wake up to receive the broadcast and multicast messages. This field indicates the time interval in the unit of Beacon Interval that system broadcast DTIM for clients in Power Saving Mode. Default value 3 is recommended.

Beacon Interval (1~65535) - This field indicates the time interval in milliseconds that system broadcast packet, called beacon, to synchronize the wireless network. 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.

IP Config

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



LAN

Selection items:

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.

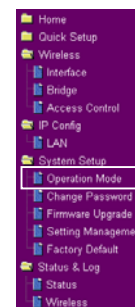
If you have a DHCP (Dynamic Host Configuration Protocol) server on the network, then the DHCP server will automatically assign the ASUS 802.11g AP an IP address when the ASUS 802.11g AP is powered up. To determine what IP address has been assigned to the ASUS 802.11g AP, review the IP address on the “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 don’t know your Gateway setting, leave it empty (not 0.0.0.0).

System Setup

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



Operation Mode

System Setup - Operation Mode	
WL300g support two operation modes to meet different requirements from different group of people. Please select the mode that match your situation.	
<input checked="" type="radio"/> Access Point	<p>In Access Point mode, ethernet port and wireless devices are set to locate in the same local area network. Those WAN related functions are not supported here.</p> <p>Explaining with technical terms, access point mode is, NAT is disabled, lan port and wireless port of WL300g are bridged together.</p>
<input type="radio"/> Home Gateway	<p>In this mode, we suppose you use the only ethernet port of WL300g to connect to Internet through ADSL or Cable Modem. And, there are many people in your environment share the same IP to ISP.</p> <p>Explaining with technical terms, gateway mode is , NAT is enabled, WAN connection is allowed by using PPPoE, or DHCP client, or static IP. In addition, some features which are useful for home user, such as UPnP and DDNS, are supported.</p>
<div>Apply</div>	

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

Home Gateway

In this mode, we suppose you use the Ethernet port to connect to Internet through ADSL or Cable Modem. And, there are many people in your environment share the same IP to ISP.

Technically, gateway mode is , NAT is enabled, WAN connection is allowed by using PPPoE, or DHCP client, or static IP. In addition, some features which are useful for home user, such as UPnP and DDNS, are supported.

Access Point

In Access Point mode, Ethernet port and wireless devices are set to locate in the same local area network. Those WAN related functions are not supported here.

Technically, access point mode is, NAT is disabled, one wan port and four LAN ports are bridged together.

By default, the ASUS 802.11g AP operates in Access Point mode.

Chapter 3 - Software Configuration

Home Gateway

After selecting “Gateway” mode and clicking “Apply”, you will enter the “Quick Setup” page of the Gateway mode. Follow the instructions to setup the ASUS 802.11g AP as a Gateway.

Quick Setup

Select Time Zone

Please choose the time zone where you are locating in.

Time Zone: (GMT-11:00) Midway Island, Samoa
(GMT-11:00) Midway Island, Samoa
(GMT-10:00) Hawaii
(GMT-09:00) Alaska
(GMT-08:00) Pacific Time
(GMT-07:00) Mountain Time
(GMT-07:00) Arizona
(GMT-06:00) Central Time
(GMT-05:00) Middle America
(GMT-05:00) Indiana East, Colombia
(GMT-05:00) Eastern Time
(GMT-04:00) Atlantic Time, Brazil West
(GMT-04:00) Bolivia, Venezuela
(GMT-03:00) Guyana
(GMT-03:00) Brazil East, Greenland
(GMT-02:00) Mid-Atlantic

Select Internet Connection Type

WL300g supports two kinds of connection to Internet through its WAN port. Please select connection type you need. In addition, before getting on Internet, please make sure you have connected WL300g's WAN port to your DSL or Cable Modem.

Connection Type: Cable
ADSL
Cable

Prev Next

Set Your Account to ISP

If you apply an ADSL account with dynamic IP. You must get user account and password from your ISP. Please fill this data into the following fields carefully. Or, if you apply an ADSL account with static IP, just ignore user name and password information.

Connect with static IP? ☐ Yes ☒ No

User Name:

Password:

☒ Yes ☐ No

WAN IP Setting

Fill TCP/IP setting for WL300g to connect to Internet through WAN port.

Get IP automatically? ☐ Yes ☒ No

IP Address:

Subnet Mask:

Default Gateway:

Get DNS Server automatically? ☐ Yes ☒ No

DNS Server 1:

DNS Server 2:

☒ Yes ☐ No

☒ Yes ☐ No

Internet Access Policy

Select your Internet access policy to block some special services at specified time. It can avoid your children to access Internet at some specified time.

Blocked Services: ☐ WWW ☐ ICQ ☐ Stream
☐ Telnet ☐ Ftp ☐ Others

Date to Block Services: ☒ Sun ☒ Mon ☒ Tue ☒ Wed
☒ Thu ☒ Fri ☒ Sat

Time of Day to Block Services: 00:00:23:59

System Setup - Operation Mode

WL300g support two operation modes to meet different requirements from different group of people. Please select the mode that match your situation.

☐ Access Point

In Access Point mode, ethernet port and wireless devices are set to locate in the same local area network. Those WAN related functions are not supported here.

Explaining with technical terms, access point mode is, NAT is disabled, lan port and wireless port of WL300g are bridged together.

☒ Home Gateway

In this mode, we suppose you use the only ethernet port of WL300g to connect to Internet through ADSL or Cable Modem. And, there are many people in your environment share the same IP to ISP.

Explaining with technical terms, gateway mode is, NAT is enabled, WAN connection is allowed by using PPPoE, or DHCP client, or static IP. In addition, some features which are useful for home user, such as UPnP and DDNS, are supported.

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

“ADSL” uses a standard phone cable.
“Cable” uses a heavy round TV cable.
Click **Next** to continue.

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

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

You can block access to web sites, ICQ, streaming data, telnet, FTP, or others on specified days and time in order to restrict use, such as when children are concerned. Click **Next** to continue.

Chapter 3 - Software Configuration

Quick Setup

Configure Wireless Interface

First step to set your wireless interface is to give it a name, called SSID. In addition, if you would like to protect transmitted data, please select the Security Level and assign a password for authentication and data transmission if it is required.

SSID:	default
Security Level:	Low
Phassphrase:	Low Middle High
WEP Key 1 (10 or 26 hex digits):	
WEP Key 2 (10 or 26 hex digits):	
WEP Key 3 (10 or 26 hex digits):	
WEP Key 4 (10 or 26 hex digits):	
Default Key:	

Finish

Enter the SSID and make WEP settings if you want to add security to your wireless network. Click **Finish** to continue.

Save&Restart

You have finished the basic setting of Home Gateway. You can just press **SaveRestart** button to apply your setting or perform other advanced settings:

- **Wireless Interface** control wireless interface related parameters.
- **Wireless Access Control** configure access control method.
- **NAT Setting** configure special applications to pass through NAT or export your server to Internet.
- **Internet Firewall** configure your filter rules between LAN and WAN.
- **Wireless Firewall** configure your filter rules among Wireless, LAN and WAN.

Save&Restart

Click **Save&Restart** to save the settings to the ASUS 802.11g AP and enable the new settings.

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



Chapter 3 - Software Configuration

Virtual Server and Dynamic-DNS (DDNS)

NAT Setting - Virtual Server

To make services, like WWW, FTP, provided by a server in your local network accessible for outside users, you should specify a local IP address to the server. Then, add the IP address and network protocol type, port number, and name of the service in the following list. Based on the list, the gateway will forward service request from outside users to the corresponding local server.

Enable Virtual Server? ☒ Yes ☐ No

Virtual Server List

Local IP	Port Range	Application
		User Defined
		User Defined
		FTP
		TELNET
		SMTP
		DNS
		FINGER
		HTTP
		POP3
		SNMP
		SNMP TRAP

IP Config - Miscellaneous

Enable UPnP? ☒ Yes ☐ No

Enable Web Access from WAN? ☐ Yes ☒ No

Enable Log for Access from WAN? ☐ Yes ☒ No

Remote Log Server:

Time Zone: (GMT-11:00) Midway Island, Samoa

NTP Server: 131.107.1.10

DDNS Setting

Dynamic-DNS (DDNS) allows you to export your server to Internet with an unique name, even though you have no static IP address. Currently, two DDNS clients are embedded in WL300g. You can click Free Trial below to start with a free trial account.

Enable the DDNS Client? ☐ Yes ☒ No

Server: WWW.DYNDNS.ORG [Free Trial](#)

User Name or E-mail Address: WWW.DYNDNS.ORG

Password or DDNS Key: WWW.TZO.COM

Host Name:

Enable wildcard? ☐ Yes ☒ No

Update Manually:

Virtual Server allows you to make services, like WWW, FTP, provided by a server in your local network accessible for outside users. DDNS allows users 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 user on the 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 behind each DDNS service provider to start with a free trial account.

Chapter 3 - Software Configuration

WAN to LAN Filter

Date to Enable WAN to LAN Filter: ☒ Sun ☒ Mon ☒ Tue ☒ Wed
☒ Thu ☒ Fri ☒ Sat

Time of Day to Enable WAN to LAN Filter: 00 : 00 : 23 : 59

Packets(WAN to LAN) not specified will be: **ACCEPT**

Filtered ICMP(WAN to LAN) packet types:

WAN to LAN Filter Table Add Del Help

Well Known Applications:	User Defined	Source IP	Port Range	Protocol
WWW				TCP
ICQ				
REAL PLAYER/QUICK TIME				
TELNET				
FTP				
MSN Messenger				
MIRC				
NETMEETING(1)				
NETMEETING(2)				
NETMEETING(3)				
NETMEETING(4)				

Restore Finish Apply

WAN to LAN Filter

Date to Enable WAN to LAN Filter: ☒ Sun ☒ Mon ☒ Tue ☒ Wed
☒ Thu ☒ Fri ☒ Sat

Time of Day to Enable WAN to LAN Filter: 00 : 00 : 23 : 59

Packets(WAN to LAN) not specified will be: **ACCEPT**

Filtered ICMP(WAN to LAN) packet types:

WAN to LAN Filter Table Add Del Help

Well Known Applications:	User Defined	Source IP	Port Range	Protocol
WWW				TCP
ICQ				
REAL PLAYER/QUICK TIME				
TELNET				
FTP				
MSN Messenger				
MIRC				
NETMEETING(1)				
NETMEETING(2)				
NETMEETING(3)				
NETMEETING(4)				

Restore Finish Apply

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 hope to configure ASUS 802.11g AP through Ethernet port, please remember to enable Web Access from WAN in IP Config - Miscellaneous.

IP Config - Miscellaneous

Enable Web Access from WAN? ☒ Yes ☐ No

Remote Log Server:

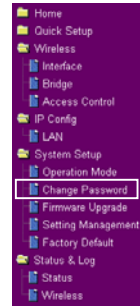
Time Zone: (GMT-11:00) Midway Island, Samoa

NTP Server: 131.107.1.10

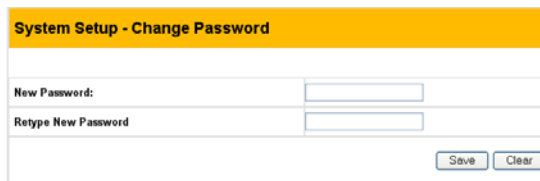
Restore Finish Apply

System Setup

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



Change Password



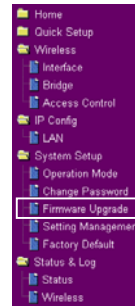
This page will allow you to change the default password “admin” (lower case) to any password of your choice. You can enter any usable characters between 1-16 characters long (cannot be left blank). Click **Save** button to save your new password. If you forget the ASUS 802.11g AP’s password, you can reset the ASUS 802.11g AP to its factory settings (see troubleshooting).



Note: The password is case sensitive.

System Setup

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



Firmware Upgrade

3. Software Web (Common)

System Setup - Firmware Upgrade

Follow instructions listed below:

1. Check if any new version of firmware is available on ASUS website.

2. Download a proper version to your local machine.

3. Specify the path of and name of the downloaded file in the "New Firmware File".

4. Click "Upload" to upload the file to WL300g. It spends about 10 seconds.

5. After receiving a correct firmware file, WL300g will automatically start the upgrade process. It takes a few time to finish the process and then the system will reboot.

Product ID:

WL300g

Firmware Version:

Bootloader Version:

Hardware Version:

New Firmware File:

Browse...

Upload

Note:

1. For a configuration parameter existing both in the old and new firmware, its setting will be kept during the upgrade process.

2. In case the upgrade process fails, WL300g will enter an emergent mode automatically. The LED signals at the front of WL300g will indicate such situation. Use the Firmware Restoration utility on the CD to do system recovery

Firmware Upgrading !

System is upgrading! Please wait until home page of WL300g setting is shown up again.

Note: It takes about 80 seconds.

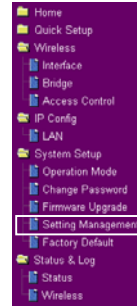
This page reports the Flash Code (Firmware) version installed in the ASUS 802.11g AP. Periodically, a new Flash Code is available for the ASUS 802.11g APs on ASUS's Web site. You can update the ASUS 802.11g AP's Flash Code using the Firmware Upgrade page under the Advanced Setup menu of the Web Manager. If you are experiencing a problem with your ASUS WLAN equipment, a Technical Support representative may ask you to give your device's Flash Code (Firmware) version.



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

System Setup

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



Setting Management

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

Save As a File

Move your cursor over the **HERE** link on the web page. Then click the right button of mouse and select **Save As...** to save current setting into a file.



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

Load From a File

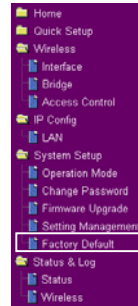
Specify the path of and name of the downloaded file in the **New Setting File** below. Then, click **Upload** to write the file to. It takes a few time to finish the process and then the system will reboot.

New Setting File

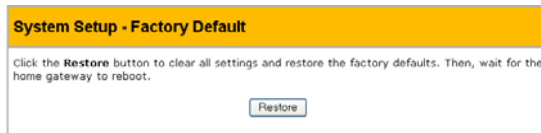
Click **Browse** to locate the file.

System Setup

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



Factory Default



Restoring Factory Default Settings

Web Manager

You can reset all settings to their factory defaults through the web manager using the “Factory Default” page in “Advanced Setup”. Click the **Restore** button and wait about 30 seconds before trying to access the ASUS 802.11g AP.

Hardware

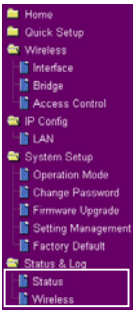
You can reset all settings to their factory defaults manually by pushing the “Restore” button in a hole on the back of the ASUS 802.11g AP while it is ON. Use a pen or straightened paper clip to hold the “Restore” button depressed over 5 seconds until the power LED on the front of the ASUS 802.11g AP starts blinking.



Note: You will be notified when factory default settings are restored while using the web manager.

Status & Log

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



Status

Status

Sytem Up Time:

1 Day : 1 Hour : 17 Min : 8 Sec

LAN Interface

IP Address:

192.168.1.1

Subnet Mask:

255.255.255.0

Default Gateway:

Refresh

Wireless

Wireless - 11g Interface

SSID : default

Channel : 6

WEP : None

STA1 00:e0:18:f4:44:8a

Refresh

System Up Time

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

LAN Interface

IP Address

Shows the IP address of the ASUS 802.11g AP. When getting IP automatically, it is necessary to see the IP address from this screen.

Default Gateway

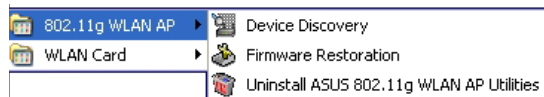
Shows the default gateway IP address if entered. This can be blank.

Firmware Restoration

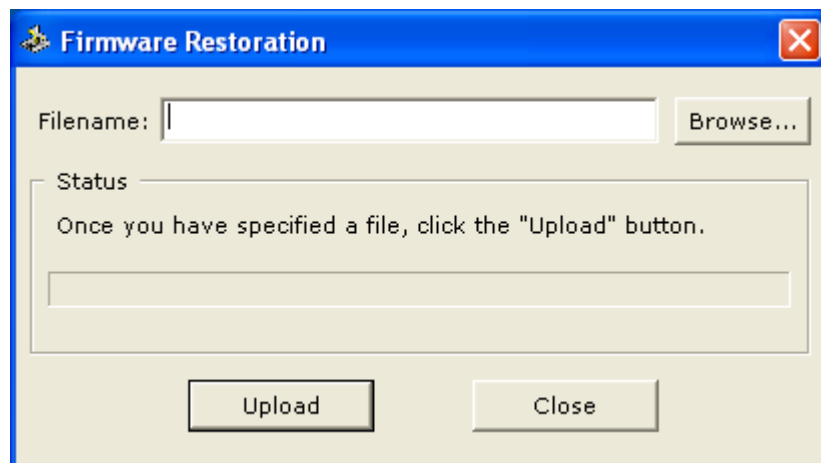
The Firmware Restoration utility is an emergency rescue tool that can automatically search out an ASUS 802.11g AP that has failed during a firmware upload and re-upload a firmware that you specify. A failed firmware upgrade will cause the ASUS 802.11g AP to enter a failure mode, waiting for the Firmware Restoration utility to find and upload a new firmware. The process takes about 3 to 4 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 manager.



The Firmware Restoration utility is launched from the Windows Start menu.



Using a Hub

If you have problems uploading a firmware while using a network hub, try connecting your computer directly to the LAN port. Either 10Base-T or 100Base-TX connections can be used.

4. Troubleshooting

The ASUS AP is designed to be very easy to install and operate. However, if you experience difficulties, use the information in this chapter to help diagnose and solve problems. If you cannot resolve a problem, contact Technical Support, as listed on the front of this manual.

Common Problems and Solutions

Problem

The ASUS AP does not power up:

Solution

- Check for faulty ASUS AP power supply by measuring the output voltage with an electrical test meter.
- Check failed AC supply (power outlet)

Problem

Cannot communicate with the ASUS AP through a wired network connection.

Solution

- Verify network configuration by ensuring that there are no duplicate IP addresses. Power down the device in question and ping the assigned IP address of the device. Ensure no other device responds to that address.
- Check that the cables used have proper pin outs and connectors or use another LAN cable.
- Check that the hub, switch, or computer that the ASUS AP is connected and that all devices support 10Mbps speed.

This is what you will see if you connect the ASUS 802.11g AP to a:

	10/100 Mbps Hub	Pure 100 Mbps Hub
Hub LED	ON	OFF
Access Point (Link) LED	ON	ON

So you will not know if the connection is bad from the ASUS AP Link LED alone, you will have to look at the Hub LED if you are not sure what kind of hub the ASUS AP is attached to.

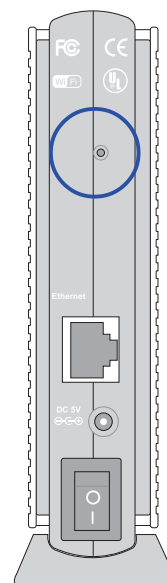
Chapter 4 -Troubleshooting

Problem

The ASUS AP Device Discovery still cannot find or connect to the ASUS AP after verifying the IP address and LAN cable, changes cannot be made, or password is lost.

Solution

In case the ASUS AP is inaccessible, you can restore the ASUS AP's factory default settings. Use a straightened paper clip to press the button located in the hole on the back of the ASUS AP and keep it depressed over 5 seconds. The power LED will darken and then light up when reset is successful.



Reset to Defaults

The following are factory default values. These values will be present when you first receive your the ASUS AP , if you push the reset button on the back of the ASUS AP over 5 seconds, or if you restore factory settings through the ASUS AP software.

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

Problem

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

Solution

Follow these steps:

1. Make sure that your WLAN Card is of the same specifications as the WLAN Access Point.
2. Try to bring the devices closer together; the ASUS WLAN Card may be out of range of the ASUS AP.
3. Confirm that the ASUS AP and ASUS WLAN Card have the same SSID.
4. Confirm that the ASUS AP and ASUS WLAN Card have the same Encryption settings, if enabled.
5. Confirm that the ASUS AP's Air and Link LEDs are solid green.
6. Confirm that the authorization table includes the MAC address of the ASUS WLAN Card if "Authorization Table" is enabled.
7. Confirm that the operational mode is "Access Point" mode.
8. Confirm that the ASUS AP and ASUS WLAN Card have the same preamble mode.

Problem

The throughput seems slow.

Solution

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 cabling.
- Verify network traffic does not exceed 37% of bandwidth.
- Check to see that the wired network does not exceed 10 broadcast messages per second.
- Verify wired network topology and configuration.

Chapter 4 -Troubleshooting

Problem

I cannot find the ASUS APs using the ASUS AP Discovery.

Solution

To configure the ASUS AP through an ASUS WLAN Card, your computer must be in the same subnet of the ASUS AP. You cannot find the ASUS APs with subnet different from your computer within the same gateway. You must change your computer to the same subnet as the ASUS AP. The factory default subnet of the ASUS AP is "192.168.1.1".

Problem

How do I upgrade the firmware on the ASUS AP?

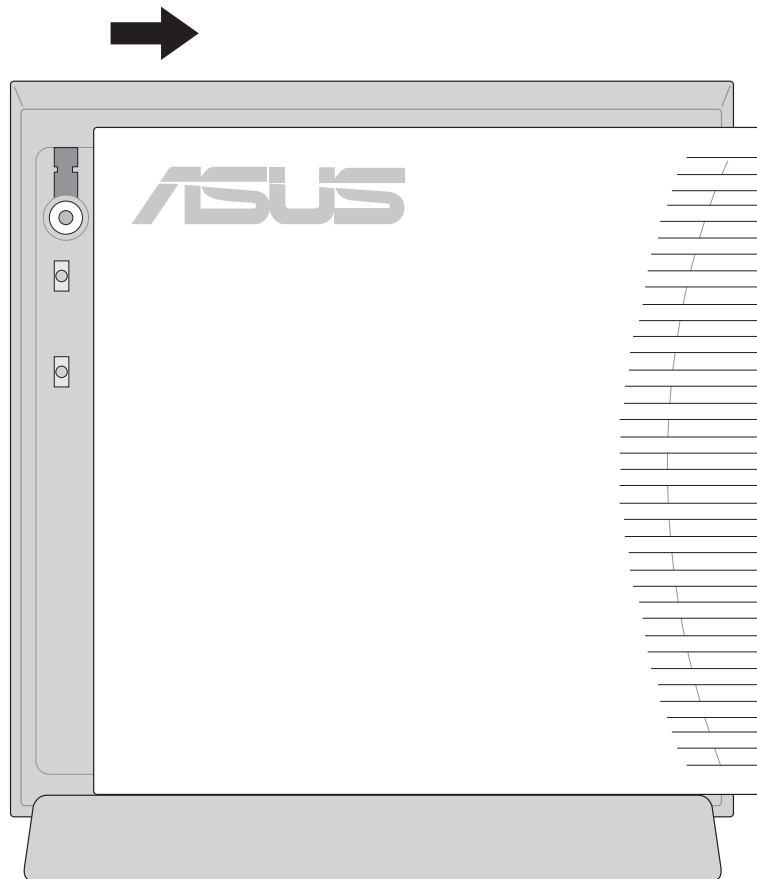
Solution

Periodically, a new Flash Code is available for the ASUS APs on the ftp site at **ftp://ftp.asus.com**. You can update the ASUS AP's Flash Code using the software described in this User's Manual.

5. Appendix

External Antenna Connector

Slide the right side cover back to reveal the antenna connector.



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.

DSSS PHY frequency channel plan

		(Regulatory Domains)					
CH ID	Frequency	X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32' France	X'40' MKK
1	2412 MHz	Yes	Yes	Yes	-	-	Yes
2	2417 MHz	Yes	Yes	Yes	-	-	Yes
3	2422 MHz	Yes	Yes	Yes	-	-	Yes
4	2427 MHz	Yes	Yes	Yes	-	-	Yes
5	2432 MHz	Yes	Yes	Yes	-	-	Yes
6	2437 MHz	Yes	Yes	Yes	-	-	Yes-
7	2442 MHz	Yes	Yes	Yes	-	-	Yes
8	2447 MHz	Yes	Yes	Yes	-	-	Yes
9	2452 MHz	Yes	Yes	Yes	-	-	Yes
10	2457 MHz	Yes	Yes	Yes	Yes	Yes	Yes
11	2462 MHz	Yes	Yes	Yes	Yes	Yes	Yes
12	2467 MHz	-	-	Yes	-	Yes	Yes
13	2472 MHz	-	-	Yes	-	Yes	Yes
14	2484 MHz	-	-	-	-	-	Yes

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.

Chapter 5 - Appendix

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 (54Mbps/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 (11Mbps/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.

Chapter 5 - Appendix

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.

Chapter 5 - Appendix

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, and
- 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.

Chapter 6 - Safety Statements

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

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Appendix - GNU General Public License

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the 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 other 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 freedom, 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 change 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 restrictions 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 you 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 gives 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 someone 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 software 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 free use or not licensed at all.

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

Appendix - GNU General Public License

Terms & conditions for copying, distribution, & modification

0. This License applies to any program 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 either the 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 limitation 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 output 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 copies 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 to 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 exchange 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 of these 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 is 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.

Appendix - GNU General Public 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 provided 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,

Appendix - GNU General Public License

- 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 be distributed 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 allowed 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 modifications to 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 special 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 component 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 the 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 copy, 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 such parties remain in full compliance.

Appendix - GNU General Public License

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 prohibited 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 modifying 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 terms 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 judgment or 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 conditions 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 would 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.

If 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 section 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 license 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 software through any other system and a licensee cannot impose that choice.

Appendix - GNU General Public License

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 restricted 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 permitted 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 License 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 this 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 of 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 permission. 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 free software and of promoting the sharing and reuse of software generally.

Appendix - GNU General Public License

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 STATED IN 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. THE 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 WRITING 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 USE 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 OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

