

Wireless LAN 11g Access Point

User's Manual



Version 0.11

WARNING - Disclaimer

Do not use this device in applications for which any failure of the wireless link or any data error may cause death, injury or damage of any kind.

Tellus Group Corp., its Sales, Manufacturing and Design Organizations, Reps., Distributors, VARs and distribution channels are absolutely not liable for any death, injury, property damage, loss of data, and loss of business of any other unmentioned loss. The aforementioned entities are not liable even in the event that any of these entities were apprized of the specifics or generalities of an application or intended installation at any time.

Radio Linkages of any type can be fragile and tenuous. Over 1/5th of the entire population of the world now owns cellular telephones, and as any user of a cell phone knows, the cell phone radio communications link may be easily disrupted or completely lost simply by turning your head or by other small environmental movements or changes. This clearly demonstrates to everyone the fragility of any radio link and why radio should not be used for critical implementations, or where death, personal injury, physical damage, property damage or environmental damage may result.

Tellus Group Corp products are not designed, manufactured, or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as, but not limited to the operation of nuclear facilities, aircraft navigation, vital communication systems, air traffic control, life support machines, weapons systems, or any industry in which environmental disruptions or technology failure could lead directly to death, personal injury, physical damage, property damage or environmental damage.

Copyright © 2005 by manufacturer. All rights reserved.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from the copyright owner. All the other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

The content described in this manual may be improved or changed at any time and it is subject to be changed without notice.

Manufacturer assumes no responsibility for errors contained herein or for direct, indirect, special, incidental or consequential damages with the furnishing, performance, or use of this manual or equipment supplied with it, even if manufacturer or its suppliers have been advised of the possibility of such damages.

Regulatory information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antenna) made to this device that are not expressly approved by manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution or attachment of connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

Limited Warranty

This product is warranted by manufacturer to be free from defects in material and workmanship for one (1) year from the date of purchase unless otherwise stated.

During this period if this product is found to be defective in material or workmanship, manufacturer or one of its authorized service facilities will at its option either repair or replace this product without charge, subject to the following conditions, limitations and exclusions:

This warranty extends to the original consumer purchaser only and is not assignable or transferable.

This warranty shall not apply to any product which has been subjected to misuse, abuse, abnormal use, negligence, alteration or accident, or has had its serial number altered or removed.

This warranty does not apply to any defects or damage directly or indirectly caused by or resulting from the use of unauthorized replacement parts and/or service performed by unauthorized personnel.

This warranty does not apply to the software driver that accompanies this product.

This warranty is made expressly in lieu of all other warranties, expressed or implied, including but not limited to any implied warranty of merchantability of fitness for a particular purpose, and all other obligations on the part of Manufacturer provided, however, that if the disclaimer of implied warranties is ineffective under applicable law, the duration of any implied warranties arising by operation of law shall be limited to one (1) year from the date of purchase or such longer period as may be required by applicable law.

Manufacturer hereby disclaims any and all liabilities for consequential and incidental damages arising out of or in connection with any breach of this warranty or any other claim with respect to this product, including but not limited to claims of negligence, strict liability in tort or breach of contract.

Table of Content

1. Introduction	6
1.1 Features	6
1.2 Applications	8
1.3 Safety Notification	8
1.4 Operation Mode	9
1.4.1 AP (Access Point) Mode	9
1.4.2 AP Client:	10
1.4.3 Repeater Mode	11
1.4.4 Bridge Mode	12
2. Installation	13
2.1 Package Contents	13
2.2 The AP Front	13
2.3 The AP's Rear Panel	14
2.4 System Requirement	14
2.5 Default Settings.....	15
2.6 Connect the Power Adapter.....	15
2.7 Connect to a Network	15
2.8 Power over Ethernet (PoE) - Optional	16
2.8.1 PoE Splitter device.....	16
2.8.2 PSE Device	16
3. Configuration	17
3.1 Primary Setting	18
3.1.1 WEP	19
3.1.2 WPA-Preshared key	20
3.1.3 WPA RADIUS	20
3.2 System.....	22
3.3 Operation Mode	24
3.4 Status	26
3.5 Traffic Log	28
3.6 Access Control	30
3.7 Advanced Wireless.....	32
3.8 SNMP Info	34
3.9 Upgrade Firmware	36
4. Troubleshooting	37
Appendix A	39
Appendix B	40
Figure 1-1 AP mode configuration example	9

Figure 1-2 AP-client mode configuration example.....	10
Figure 1-3 Repeater mode configuration example.....	11
Figure 1-4 Bridge mode configuration example.....	12
Figure 2-1 Rear Panel	14
Figure 2-2 PoE Splitter Device	16
Figure 2-3 PSE Device.....	16
Figure 3-1 Primary Setup.....	18
Figure 3-2 System Setting.....	22
Figure 3-3 Operation Mode	24
Figure 3-4 Status	26
Figure 3-5 Traffic Log.....	28
Figure 3-6 View Traffic Log	29
Figure 3-7 Access Control	30
Figure 3-8 Advanced Wireless	32
Figure 3-9 SNMP Info	34

1. Introduction

Thank you for purchasing this 802.11g Access Point (hereafter this product will be referred as **The AP**). It supports IEEE802.11g/b, IEEE802.1x, IEEE 802.3/802.3u and IEEE 802.3af compliance devices. It is designed to meet the mobility, performance, security, interoperability, manageability, and reliability requirements in the ever demanding wireless networking application environments.

It is extremely easy and secure to set up its configuration via web browser. **The AP**'s SNMP feature provides IT managers the ability to conveniently monitor the remote network device quickly. In addition, its access control is achieved through the MAC address filtering and the WPA (WiFi Protected Access) security algorithm meets the stringent security protection needs.

The AP provides bridging mode function which allows two geographically separated LANs to be wirelessly interlinked in addition to serve as a WLAN base station (Access Point). Its repeater mode function will extend the range of the existing radio network and its AP-Client mode function let **The AP** be used as wireless NIC. Its external antenna design allows the use of third party antenna for extended range and performance.

The AP is designed for the ease of installation and future upgradeability with features such as Power over Ethernet (optional feature), automatic MDI –MDIX detection on the RJ45 LAN port and downloadable flash-upgradeable firmware which allows future ease of support.

Overall, **The AP** is a versatile and cost effective solution for your office, commercial or home WLAN applications need.

1.1 Features

- Compatible with WLAN 802.11g/b devices
- Supports IEEE 802.3af Power over Ethernet (optional feature)
- Turbo-G mode enhances throughput up to 40%
- Supports RADIUS (Remote Authentication Dial-In User Service) security function
- Enhances security through WPA (WiFi Protected Access) supports of TKIP (Temporary Key Integrity Protocol) or AES (Advanced Encryption Standard) algorithm
- WEP (Wired Equivalent Privacy) supports 64/128-bit encryption
- MAC address filtering enhancement
- Web browser user interface for easy configuration and management
- Supports VPN pass through
- Login security through password protection
- Supports SNMP management functions
- AP mode or AP-client mode selection
- WDS (Wireless Distribution Systems) enables WLAN bridging and repeater modes

- Supports full mobility and seamless roaming
- Supports traffic log functions
- Auto MDI-MDIX connection
- Downloadable firmware upgradeability
- Enhances reliable connectivity through automatic data rate fallback in noisy environment
- Reset button for fast default setting recovery
- Desktop and wall/ceiling mounting hardware included
- External antenna connector supports third party products for extended range and performance

1.2 Applications

- Networking for device sharing - Remote access to corporate network information, email, file transfer and terminal emulation.
- Frequently changing environments - Retailers, manufacturers and banks that frequently rearrange the workplace and change location.
- SOHO (Small Office and Home Office) users - SOHO users need easy and quick installation of a small computer network functions.
- Inter-building connection - The wireless building-to-building network installs quickly, requires no monthly lease fees, and provides the flexibility to reconfigure easily.
- Typical applications include hard-to-wire buildings, campuses, hospitals/medical offices, warehouse, security huts, exhibition centers, etc.
- Temporary LANs for special projects or occasions - Auditors require workgroups at customer sites. Trade shows, exhibitions, retailers, airline, and shipping companies need additional workstations for the peak periods of data traffic.

1.3 Safety Notification

Your Wireless AP should be placed in a safe and secure location. To ensure proper operation, please keep the unit away from water and other damaging elements. Please read the user manual thoroughly before you install the device. The device should only be repaired by authorized and qualified personnel.

- Please do not try to open or repair the device yourself.
- Do not place the device in a damp or humid location, i.e. a bathroom.
- The device should be placed in a sheltered and non-slip location within a temperature range of 0 to +40 Celsius degree.
- Please do not expose the device to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.

1.4 Operation Mode

The AP supports four operation modes:

- AP mode
- AP Client mode
- Repeater mode
- Bridge mode

1.4.1 AP (Access Point) Mode

The AP mode is a typical "Infrastructure mode". The WLAN station (e.g. Note Book with WLAN card) can access the LAN/Internet via the AP. The following figure (Figure 1-1) shows a typical configuration.

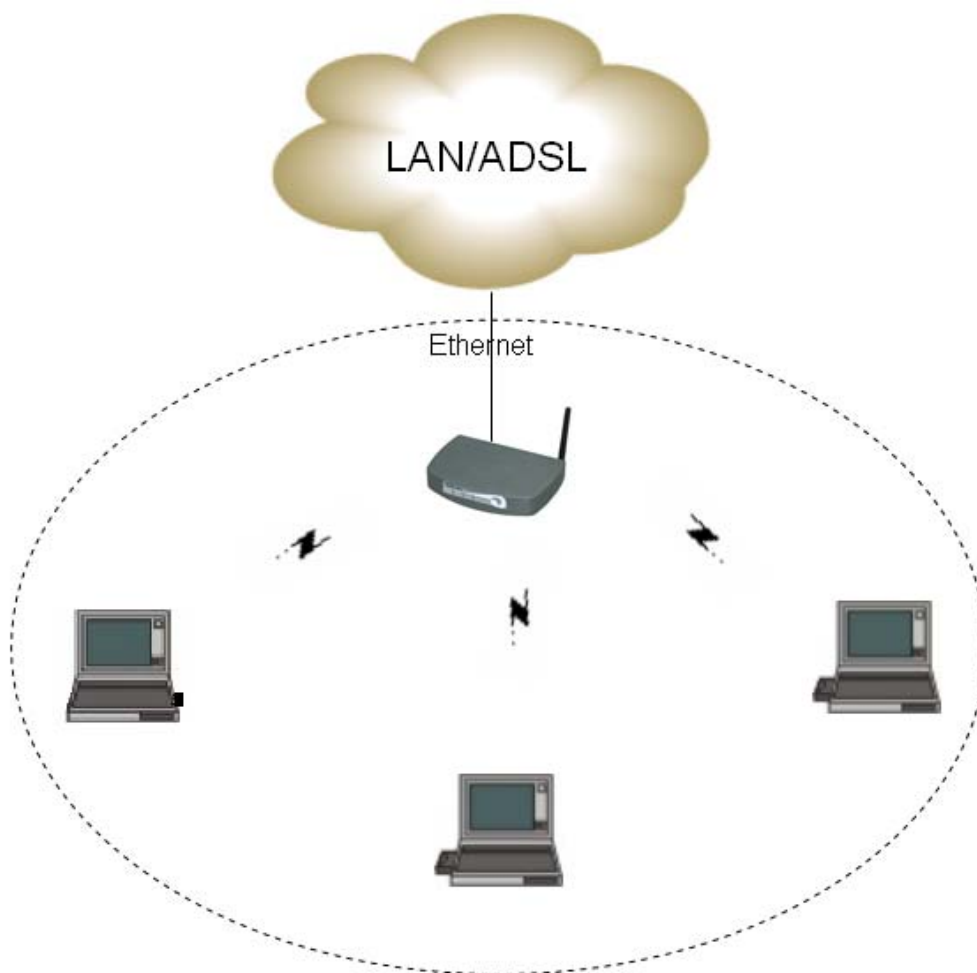


Figure 1-1 AP mode configuration example

1.4.2 AP Client:

The AP can be configured as an AP client to access other AP. In this operating mode, the device will be used as a wireless NIC. The following figure (Figure 1-2) shows the possible configuration:

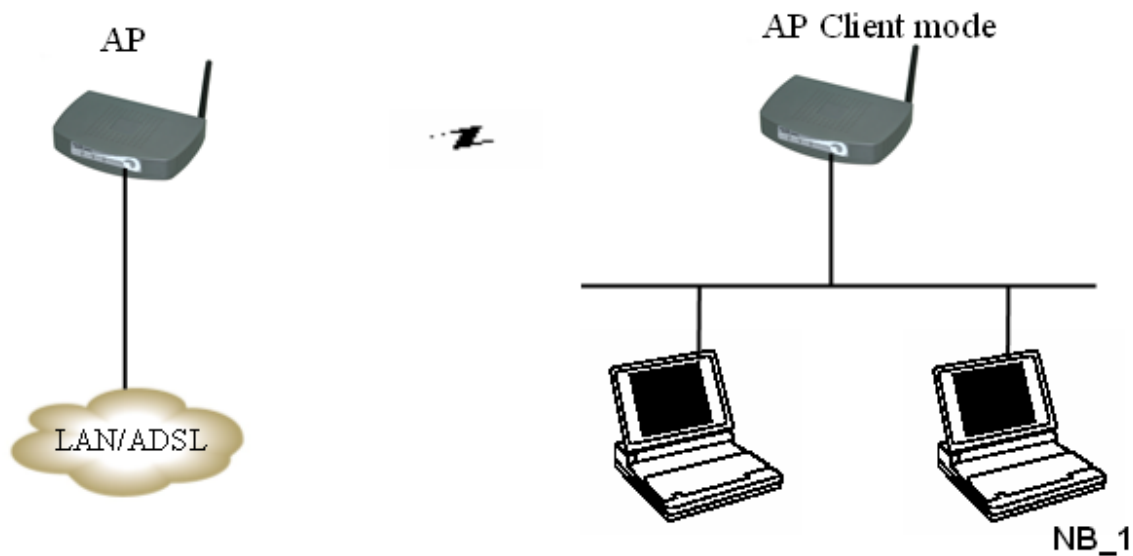


Figure 1-2 AP-client mode configuration example

The NB_1 can access the LAN/WAN at the left side via the AP Client which acts as wireless NIC station.

1.4.3 Repeater Mode

This mode allows the AP to keep the AP function role and at the same time establishing a connection with other 802.11g AP to extend your wireless network. The following figure (Figure 1-3) shows the possible configuration:

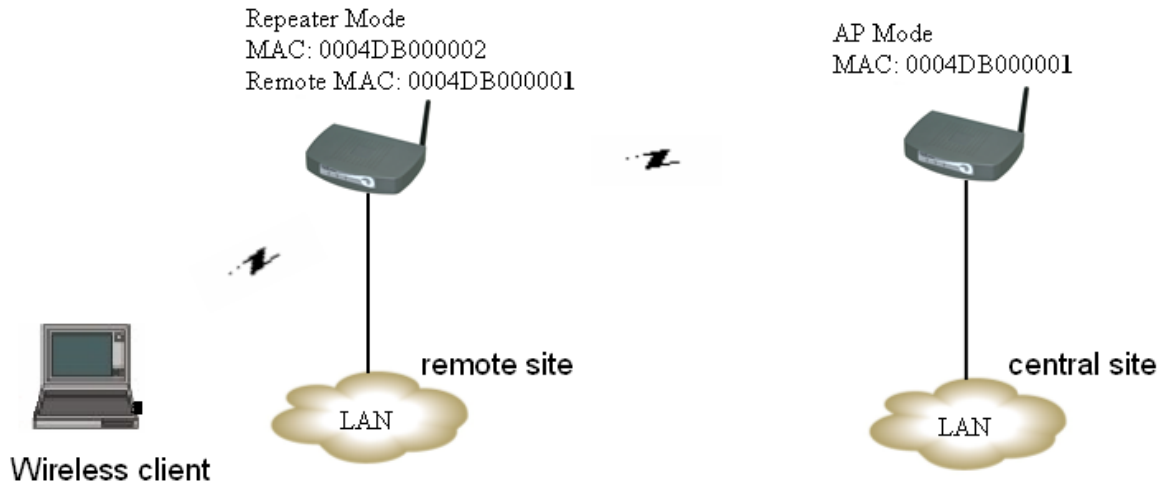


Figure 1-3 Repeater mode configuration example

1.4.4 Bridge Mode

As shown in the following configuration (Figure 1-4), the two AP are linked to each other via the wireless connection. Each AP can use its LAN port to connect to one LAN. So, the two wired Ethernet Network are linked together logically by a pair of wireless bridges. Once **The AP** has been set into the bridge mode, **The AP's** Access Point function is disabled.

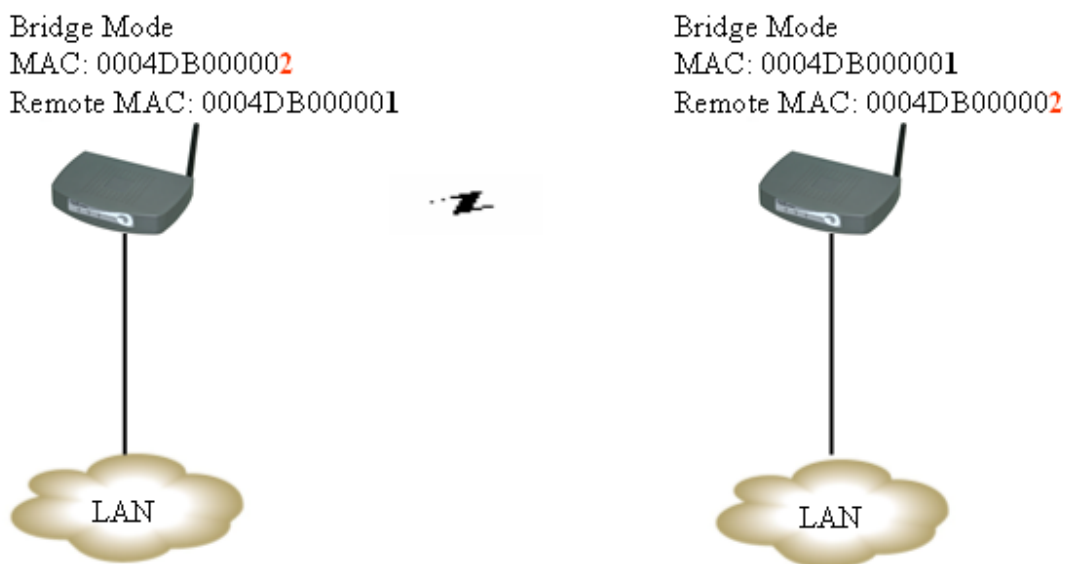


Figure 1-4 Bridge mode configuration example

2. Installation

2.1 Package Contents

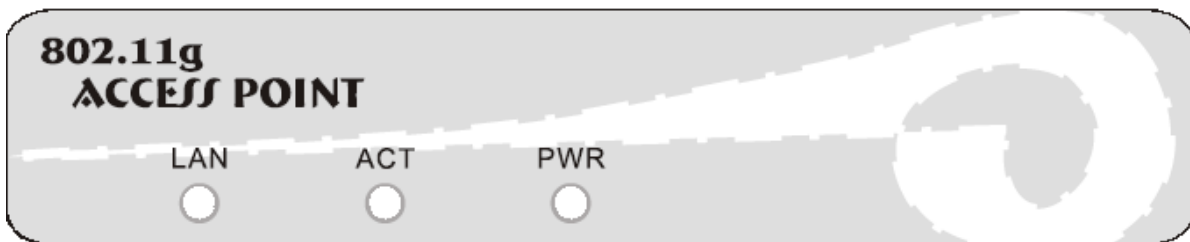
The product package should contain the following items:

- 802.11g/b Access Point
- Antenna
- CD-ROM (User manual)
- Power Adapter

If any of the parts are incorrect, missing, or damaged, please contact your vendor. Retain the carton and the original packing materials in case you need to return the product.

2.2 The AP Front

The front panel provides LED's for device status.



Refer to the following table for the meaning of each feature.

LED	Status	Description
LAN	Off	No Ethernet link detected
	Green On	10/100Mbps Fast Ethernet link detected. No Activity.
	Green Blinking	Indicates data traffic on 10/100 Mbps LAN
ACT	Yellow Blinking	Indicates the device is linking or active data through wireless links
PWR	Off	No Power
	Green On	1. Power on 2. Reset to default 3. Firmware upgrade (first 1 minute)
	Green Blinking	1. System up 2. Power on 3. Firmware upgrade

2.3 The AP's Rear Panel

The rear panel contains the port connections described below (Figure 2-1):

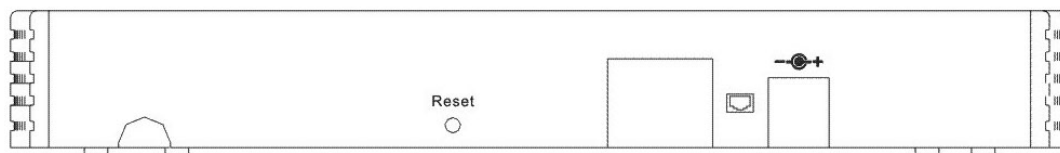


Figure 2-1 Rear Panel

Items	Description
Power Inlet	Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may damage your AP.
LAN Port	Connect device (such as a PC, hub, switch or router) on your local area network to this port.
Reset Button	Press the button (10 second) to restore the default factory settings.
Wireless antenna	Rotate antenna to the best position for more effective coverage.

2.4 System Requirement

Your system should meet the following requirements to install the AP successfully.

- A Cable/DSL modem/router with 10/100 Mbps Ethernet port or a 10/100 Mbps LAN device such as a hub or switch.
- A category 5 UTP Ethernet cable with RJ-45 connectors and enough length from the location of AP to the modem, router, hub or switch.
- An A/C power outlet (100~240V, 50~60Hz) or device with PSE (refer to 2.8) close to the location of AP
- Microsoft Internet Explorer 5.00.3700.1000 or later (Netscape V6/7 or later) web browser for configuration.
- One computer with TCP/IP protocol installed.
- 802.11g/b compliant adaptors.

2.5 Default Settings

The following table shows **The AP** default settings.

Items	Default Setting
IP Address	192.168.1.250
User Name/Password	admin/admin
IP Subnet Mask	255.255.255.0
SSID	ap11g
RF channel	6
Mode	11b+g
WEP	Disabled

2.6 Connect the Power Adapter

Plug the power adapter into the power inlet on **The AP**, and the other end into a power outlet. Check the **Power** LED on the front panel to make sure it is on. **Warning:** Use only power adapter supplied with **The AP**; otherwise, **The AP** may be damaged.

2.7 Connect to a Network

Use twisted-pair RJ-45 connector Ethernet cable to connect the LAN ports to a cable/DSL modem, Ethernet hub, switch or router. If it is correctly connected, the LAN LED will be on.

2.8 Power over Ethernet (PoE) - Optional

In addition to use the power adapter to provide the DC power to **The AP**. It also supports the Power over Ethernet (IEEE 802.3af standards) function. The DC power can be provided via the Ethernet cable as described below:

2.8.1 PoE Splitter device

The AP can be powered from Ethernet cable with 48Vdc. The 48Vdc power is provided by the PoE splitter devices (Figure 2-2) that meet IEEE802.3af standard. This splitter device will inject 48Vdc power into the Ethernet cable.

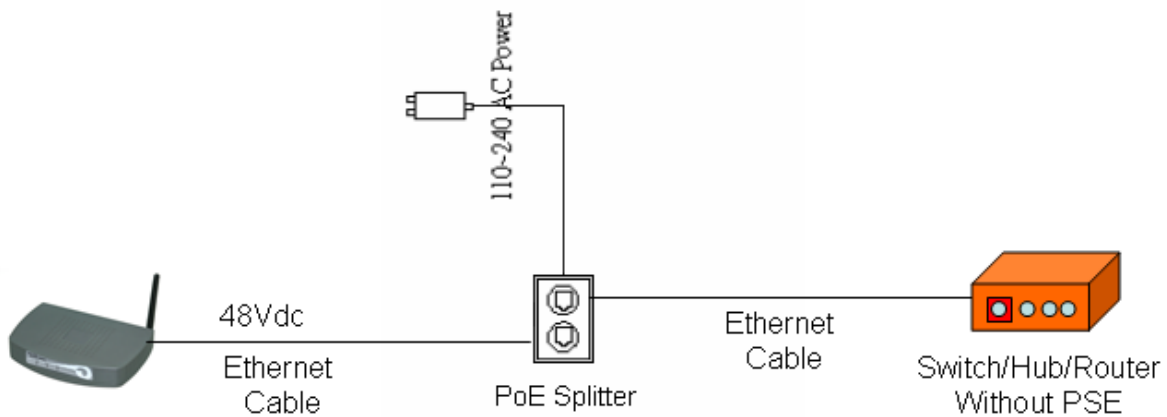


Figure 2-2 PoE Splitter Device

2.8.2 PSE Device

The AP can be powered from Ethernet cable with 48VDC. The 48Vdc power is provided by the Power Sourcing Equipment (PSE) device that meet IEEE802.3af standard (Figure 2-3).

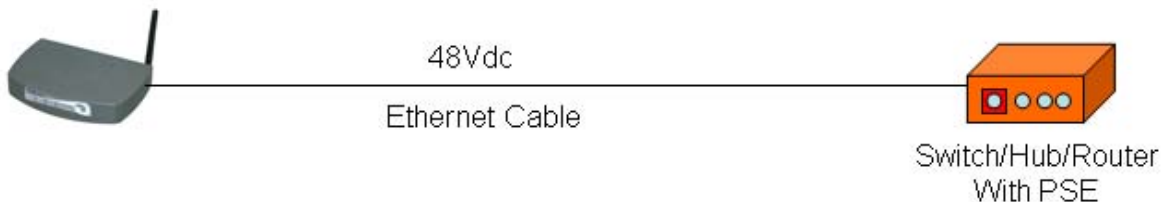


Figure 2-3 PSE Device

3. Configuration

TURN ON POWER SUPPLY

Quick power cycle can caused system corruption. When power on, be careful not to shut down in about 5 seconds, because data is writing to the flash.

START UP & LOGIN

Before Starting

The default IP address setting for the unit is a class C IP address (192.168.1.250/255.255.255.0). Please make sure that the current workstation is following the class C IP address range, from 192.168.1.1 to 192.168.1.254, refer to Appendix A.

In order to configure **The AP**, you must use your web browser and manually input <http://192.168.1.250> into the Address box and press Enter. To start configure **The AP**, you must login as “**admin**” in the **User Name** box. And input password “**admin**” on the password section.

Once you have logged-in as administrator, it is a good idea to change the administrator password to ensure a secure protection to **The AP**. The Security Settings section described later in this manual describes how to change the password.

Once you have input the correct password and logged-in, the screen will change to the Setup page screen.

3.1 Primary Setting

MAKE CORRECT NETWORK SETTINGS OF YOUR COMPUTER

To change the configuration, use Internet Explorer (IE) or Netscape Communicator to connect the web management via IP address **192.168.1.250**.

Primary Setup screen contains all of the AP's basic setup functions, refer to Figure 3-1.

Primary Setup This section contains the primary configuration for the Access Point. You should be able to customize easily the Ethernet and Wireless interface in this section. **Remember to press Apply for finalizing your configuration.**

AP Name:

LAN MAC Address: **00:0E:8E:7A:2B:5C**

Configuration type:

IP Address: . . . This is the IP Address, Subnet Mask and

Subnet Mask: . . . Default Gateway of the Access Point as it is

Gateway: . . . seen by your local network.

Wireless MAC Address: **00:0E:8E:7A:2B:5C**

Mode:

SSID: SSID Broadcast:

Channel:

Domain: Europe

Security: Enable Disable

Firmware Version: v1.3.02

Figure 3-1 Primary Setup

Most users will be able to configure the AP and get it working properly using the settings on this

screen.

LAN IP Address and Subnet Mask: This is the AP's IP Address and Subnet Mask as seen on the internal LAN. The default value is 192.168.1.250 for IP Address and 255.255.255.0 for Subnet Mask.

Wireless: This section provide the Wireless Network settings for your WLAN

SSID: The service set identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. You shall have selected the same SSID for all the APs that will be communicating with mobile wireless stations.

Channel: Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP to avoid signal interference.

Security: There are 3 types of security to be selected. To secure your Wireless Networks, it's strongly recommended to enable this feature.

3.1.1 WEP

Make sure that all wireless devices on your network are using the same encryption level and key. WEP keys must consist of the letters "A" through "F" and the numbers "0" through "9."

Make sure that all wireless devices on your 2.4GHz network are using the same encryption level and key. WEP keys must consist of the letters "A" through "F" and the numbers "0" through "9".

Default Transmit Key: 1 2 3 4

WEP Encryption: 64Bit (10 hex digits) ▾

Passphrase:

key 1:

key 2:

key 3:

key 4:

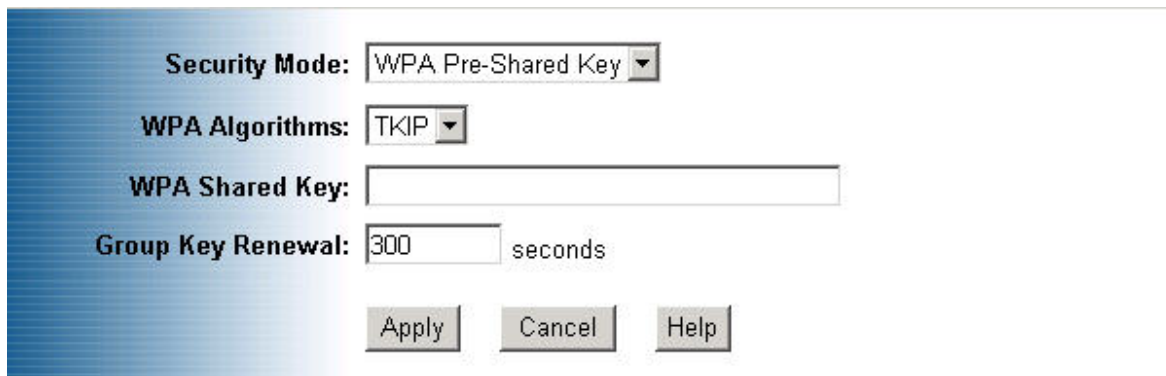
3.1.2 WPA-Preshared key

Important Notice

In order to make right use of WPA, please ensure that your current Wireless Adapter's driver, and Wireless Utility can support it, WPA needs 802.1x authentication (when RADIUS mode is chosen), though the Operating System must also support 802.1x protocol. For Microsoft's OS family, only Windows XP has incorporated this by default. The rest of the OS must installed third party's client software such as Funk ODySSey.

There are two encryption options for WPA Pre-Shared Key: TKIP and AES. TKIP stands for Temporary Key Integrity Protocol. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. AES stands for Advanced Encryption System, which utilizes a symmetric 128-Bit block data encryption.

To use WPA Pre-Shared Key, enter a password in the WPA Shared Key field between 8 and 63 characters long. You may also enter a Group Key Renewal Interval time between 0 and 99,999 seconds.



The screenshot shows a configuration window for WPA Pre-Shared Key. It includes the following fields and controls:

- Security Mode:** A dropdown menu currently showing "WPA Pre-Shared Key".
- WPA Algorithms:** A dropdown menu currently showing "TKIP".
- WPA Shared Key:** An empty text input field.
- Group Key Renewal:** A text input field containing "300" followed by the label "seconds".
- Buttons:** Three buttons labeled "Apply", "Cancel", and "Help" are located at the bottom of the dialog.

WPA Algorithms	Please choose your algorithms method. You can select between TKIP and AES.
WPA Shared Key	Please input the Pre-Shared Key. The key should be 8 characters or 63 characters in alphanumeric.
Group Key Renewal	Please input the period of renewal time. The default selection is 300 seconds.

3.1.3 WPA RADIUS

WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS Port (default is 1812) and the shared secret from the RADIUS server.

The screenshot shows a configuration window with a blue gradient background. It contains several fields and buttons:

- Security Mode:** A dropdown menu with "WPA RADIUS" selected.
- WPA Algorithms:** A dropdown menu with "TKIP" selected.
- RADIUS Server Address:** Four input boxes containing "0", "0", "0", and "0" separated by dots.
- RADIUS Server Port:** An input box containing "1812".
- Radius Shared Secret:** A long, empty text input box.
- Group Key Renewal:** An input box containing "300" followed by the text "seconds".
- At the bottom, there are three buttons: "Apply", "Cancel", and "Help".

WPA Algorithms	Please choose your algorithms method. You can select between TKIP and AES.
RADIUS Server Address	Please input your RADIUS Server IP address.
RADIUS Server Port	Please input the Authentication port of your RADIUS server. The default port being used is 1812
RADIUS Shared Secret	The RADIUS server will accept the authentication if both Shared Secret matched.
Group Key Renewal	Please input the period of renewal time. The default selection is 300 seconds.

* Click **Apply** to save your settings.

3.2 System

Click the **System** option on the upper frame to manage the password, restore factory defaults, backup/restore settings, or upgrade the system firmware, refer to Figure 3-2.

The screenshot shows the 'System' configuration page of a wireless access point. At the top, there is a navigation bar with the following tabs: Primary Setup, System (selected), Operating Mode, Status, Traffic Log, Advanced Setup, and Help. The main content area is titled 'System' and contains the following sections:

- System:** A text block stating: "It is strongly recommended to change the default password for you Access Point in order to avoid any security risks. In this section you can also Restore and Backup the Setting to a Profile."
- AP Password:** Two input fields for password entry. The first is labeled "(Enter New Password)" and the second is labeled "(Re-enter to Confirm)". Both fields contain six black dots.
- Restore Factory Defaults:** Radio buttons for "YES" and "NO". The "NO" option is selected.
- Note:** "Note: If YES, all setting will be restored as factory default setting."
- Backup/Restore Setting:** Two buttons: "Backup Setting" and "Restore Setting".
- Note:** "Note: Click on 'Backup Setting' to create and save the setting on your local hard drive. Click on 'Restore Setting' to load the setting profile from your hard drive."
- Firmware Upgrade:** A section showing "Current Version: v1.3.02" and a "Firmware Upgrade" button.
- Buttons:** At the bottom, there are three buttons: "Apply", "Cancel", and "Help".

Figure 3-2 System Setting

AP Password: Changing the password for the AP is as easy as typing the password into the **Enter New Password** field. Then, type it again into the **Re-enter to Confirm** field.

* Click the **Apply** button to save the setting.

Note: Use the default password when you first open the configuration pages, after you have configured these settings, you should set a new password for the AP (using the Password screen). This will increase security, protecting the AP from unauthorized changes.

Restore Factory Defaults: Click the **Yes** button to reset all configuration settings to factory default values. Note: Any settings you have saved will be lost when the default settings are restored. Click the **No** button to disable the Restore Factory Defaults feature.

Click the **Apply** button to save the setting.

Backup/Restore Setting: Click Backup to store the Access Point's configuration on your local PC.
Click Restore to restore Access Point's configuration from your local PC

Firmware Upgrade: Refer to section 3.9.

* Check all the settings and click **Apply** to save them.

3.3 Operation Mode

The AP supports 4 operation modes: Access Point, AP Client, AP Repeater and Wireless Bridge.

54Mbps 2.4 Wireless-G

Primary Setup System **Operating Mode** Status Traffic Log Advanced Setup Help

Operating Mode

Please assign the operating mode to the device. You can select between "AP", "AP Client", "AP Repeater" or "Wireless Bridge" mode. The default operating mode of the device is "AP". For further understanding on Operating Mode selection, please refer to the User Guide or Help.

LAN MAC Address: **00:0E:8E:7A:2B:5C**

Access Point (Default Selection)

AP Client

Please input the MAC Address of the remote AP:

AP Repeater

Please input the MAC Address of the remote AP:

Enable LAN port

Note: Please leave the option "Enable LAN port" selected. This will allow your wired PC to join the remote AP's network. In other case, you will only be able to configure the unit through Wireless Interface.

Wireless Bridge

Please input the MAC Address of the remote Wireless Bridge:

Note: When the unit is operating as "Wireless Bridge", it will interact only with other remote Wireless Bridge on the MAC Address list.

Figure 3-3 Operation Mode

Click the **Operation Mode** option on the upper frame to select the AP operation mode, refer to Figure 3-3.

Access Point: This mode provides access for wireless stations to wired LANs and from wired LANs to wireless stations.

AP Client: Input the MAC Address of the remote AP. In this operating mode, the device will be used as wireless NIC.

AP Repeater: This mode allows the AP to keep the AP function role and at the same time performing a communication with other 802.11g AP to establish and extend your Wireless Network cover. Please enter the Remote Access Point's MAC address to enable this feature.

Wireless Bridge: This mode allows the connection of one or more remote LANs with a central LAN. Input the MAC Address of the remote AP.

* Click **Apply** to save your settings.

3.4 Status

Click the **Status** option on the upper frame to display AP existing status, refer to Figure 3-4.

The screenshot shows the 'Status' page of a 54Mbps Wireless-G AP. The top navigation bar includes 'Primary Setup', 'System', 'Operating Mode', 'Status', 'Traffic Log', 'Advanced Setup', and 'Help'. The 'Status' section contains a summary of the system, updated every 10 seconds. Below this, the 'AP Name' is 'ap11g' and the 'Firmware Version' is 'v1.3.02, May 24, 2004'. The 'LAN' section shows the MAC Address as '00:0E:8E:7A:2B:5C' and configuration details: Static IP Address, IP Address '192.168.1.250', and Subnet Mask '255.255.255.0'. The 'Wireless' section shows the same MAC Address and SSID 'ap11g', with Mode '11b+g', Channel '6', and Security 'Disable'. It also displays packet statistics for 'Send' and 'Received' traffic, with 57 Good Packets sent and 0 Dropped Packets. A note states that dropped packets are normal in wireless transmission. 'Refresh' and 'Help' buttons are at the bottom.

Status		
This section contains a summary of the system. Please note that the information will be updated and displayed automatically every 10 seconds.		
AP Name: ap11g		
Firmware Version: v1.3.02, May 24, 2004		
LAN		
MAC Address: 00:0E:8E:7A:2B:5C		
Configuration Type:	Static IP Address	
IP Address:	192.168.1.250	
Subnet Mask:	255.255.255.0	
Wireless		
MAC Address: 00:0E:8E:7A:2B:5C		
SSID:		ap11g
Mode:		11b+g
Channel:		6
Security:		Disable
Send	Good Packets:	57
	Dropped Packets:	0
Received	Good Packets:	0
	Dropped Packets:	0
Note: In wireless transmission, some dropped packets occurrence is normal.		
Refresh Help		

Figure 3-4 Status

This screen displays the AP current status and settings. This information is read-only. This page will auto re-flash every 10 seconds to keep most update information.

LAN section will be displaying all information related on AP, such as the IP address and the current configuration type.

Wireless section will be displaying information related on the Wireless interface, such as SSID, Channel, Encryption and statistics of network traffic.

*Click the **Refresh** button to refresh the AP's status and settings.

3.5 Traffic Log

Click the **Traffic Log** option on the upper frame to manage AP traffic log, refer to Figure 3-5.



Figure 3-5 Traffic Log

Traffic Log: The AP can keep logs of all incoming or outgoing traffic for your network traffic. This feature is disabled by default. To keep activity logs, select **Enable**, refer to Figure 3-6.

To keep a permanent record of activity log, the IP address of Syslog Daemon should be specified.

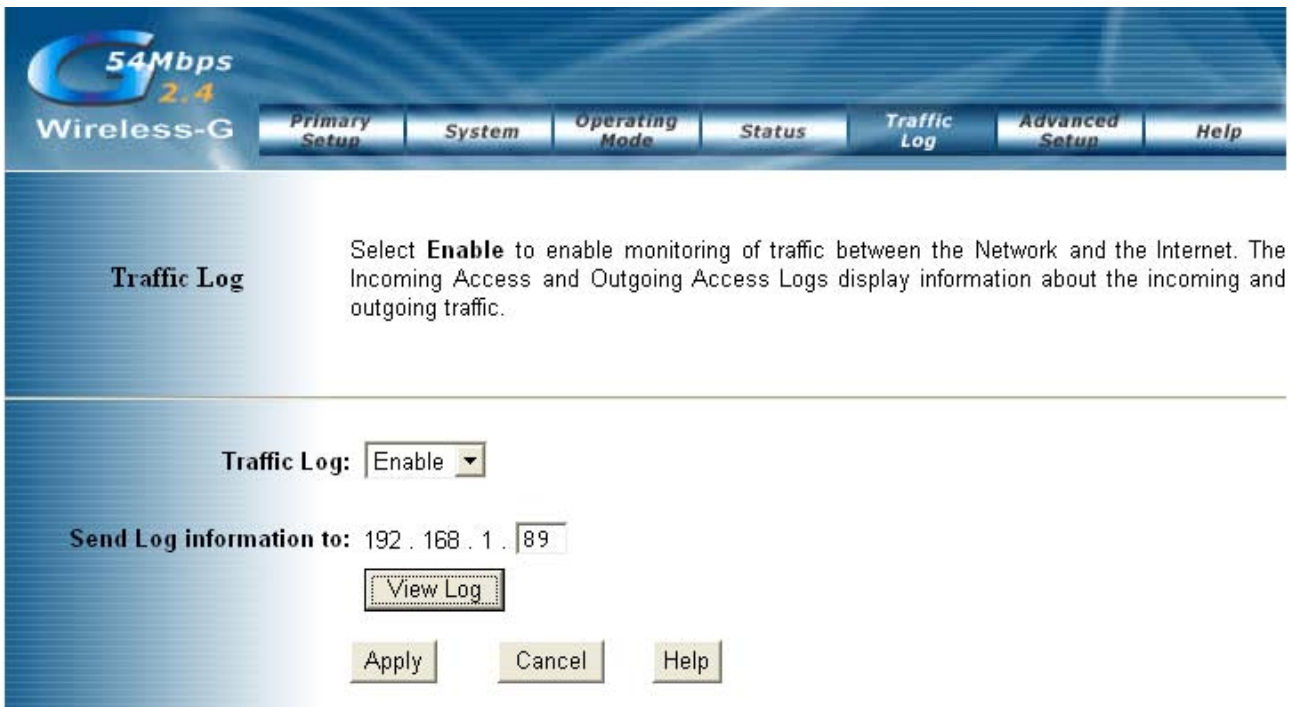


Figure 3-6 View Traffic Log

To see a temporary log of the AP's most recent traffic, click the **View Log** button.

Click the **Apply** button to save the setting.

3.6 Access Control

Click the **Advanced Setup** on the upper frame and then select **Enable** for the **Access Control**. After clicking the **Apply** button, Figure 3-7 will be displayed. Enter the MAC address of the target workstation that will be permitted or denied the connection to the network.

Access Control Please input the MAC address of each target workstation in order to Permit or Deny the connection to the network.

Access Control:

Deny wireless connection to join the unit from the list.
 Allow wireless connection to join the unit from the list.

(Enter the MAC Addresses in the this format:xxxxxxxxxxxx)

MAC 01	<input type="text"/>	MAC 11	<input type="text"/>
MAC 02	<input type="text"/>	MAC 12	<input type="text"/>
MAC 03	<input type="text"/>	MAC 13	<input type="text"/>
MAC 04	<input type="text"/>	MAC 14	<input type="text"/>
MAC 05	<input type="text"/>	MAC 15	<input type="text"/>
MAC 06	<input type="text"/>	MAC 16	<input type="text"/>
MAC 07	<input type="text"/>	MAC 17	<input type="text"/>
MAC 08	<input type="text"/>	MAC 18	<input type="text"/>
MAC 09	<input type="text"/>	MAC 19	<input type="text"/>
MAC 10	<input type="text"/>	MAC 20	<input type="text"/>

Figure 3-7 Access Control

Access Control: This function will allow administrator to have access control by enter MAC address of client stations. When **Enable** this function, two new options will show up.

Depend on the filtering propose, it can be selected to **Deny** or **Allow**.

Fill the client stations MAC list to complete the configuration. The table could store up to **40** different MAC addresses. Please follow the format that it required when an address is input.

* Click **Apply** to save your settings.

3.7 Advanced Wireless

Click the **Advanced Wireless** option on the upper frame to set WLAN related parameters, refer to Figure 3-8. You can change the values of AP to have better interoperability with WLAN station. It is suggested to use the default values.

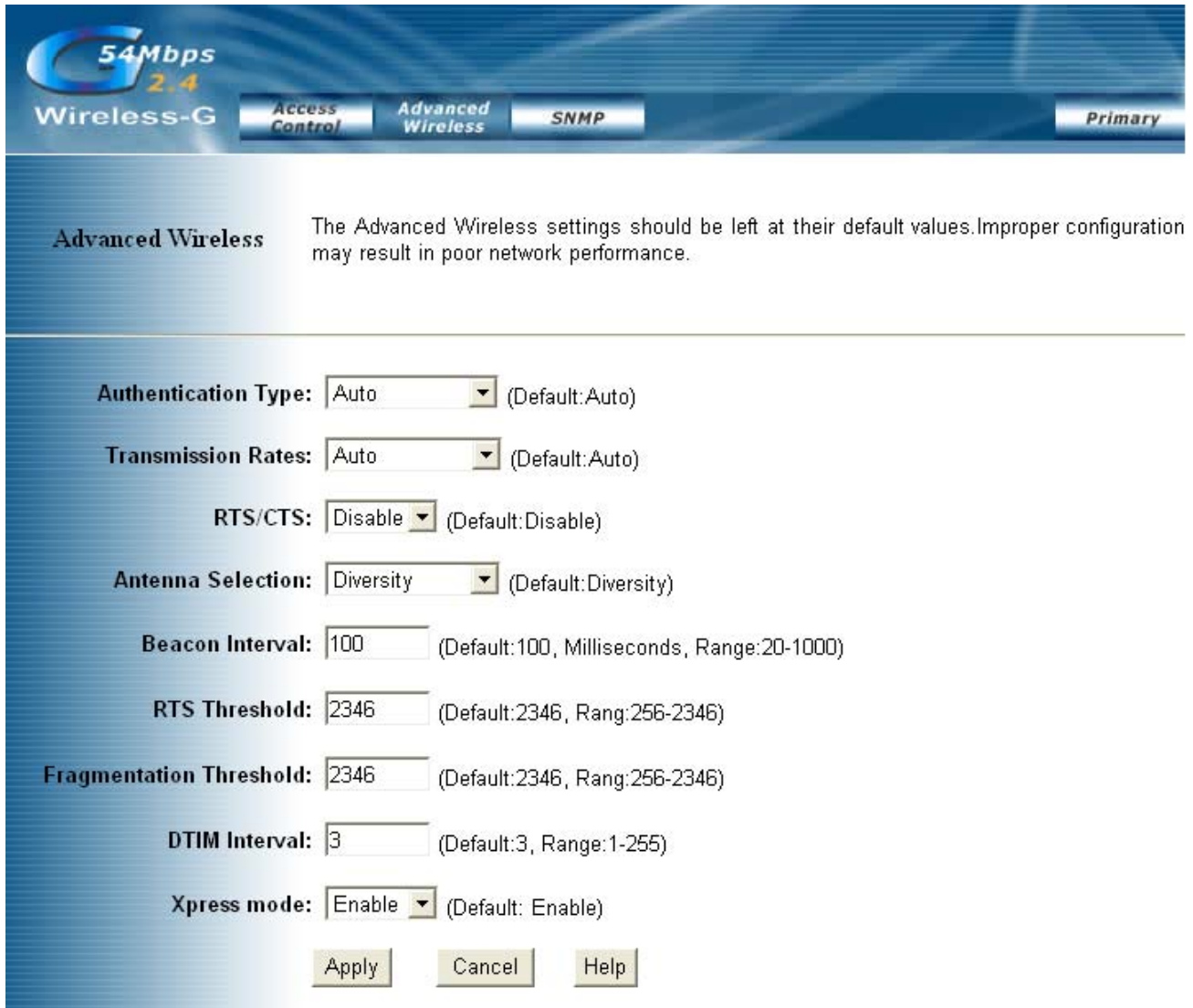


Figure 3-8 Advanced Wireless

Authentication Type:

Auto: Auto is the default authentication algorithm. It will change its authentication type automatically to fulfill client's requirement.

Open System: Open System authentication is not required to be successful while a client may

decline to authenticate with any particular other client.

Shared Key: Shared Key is only available if the WEP option is implemented. Shared Key authentication supports authentication of clients as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in clear. Requiring the use of the WEP privacy mechanism.

Transmission Rate: The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **AUTO** to have the AP automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client. The default setting is **AUTO**.

Beacon Interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the AP to synchronize the wireless network. The default value is **100**.

Antenna selection: There are 3 types antenna setting for this device. Default setting is Diversity.

RTS Threshold: This value should remain at its default setting of 2346. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The AP sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

Fragmentation Threshold: This value specifies the maximum size for a packet before data is fragmented into multiple packets. It should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Access Point Clients hear the beacons and awaken to receive the broadcast and multicast messages.

Turbo mode: Enable this setting can accelerate the transmit data rate up to 40%.

* Click **Apply** to save your settings.

3.8 SNMP Info

Click the **SNMP Info** option on the upper frame to monitor network device, refer to Figure 3-9.

SNMP INFO Based on Simple Network Management Protocol, you can quickly control and monitor any network device. Please fill out the correspond information on this page to start the monitoring.

SNMP V1/V2c:

Information: Contact:
Unit Name and description:
Physical Location:

SNMP Community:

Figure 3-9 SNMP Info

SNMP INFO: The SNMP screen allows you to customize the Simple Network Management Protocol (SNMP) settings. SNMP is a popular network monitoring and management protocol.

SNMP V1/V2c		To enable the SNMP feature, select Enable . Otherwise, select Disable .
Information	Contact	In the contact field, enter contact information for the AP.
	Unit Name and description	In the Unit Name and description field, enter the name of the AP or AP description.
	Physical Location	In the Physical Location field, specify the area or location where the AP resides.

SNMP Community	public	You may change the SNMP Community's name from its default, public . Then configure the community's access as either Read-Only or Read-Write .
	private	You may change the SNMP Community's name from its default, private . Then configure the community's access as either Read-Only or Read-Write .

Click **Apply** to save your settings.

3.9 Upgrade Firmware

To perform the firmware upgrade, please refer to the Figure 3.2

Click the **Firmware Upgrade** button to load new firmware onto the **The AP**. If the AP is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

Warning: When you upgrade the AP's firmware, you may lose its configuration settings, so make sure you write down the AP's settings before you upgrade its firmware.

To upgrade the AP's firmware:

1. Download the firmware upgrade file
2. Extract the firmware upgrade file.
3. Click the Firmware Upgrade button.
4. On the Firmware Upgrade screen, click the **Browse** button to find the firmware upgrade file.



5. Double-click the firmware upgrade file.
6. Click the Upgrade button, and follow the on-screen instructions.

Note: Do not power off the AP or press the Reset button while the firmware is being upgraded.

4. Troubleshooting

a). My Wireless AP will not turn on.

No LED's light up.

Cause:

- The power is not connected.

Resolution:

- Connect the power adapter to your AP and plug it into the power outlet or check the PSE.

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

b). LAN Connection Problems:

I can't access my AP.

Cause:

- The unit is not powered on.
- There is not a network connection.
- The computer you are using does not have a compatible IP Address.

Resolution:

- Make sure your AP is powered on.
- Make sure that your computer has a compatible IP Address. Be sure that the IP Address used on your computer is set to the same subnet as the AP. For example, if the AP is set to 192.168.1.250, change the IP address of your computer to 192.168.1.15 or another unique IP address that corresponds to the 192.168.1.X subnet.
Use the Reset button located on the rear of the AP to revert to the default settings.

I can't connect to other computers on my LAN.

Cause:

- The IP Addresses of the computers are not set correctly.
- Network cables are not connected properly.
- Windows network settings are not set correctly.

Resolution:

- Make sure that each computer has a unique IP address. And the IP must be in the same subnet as the AP.
- Make sure that the Link LED is on. If it is not, try a different network cable.
- Check each computer for correct network settings.

c). Wireless Troubleshooting

I can't access the Wireless AP from a wireless network card

Cause:

- Out of range.
- IP Address is not set correctly.

Resolution:

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

d). Lost or forgot Administrator password.

- Reset system setting (by holding **Reset** button down for 10 seconds) into factory default, this will restore administrator password to **admin/admin**.
- Re-configure your AP according to your previous setting.

Warning: When you reset the AP device, the configuration settings will also be reset to the factory default. Make sure you have written down the AP settings for record.

Appendix A

Configure PC's IP address manually

- (a). Select **IP Address** tab, and then choose **Specify an IP Address**. Type in your customized IP address (the default IP address of this product is 192.168.1.250. So you can type in an IP Address such as 192.168.1.xxx.). Set the Subnet Mask as 255.255.255.0.
- (b). Click **Gateway** tab, and add IP address of the router (e.g. the AP's IP Address is 192.168.1.250).
- (c). Change to **DNS Configuration** tab; enable DNS and add DNS values provided by your ISP into **DNS Server Search Order** (See Figure A-1).

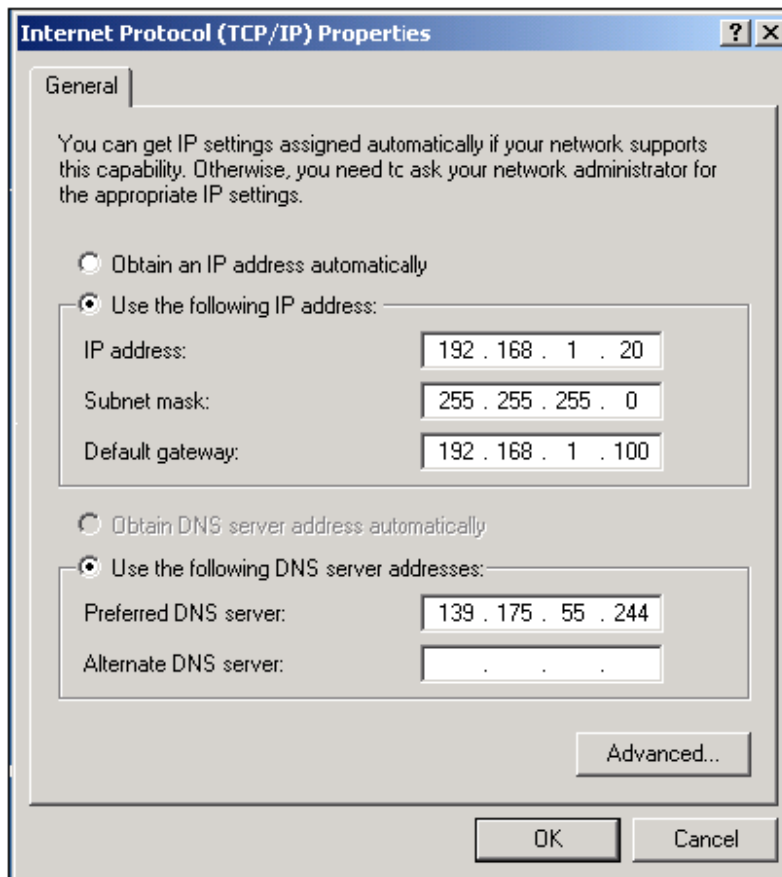


Figure A-1 DNS Configuration tab

- (d). Click **OK** to finish.

Appendix B

Technical information

General:

- Standard Compliance: IEEE 802.11g/b, IEEE 802.3af, IEEE 802.3, IEEE 802.3u, IEEE 802.1x
- Security: WEP 64 and 128 Bit Encryption, WPA, IEEE802.1x

LAN Interface:

- LAN Port Connection (RJ45): 10/100 Mbps auto-sensing, MDI- MDIX auto-sensing, PoE

WLAN Radio:

- Frequency Band: 2.4 ~ 2.4835 GHz
- Spread Spectrum Technology: DSSS (Direct Sequence Spread Spectrum)
- Modulation: DBPSK for 1 Mbps, DQPSK for 2 Mbps, CCK for 5.5 /11 Mbps,
OFDM for 6/9/12/18/24/36/48/54 Mbps
- Data Rate: up to 54Mbps with Auto Fallback
- Radio Output Power (Typical): +15 dBm
- Receive Sensitivity (Typical @BER < 10E-5): -80 dBm @ 11 Mbps
-65 dBm @ 54 Mbps
- Operating range: Open environment: Up to 300m, Office environment: 30 ~ 100m

Management:

- Web-Based management (single log-in with timeout protection)
- Supports SNMP (get)

Maximum Users:

- Up to 64 wireless users per channel

Mechanical:

- Antenna Connector: RSMA for external antenna
- Antenna type: External Dipole Antenna
- LED Indicators: LAN, Activity, Power, PoE
- Dimension: 167.0 × 117.5 × 31.7mm/ 6.6 × 11.8 × 12.5 in
- Weight: 300g / 10.6 oz
- Mounting: Desktop, ceiling or wall-mounted hardware included
- Power Adapter: 90 ~ 264 Vac input, 5 Vdc, 2A output
- Typical load: 560 mA @ 5VDC, 630mA @ PoE

Environmental:

- Temperature: Operating: 0 to +40°C / 32 to 104°F
Storage: -20 to +70°C / -4 to +158°F
- Humidity: 0 ~ 90% (non-condensing)

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection 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 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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.