

GL2411AP-0A
Access Point

Version:4.0 Date:2001/7/15

Federal Communications Commission Statement

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

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the 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. If this equipment is not installed and used in accordance with the manufacturer's instructions, it 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 to 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.

The use of shielded cables for connection of the monitor to the graphics card is required to assure compliance with FCC regulations. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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 and your body.

Manufacturer's Disclaimer Statement

The information in this document is subject to change without notice and does not represent a commitment on the part of the vendor. No warranty or representation, either expressed or implied, is made with respect to the quality, accuracy or fitness for any particular purpose of this document. The manufacturer reserves the right to make changes to the content of this document and/or the products associated with it at any time without obligation to notify any person or organization of such changes. In no event will the manufacturer be liable for direct, indirect, special, incidental or consequential damages arising out of the use or inability to use this product or documentation, even if advised of the possibility of such damages. This document contains materials protected by copyright. All rights are reserved. No part of this manual may be reproduced or transmitted in any form, by any means or for any purpose without expressed written consent of its authors. Product names appearing in this document are mentioned for identification purposes only. All trademarks, product names or brand names appearing in this document are registered property of their respective owners.

Printed in Taiwan

Contents

SECTION 1 ABOUT GL2411AP-0A ACCESS POINT.....	3
INTRODUCTION.....	3
1-1 FEATURES.....	3
1-2 FIRMWARE FUNCTIONALITY.....	錯誤! 尙未定義書籤。
1-3 APPLICATIONS.....	3
1-4 PRODUCT KIT.....	4
SECTION 2 HARDWARE INSTALLATION.....	5
2-1 EQUIPMENT REQUIREMENT.....	5
2-2 GL2411AP-0A HARDWARE INSTALLATION.....	5
2-3 SOFTWARE LIMITATION.....	5
SECTION 3 CONFIGURING GL2411AP-0A ACCESS POINT.....	7
3-1 INSTALLING USB DRIVER FOR ACCESS POINT.....	7
3-1-1 Installing GL2411AP-0A USB Driver for Windows® 98.....	7
3-1-2 Installing GL2411AP-0A USB Driver for Windows® 2000.....	9
3-1-3 Installing GL2411AP-0A USB Driver for Windows® Millennium.....	11
3-2 GL2411AP-0A ACCESS POING DFU UTILITY.....	13
3-2-1 DFU (USB Configuration Utility) Utility Installation.....	13
3-2-2 DFU (USB Configuration Utility) Utility Configuration.....	14
3-3 GL2411AP-0A ACCESS POING SNMP MANAGER UTILITY.....	18
3-2-1 SNMP Manager Utility Installation.....	18
3-2-2 SNMP Manager Utility Configuration.....	19
APPENDIX A NETWORK CONFIGURATION.....	29
A-1 NETWORK TOPOLOGY.....	29
Ad-Hoc Mode.....	29
Infrastructure.....	30
A-2 ROAMING.....	30
APPENDIX B SPECIFICATIONS.....	32
APPENDIX C GLOSSARY.....	33

Section 1 About GL2411AP-0A Access Point

Introduction

The GL2411AP-0A (11 Mbps WLAN Access Point) is a long-range, high performance LAN product, which provides Access Point services to a 2,4 GHz RF network and bridges to an Ethernet backbone. The design of this product is based on AT76C510 (bridge-on-a-chip) module, a highly integrated ASIC designed to combine legacy LANs with wireless LANs. AT76C510 performs all the necessary inter-networking and bridging functions. It receives data from both networks, stores them locally for further processing, installs and maintains connections and transmits the packets to the proper destination. Furthermore, AT76C510 interfaces three more modules, the Ethernet PHY, the wireless PHY and the RAM modules, for allowing compact system implementation and flexibility for supporting almost all the possible physical interfaces.

1-1 Features

- Supports 11 Mbps rates with automatic fallback to 5.5, 2 and 1 Mbps
- For the security issue, the GL2411AP-0A in the firmware version of 1.4f supports 64/128 Bit WEP encryption/decryption and Password Setting function.
- Ethernet MAC supports MII interface and 10/100Mbit speeds
- Hardware modules for Packet Filtering and statistics gathering
- Glueless SRAM, Flash interface for data buffering and program storage, supporting up to 16 MB of memory
- Integrated 2 x 6K x 32 bit internal SRAM modules for fast 32-bit program execution and temporary storage of data
- Supports 3V supply
- JTAG Boundary Scan (IEEE 1149.1) test access port for board-level production test
- Support DHCP Client Function, Building to Building Bridge Function.
- Support MAC Filtering function to avoid the Access Point loading thru connection with the un-permitted MAC addresses.
- Support Station information to check the association status with which stations.
- Support Statistic data for the connection.

1-3 Applications

The Serial of LAN products offer a fast, reliable, cost-effective solution, allowing clients to wirelessly

access the network in applications such as following:

1. Remote access to corporate network information

E-mail, file transfer and terminal emulation

2. Difficult-to-wire environments

Historical or old buildings, asbestos installations, and open area where wiring is difficult to employ

3. Frequently changing environments

Retailers, manufacturers and banks who frequently rearrange the workplace and change location

4. Temporary LANs for special projects or peak time

Trade shows, exhibitions and construction sites need temporary setup for a short time period. Retailers, airlines and shipping companies need additional workstations for a peak period. Auditors require workgroups at customer sites.

5. Access to database for mobile workers

Doctors, nurses, retailers, white-collar workers need access to database while being mobile in the hospital, retail store or office campus.

6. SOHO (Small Office and Home Office) users

SOHO users need easy and quick installation of a small computer network.

1-4 Product Kit

- ◆ **GL2411AP-0A**x 1
- ◆ **Antenna (fixed)**.....x 2
- ◆ **GL2411AP-0A utility CD**.....x 1
- ◆ **A/C Power Adapter**.....x 1
- ◆ **USB cable**.....x 1

If any of the listed items are not included or found damaged, please contact your local dealer.

Section 2 Hardware Installation

2-1 Equipment Requirement

Installation of GL2411AP-0A requires:

1. An A/C power outlet (100~240V,50~60Hz) which supply the power for the GL2411AP-0A Access Point
2. A 10/100 Base-T (UTP) Ethernet cable drop (RJ-45 connector)

2-2 GL2411AP-0A Hardware Installation

Please follow these procedures while setting up the hardware:

1. Site Selection

Choose a proper place for your GL2411AP-0A.

In general, the best location to place your GL2411AP-0A is the center of your wireless coverage, with line of sight to all your mobile stations.

2. Adjust the direction of the Antenna

Adjust the direction of the antenna placement to improve the GL2411AP-0A's performance. Try to place the antenna in the position which can best cover its BSS. Normally, the higher you place the antenna, the better the performance will be. The character of diversity enhances the receiving sensitivity.

3. Connect the Ethernet Cable

GL2411AP-0A can be connected to the 10/100 Base-T Ethernet network. Connect your UTP Ethernet cable to the RJ-45 connector of the GL2411AP-0A AP and connect the other side of UTP Ethernet cable to a hub.

4. Connect the Power Cable

Connect the power adapter cable to the DC5V Power Socket of the GL2411AP-0A. ONLY use the power adapter supplied with the GL2411AP-0A. Otherwise, the product may be damaged.

2-3 Software Limitation

1. DFU Software

Operation System:

Chinese Windows 98/2000/ME, English Windows 98/2000/ME

2. SNMP Software

Operation System:

English Windows 98/NT/ME

Section 3 Configuring GL2411AP-0A Access Point

3-1 Installing USB Driver For Access Point

The Wireless Network Access Point GL2411AP-0A can be configured by DFU utility for Windows[®] 98/2000/ME. You need plug the USB cable with the GL2411AP-0A and the USB slot of the PC to run DFU.exe for configuring the GL2411AP-0A and setting the setup.

3-1-1 Installing GL2411AP-0A USB Driver For Windows[®] 98

1. Please boot your PC into Windows[®] 98.
2. Run DFUzip.exe in GL2411AP-0A Access Point utility CD to decompress the files into C:\DFU.
3. Ensure you have followed the procedure as described in the previous section to finish hardware installation.
4. Plug the two sides of the USB cable into the USB slots of GL2411AP-0A and your PC.
5. Windows[®] 98 will automatically detect the GL2411AP-0A and prompt you to install the necessary driver.
Please make sure that the Setup Utility CD is inserted into your CD ROM and click “Next” to begin the installation.



6. Select “Search for the best driver...” and click “Next”.



7. Select “Specify a location” and click “Browse”. On the windows information dialog, double-click the “D:\AP-OEM\USB DRIVER” folder icon from the list and Windows® 98 will automatically enter the path. Then click “Next”.



8. Windows® 98 will then acknowledge that it has found the appropriate driver and click "Next".
9. Windows® 98 will install the driver. As the driver files are being copied to the appropriate location, you will be prompted to insert the Windows® 98 CD.



NOTE: You must insert the Windows® 98 CD as the driver installation requires special files that will not be available, even if you have stored a copy of Windows® 98 source on your hard drive.

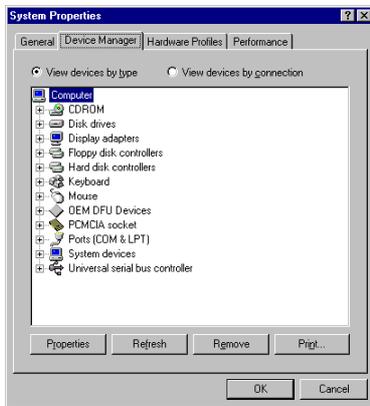
10. After Windows® 98 has finished installing the appropriate files, click “Finish”.



11. From the **Control Panel**, double-click the “System” icon.



12. From the “**Properties**” menu, please select the “**Device Manager**” tab. And check the “BRIDGE DFU DEVICE” device whether it works fine.

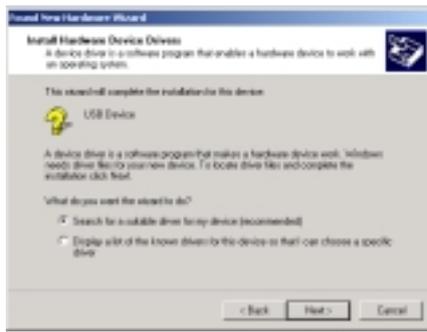


3-1-2 Installing GL2411AP-0A USB Driver For Windows® 2000

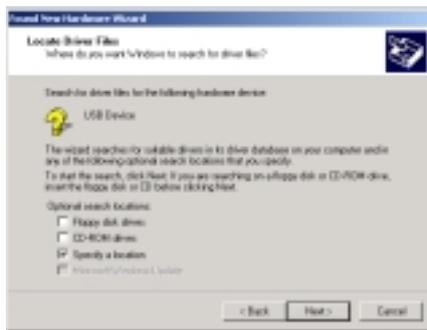
1. Please boot your PC into Windows® 2000.
2. Plug the two sides of the USB cable into the USB slots of GL2411AP-0A and your PC.
3. Windows® 2000 will automatically detect the GL2411AP-0A and prompt you to install the necessary driver. Make sure that the Setup Utility CD is inserted in the CD-Rom drive and click “Next” on the **Found New Hardware Wizard** screen to proceed.



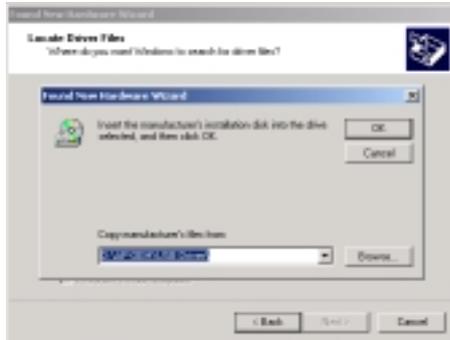
4. Select “Search for a suitable driver..” and click “Next” to search for the Windows® 2000 driver.



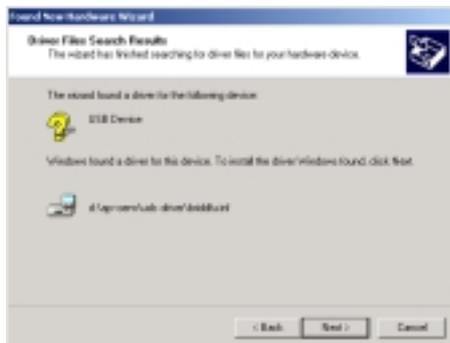
5. In “Optional Search Location”, Select “CD-ROM Drive” and click “Next”.



6. Please browse the file as shown in the dialog box, then click “OK”.



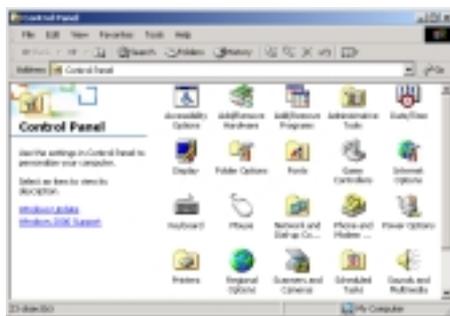
7. Windows® 2000 is now ready to install the driver. Click “Next” to continue.



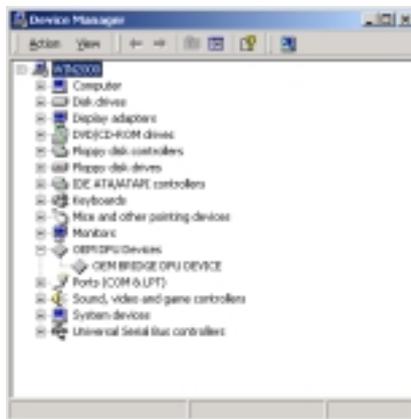
8. After Windows® 2000 has finished installing the appropriate files, click “Finish”.



9. From the **Control Panel**, double-click the “System” icon.



10. From the **“Properties”** menu, please select the **“Device Manager”** tab. And check the **“BRIDGE DFU DEVICE”** device whether it works fine.



3-1-3 Installing GL2411AP-0A USB Driver For Windows® Millennium

1. Please boot your PC into Windows® Millennium.
2. Plug the two sides of the USB cable into the USB slots of GL2411AP-0A and your PC.
3. Windows® ME will automatically detect the GL2411AP-0A and prompt you to install the necessary driver. Select “Automatic Search for a better driver (Recommended)” and click the “Next” button to continue.

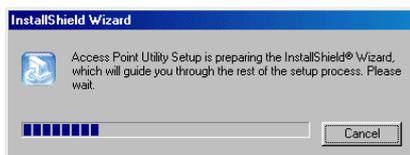
3-2 GL2411AP-0A Access Point DFU Utility

3-2-1 DFU (USB Configuration Utility) Utility Installation

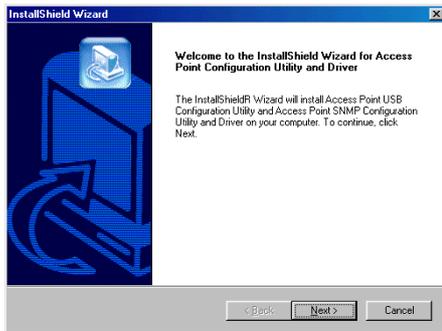
1. Please insert the driver and utility CD for the installation and click the “Access Point” to



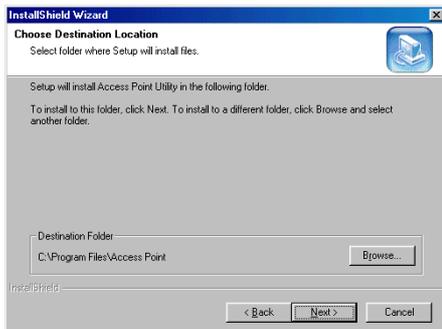
2. The Access Point will start to prepare the InstallShield Wizard for the setup process.



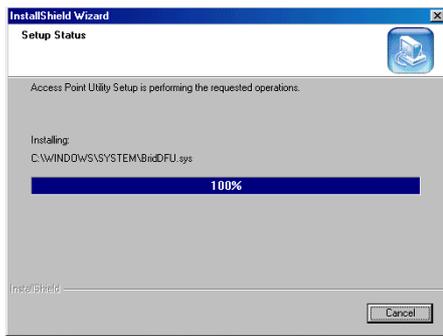
3. A message will prompt to inform you the status. Please click “Next” for further processing.



4. Please browse the file shown in the dialog box, then click “Next”.



5. The PC will start to install the USB Utility and show the installation complete status.



6. The configuration utility will be shown installed. Please click “Yes” to restart your PC and then click the “Finish”.



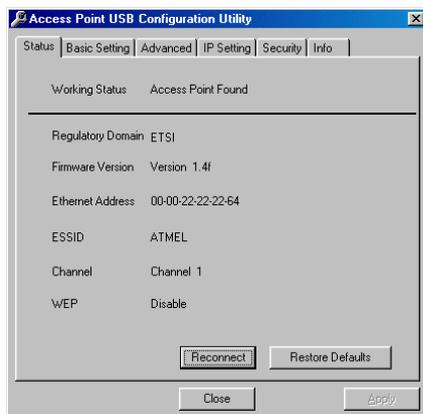
3-2-2 DFU (USB Configuration Utility) Utility Configuration

Click “Start” then, “Program” folder, you will find icon, please press icon “DFU” to execute program.



Click “Basic Setting” “Advanced” “IP Setting” “WEP” “About” Tab to change other function.

1. The “Status” Tab, it will show the Wireless Network Access Point current status.



Working Status: This will display the connection situation to notify any connection problem.

Regulation Domain: It will display the current domain operated with FCC from 1 to 11 channels.

Firmware Version: It will display the current firmware version of this Access Point.

Ethernet Address: This will display the MAC ID address of the Access Point.

ESSID: This will display the name that is shared with all the stations in your wireless network system.

Channel: This will display the current working channel in which the AP and the with it associated stations work.

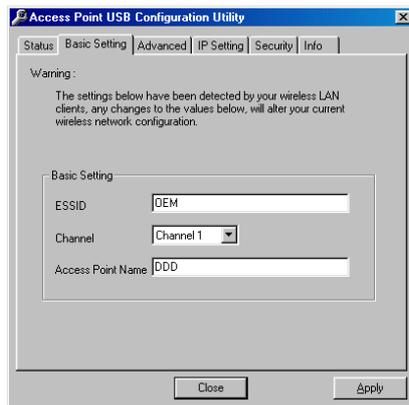
WEP: This will display the status of encryption protocol. It will read “Disabled”, if the WEP encryption protocol is not enabled. When it is in use, it will show “Enabled”.

Reconnect: This button is to be clicked for reconnect AP, if the connection is broken. The parameter date will be re-read and retrieved.

Restore Default: To click this button the default values will be restored and any setting you may have changed thru the DFU utility will be lost.

If you had changed any configuration, please click “**Apply**” Button.

2. The “Basic Setting” Tab, you can change ESSID, Channel.

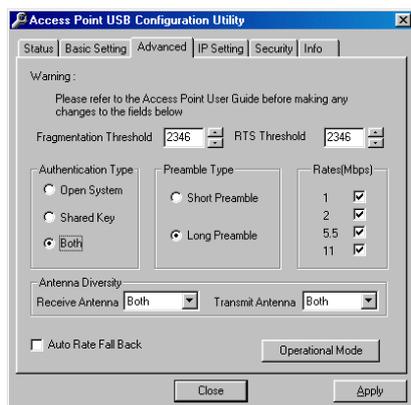


ESSID: ESS stands for “Extended Service Set”. The ESS ID is the name shared among all points in a wireless network system. The ESSID must be identical for all points in the system and must not exceed over 30 characters. After changing, please click “Apply” button for setup. Default will be “OEM”.

Channel: The value of channel can be selected from channel 1 to 11 for the FCC domain and between channels 1 to 13 for ETSI domain.

Access Point Name: you may assign any name for this Access Point, just easy to memory and unique. If you had changed any configuration, please click “**Apply**” Button.

7. The “Advanced” Tab, you can change “Authentication Type” “Preamble Type” and “Basic Rate”.



Fragmentation Threshold: The value indicates how much of the network resources devoted to recovering packet errors. The value should remain at its default setting of 2432 bytes. If you have decreased this value and experience high packet error rates, you can increase it again, but will likely decrease overall network performance.

RTS Threshold: The value should remain on its default setting 2432 bytes. If you encounter any data flow, only minor modifications are recommended.

Authentication Type: It can be selected for “Open System”, “Shared Key” or “Both” for the indication of an authentication algorithm. “Shared Key” is to be selected while the WEP for PC card and Access Point are both enabled and setup with the same passphrase key. And “Open System” is for disabled WEP in Wireless Network system.

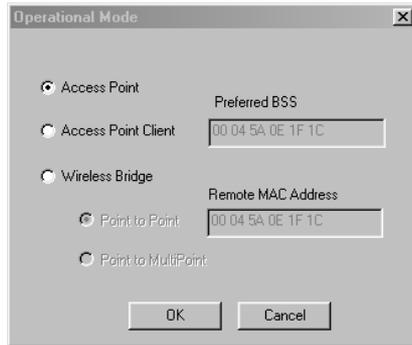
Please note that the Authentication Type setting for the Access Point and wireless Client side should be the same.

Preamble Type: There is the “Long” or “Short” selection to ensure that systems receiving the information correctly interpret when the data transmission starts. To select “long” Preamble may be used to minimize overhead and “Long” to maximize the network data throughput. The default value will be set for “Long”.

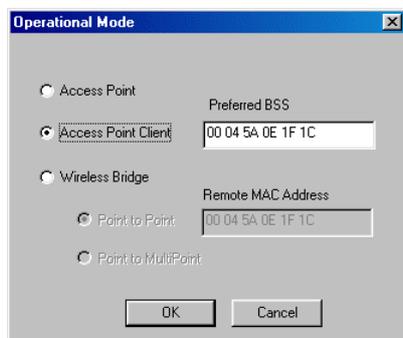
Basic Rate: The basic transfer rate is to set based on the speed of the wireless network system. For slower network system is to be selected 1-2 Mbps and faster network 1-2-5.5-11 Mbps.

Antenna Diversity: This option is defined that either one or both antennas are used for the transmission or receiving. The default value is for “Both”, it means the two antennas will work together by transmission and receiving which can especially back up each other by receiving no matter where the wireless signals come from.

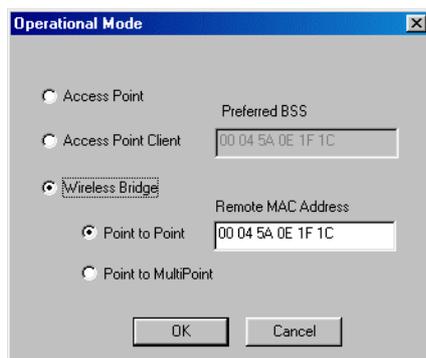
Operational Mode: In this option the user can have the chance to let the two access points communicate with each other.



Access Point: This mode provides access for wireless stations to wired LANs and from wired LANs to wireless stations. Furthermore, wireless station within the range of the Access Point device may communicate with each other via the Access Point. In this option the Access Point is as a base station to build up a basic Wireless Local Area Networking.



Access Point Client: In this option, the Access Point can be a base station in a WLAN system, but also as a client station to communicate with other stations in the WLAN system. In this option please type in the "Preferred BSS" for the WLAN network system which it wants to join in.



Wireless Bridge: This mode allows the connection of one or more remote LANs with a central LAN, creating thus an extended single virtual LAN. In this way, any station of the Remote LAN can successfully communicate with any station of the central LAN, as if all of them belonged to the same physical LAN. Wireless station can't associate with wireless bridges. The Access Point conducts the designated traffic to the appropriate wired or wireless station.

Point to Point: This mode allows only two individual LANs to be connected through two Wireless

Bridges, creating thus the optimum connection between the two LANs. Packets from any station of the LAN to a station of the same LAN never cross to the other LAN.

For operating this function, the **Remote MAC Address** must be setup. The user has to type the MAC address of another Access Point in this column, with which his Access Point will connect.

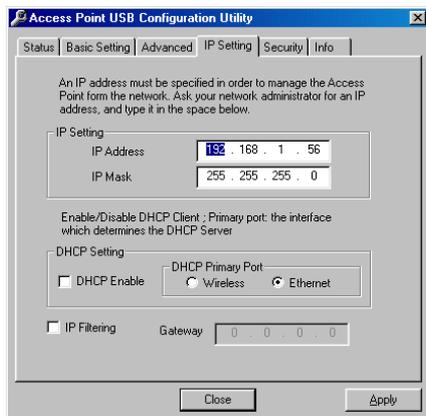
Point to Multipoint:

This function allow one Access Point to communicate with more than one Access Points.

Auto Rate Fall Back setting allows you to have flexible automatic data rate adjustment according to the connection situation.

If you had changed any configuration, please click “**Apply**” Button.

8. The “**IP Setting**” Tab, you can change “IP address” and “IP mask.



IP Address : The IP address of Wireless Network should be different as the network IP addresses.

IP Mask: The value should be same as the Subnet Mask address of wireless Network IP address.

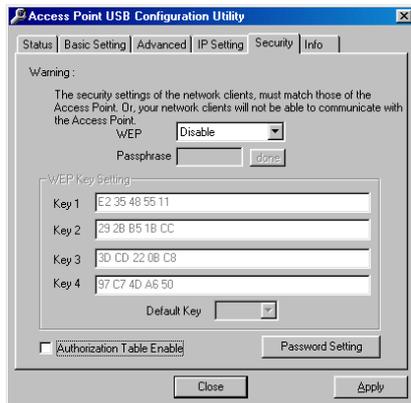
DHCP Setting: If DHCP Client is enabled, the IP Address Field displays the IP Address that was dynamically assigned to the Access Point by the network DHCP server. Select the **Primary Port** which is the interface that determines the DHCP server from **Ethernet** Port or **Wireless** Port and press “OK”. If the network server failed to give an IP Address to the Access Point, then the Access Point IP Address is the default one.

IP Filtering: Enable/Disable the possibility to allow only IP Protocol packets to pass through the WLAN and any other protocol packets filtered out.

Gateway: The Gateway IP Address of Network can be shown in this column.

If you had changed any configuration, please click “**Apply**” Button.

9. The “**WEP**” Tab, Wired Equivalent Privacy is a data privacy security mechanism based on a 40 bit shared key algorithm.

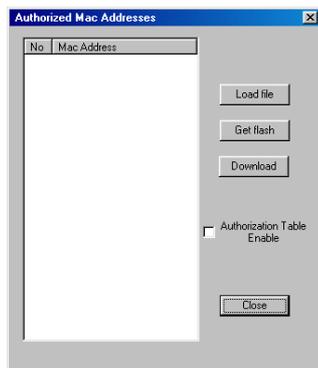


WEP(ON/OFF): With “Disabled” the WEP function will be not active. If you wish to utilize the WEP function, please select “Enabled”.

Passphrase: To generate the key, if the WEP is enabled. This is the code used while a wireless point is to log on to the network thru the WEP encryption function. All points in the Wireless Network system have to have the same key shared which is set with a maximum of 32 alphanumeric characters.

WEP Key Setting: This setting key is to configure the WEP encryption in the wireless network system. To generate the key, please insert the same PassPhrase in the field and click the “Done” to create the encryption key which must be same as the every points on the Wireless Network system. Then Click the “Apply” to store the setting keys.

Authorized Mac: For Security reason the Access Point has the ability to associate with authorized MAC Addresses stations, if the Authorization Table option is enabled. Only the authorized MAC Addresses in this table can communicate with this Access Point. Thus, under the Authorized MAC Address option you many press the following botton :



The **Load file** button is to load a file with the MAC Addresses that can be associated with the Access Point. The user can type in the MAC Addresses which are permitted to access into this WLAN network.

The **Download** button is to download the Authorized MAC Address to the Access Point.

The **Get Flash** button is to get the list of the Authorized MAC Addresses from the Access Point.

1. Please Create a text file (e.g. MAC.txt) using Notepad or some other text editor files.
2. Enter the 10 digit MAC address of the wireless clients which are authorized to be connection with this Access Point.

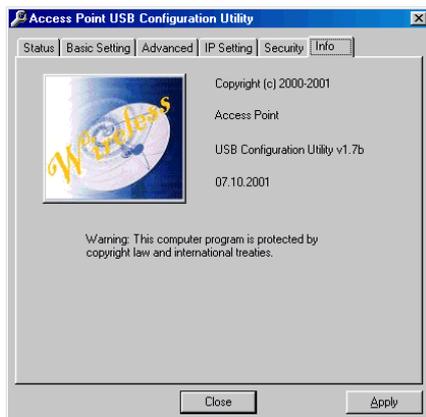
3. Save the File and also make sure the path to this saving file.
4. Click the **“Load file”** button. A Screen will ask you to browse the file (MAC.txt). Once you have loaded the file, you can highlight it and click open. Then all the MACs which you saved in the file (MAC.txt) will be shown on the screen.
5. Click the **“Download”** button to save all the MAC addresses into the Authorized MAC table.
6. After the download is successful, please click **“Close”** button and then the **“Apply”** button in the WEP tab.
7. If you decide to entry or delete the authorized MAC addresses, please just repeat the step from 4-6.

Password Setting: For the security reason the user can setup the Password for any log into his WLAN system to be connected with the Access Point. You can select for “Read/Write” or “Read Only”. With the authority for “Read/Write” the users can setup or modify the password as they want.



If you had changed any configuration, please click **“Apply”** Button.

7. The **“About”** Tab, it is the trademark and USB configuration utility version.



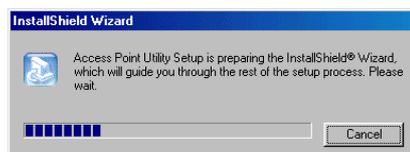
3-3 GL2411AP-0A Access Point SNMP Manager Utility

3-3-1 SNMP Manager Utility Installation

1. Please insert the driver and utility CD for the installation and click the “Access Point” to



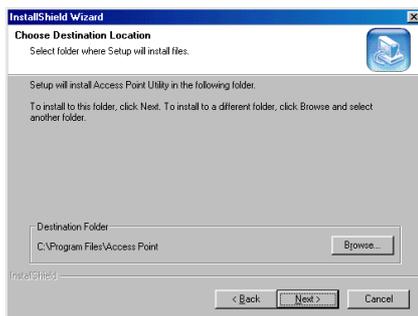
2. The Access Point will start to prepare the InstallShield Wizard for the setup process.



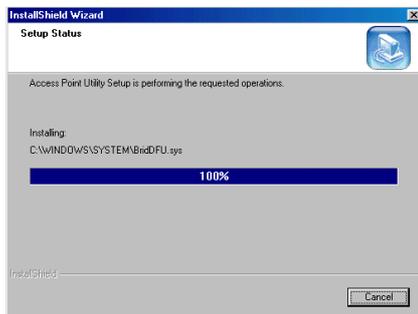
3. A message will prompt to inform you the status. Please click “Next” for further processing.



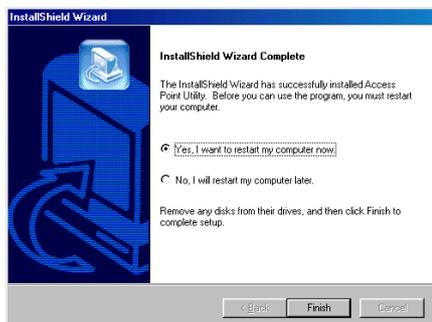
4. Please browse the file shown in the dialog box, then click “Next”.



5. The PC will start to install the USB Utility and show the installation complete status.



6. The configuration utility will be shown installed. Please click “Yes” to restart your PC and then click the “Finish”.

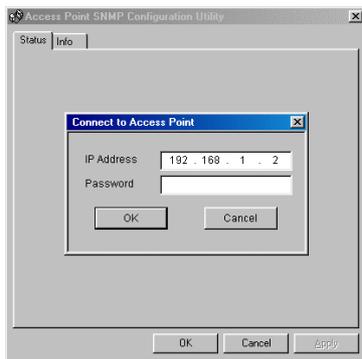


3-3-2 SNMP Manager Utility Configuration

1. Click “Start” then, “Program” folder, you will find icon, please press icon “SNMP Configuration Utility:
To execute the program.

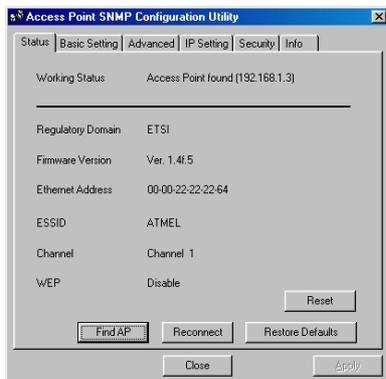


2. Please key in “IP Address” for your AP. (Default IP: 192.168.1.250) and type the password, if you have any password setting and then click “OK”.



Click “Status” “Basic Setting” “Advanced” “IP Setting” “WEP” “About” Tab to change other function.

2. The “Status” Tab, this will display the current wireless connecting status.



Working Status: This will display the connection situation to notify any connection problem.

Regulation Domain: It will display the current domain operated with FCC from 1 to 11 channels.

Firmware Version: It will display the current firmware version of this Access Point.

Ethernet Address: This will display the MAC ID address of the Access Point.

ESSID: This will display the name that is shared with all the stations in your wireless network system.

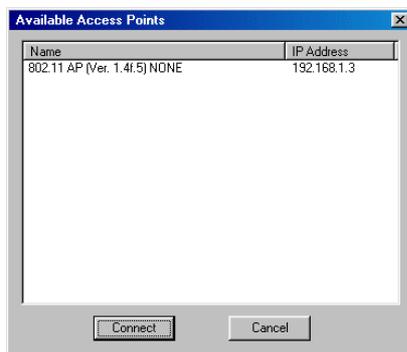
Channel: This will display the current working channel in which the AP and the with it associated stations work.

WEP: This will display the status of encryption protocol. It will read “Disabled”, if the WEP encryption protocol is not enabled. When it is in use, it will show “Enabled”.

Reconnect: This button is to be clicked for reconnect AP, if the connection is broken. The parameter date will be re-read and retrieved.

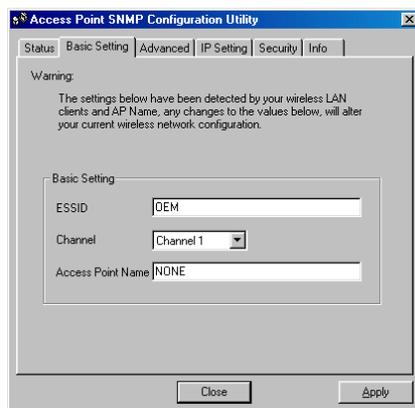
Restore Default: To click this button the default values will be restored and any setting you may have changed thru the DFU utility will be lost.

Find AP : This submenu allows you to find and connect with an Access Point without the necessity of knowing its IP Address. Choose this submenu in order to find the Access Point available for connection. Select one of the available Access Points and press “**Connect**”. Then it will appear indicating the IP Address of the selected Access Point and prompting you to select Authority and to write the appropriate password at the Community field. Please key in the password, then press “**OK**” for enter into this WLAN system.



If you had changed any configuration, please click “**Apply**” Button.

3. The “**Basic Setting**” Tab, you can change ESSID, Channel .

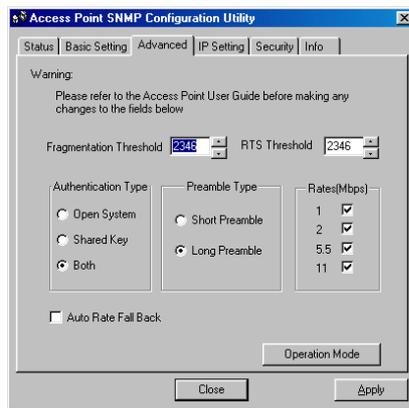


ESSID: ESS stands for “Extended Service Set”. The ESS ID is the name shared among all points in a wireless network system. The ESSID must be identical for all points in the system and must not exceed over 30 characters. After changing, please click “**Apply**” button for setup.

Channel: The value of channel can be selected from channel 1 to 11 for the FCC domain and between channels 1 to 13 for ETSI domain.

Access Point Name: you may assign any name for this Access Point, just easy to memory and unique. If you had changed any configuration, please click “**Apply**” Button.

4. The “Advanced” Tab, you can change “Authentication Type” “Preamble Type” and “Basic Rate”.



Fragmentation Threshold: The value indicates how much of the network resources devoted to recovering packet errors. The value should remain at its default setting of 2432 bytes. If you have decreased this value and experience high packet error rates, you can increase it again, but will likely decrease overall network performance.

RTS Threshold: The value should remain on its default setting 2432 bytes. If you encounter any data flow, only minor modifications are recommended.

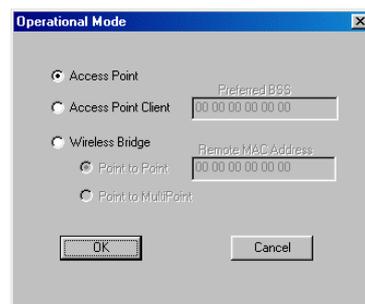
Authentication Type: It can be selected for “Open System”, “Shared Key” or “Both” for the indication of an authentication algorithm. “Shared Key” is to be selected while the WEP for PC card and Access Point are both enabled and setup with the same passphrase key. And “Open System” is for disabled WEP in Wireless Network system.

Preamble Type: There is the “Long” or “Short” selection to ensure that systems receiving the information correctly interpret when the data transmission starts. To select “long” Preamble may be used to minimize overhead and “Long” to maximize the network data throughput. The default value will be set for “Long”.

Basic Rate: The basic transfer rate is to set based on the speed of the wireless network system. For slower network system is to be selected 1-2 Mbps and faster network 1-2-5.5-11 Mbps.

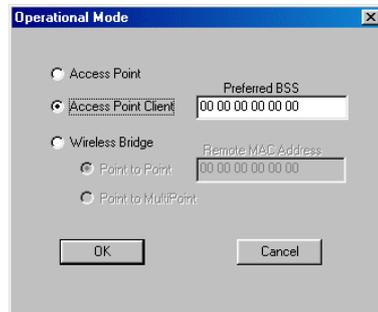
Auto Rate Fall Back setting allows you to have flexible automatic data rate adjustment according to the connection situation.

Operational Mode: In this option the user can have the chance to let the two or more access points communicate with each other.

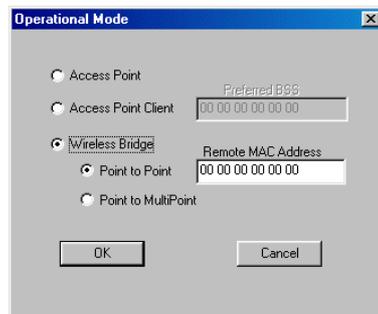


Access Point: This mode provides access for wireless stations to wired LANs and from wired LANs

to wireless stations. Furthermore, wireless station within the range of the Access Point device may communicate with each other via the Access Point. In this option the Access Point is as a base station to build up a basic Wireless Local Area Networking.



Access Point Client: In this option, the Access Point can be a base station in a WLAN system, but also as a client station to communicate with other stations in the WLAN system.



Wireless Bridge: This mode allows the connection of one or more remote LANs with a central LAN, creating thus an extended single virtual LAN. In this way, any station of the Remote LAN can successfully communicate with any station of the central LAN, as if all of them belonged to the same physical LAN. Wireless station can't associate with wireless bridges. The Access Point conducts the designated traffic to the appropriate wired or wireless station.

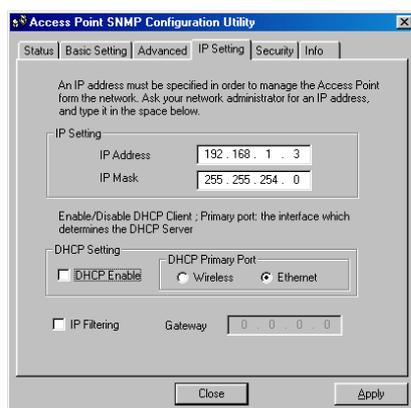
Point to Point: This mode allows only two individual LANs to be connected through two Wireless Bridges, creating thus the optimum connection between the two LANs. Packets from any station of the LAN to a station of the same LAN never cross to the other LAN. For operating this function, the **Remote MAC Address** must be setup. The user has to type the MAC address of another Access Point in this column, with which his Access Point will connect.

Point to Multipoint:

This function allow one Access Point to communicate with more than one Access Points.

If you had changed any configuration, please click “**Apply**” Button.

5. The “**IP Setting**” Tab, you can change “IP address” and “IP mask.”



IP Address : The IP address of Wireless Network should be different as the network IP addresses.

IP Mask: The value should be same as the Subnet Mask address of wireless Network IP address.

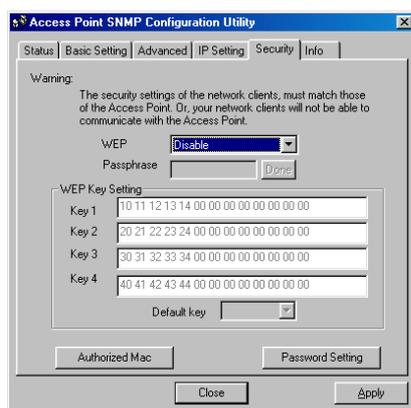
DHCP Setting: If DHCP Client is enabled, the IP Address Field displays the IP Address that was dynamically assigned to the Access Point by the network DHCP server. Select the **Primary Port** which is the interface that determines the DHCP server from **Ethernet** Port or **Wireless** Port and press “OK”. If the network server failed to give an IP Address to the Access Point, then the Access Point IP Address is the default one.

IP Filtering: Enable/Disable the possibility to allow only IP Protocol packets to pass through the WLAN and any other protocol packets filtered out.

Gateway: The Gateway IP Address of Network can be shown in this column.

If you had changed any configuration, please click “**Apply**” Button.

6. The “**WEP**” Tab, Wired Equivalent Privacy is a data privacy security mechanism based on a 40 bit shared key algorithm.



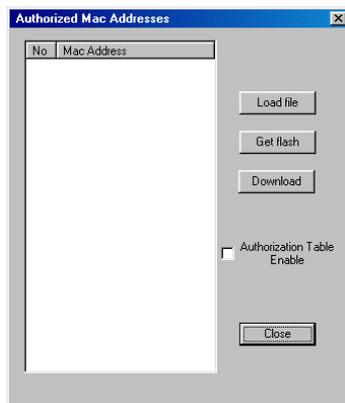
WEP(ON/OFF): With “Disabled” the WEP function will be not active. If you wish to utilize the WEP function, please select “Enabled”.

Passphrase: To generate the key, if the WEP is enabled. This is the code used while a wireless point is to log on to the network thru the WEP encryption function. All points in the Wireless Network system have to have the same key shared which is set with a maximum of 32 alphanumeric characters.

WEP Key Setting: This setting key is to configure the WEP encryption in the wireless network system. To

generate the key, please insert the same PassPhrase in the field and click the “Done” to create the encryption key which must be same as the every points on the Wireless Network system. Then Click the “Apply” to store the setting keys.

Authorized Mac: For Security reason the Access Point has the ability to associate with authorized MAC Addresses stations, if the Authorization Table option is enabled. Only the authorized MAC Addresses from the wireless stations can associate with this Access Point. Thus, under the Authorized MAC Address option you many press the following bottom :



The **Load file** button is to load a file with the MAC Addresses that can be associated with the Access Point. The user can type in the MAC Addresses which are permitted to access into this WLAN network.

The **Download** button is to download the Authorized MAC Address to the Access Point.

The **Get Flash** button is to get the list of the Authorized MAC Addresses from the Access Point.

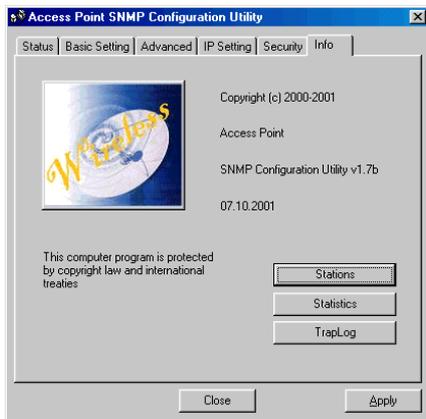
1. Please Create a text file (e.g. MAC.txt) using Notepad or some other text editor files.
2. Enter the 10 digit MAC address of the wireless clients which are authorized to be connection with this Access Point.
3. Save the File and also make sure the path to this saving file.
4. Click the “**Load file**” button. A Screen will ask you to browse the file (MAC.txt). Once you have loaded the file, you can highlight it and click open. Then all the MACs which you saved in the file (MAC.txt) will be shown on the screen.
5. Click the “**Download**” button to save all the MAC addresses into the Authorized MAC table.
6. After the download is successful, please click “**Close**” button and then the “**Apply**” button in the WEP tab. Please do remember to click “Apply” button, if you only click “Close” button, all the MAC data what you have done, will get lost.
7. If you decide to entry or delete the authorized MAC addresses, please just repeat the step from 4-6.

Password Setting: For the security reason the user can setup the Password for any log into his WLAN system to be connected with the Access Point. You can select for “Read/Write” or “Read Only”. With the authority for “Read/Write” the users can setup or modify the password as they want.



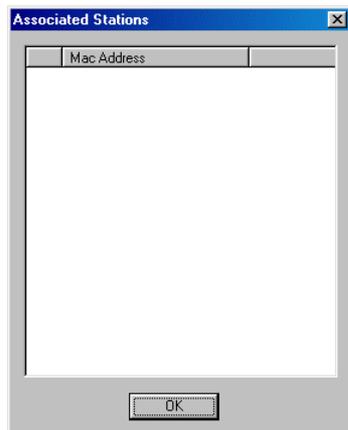
If you had changed any configuration, please click “**Apply**” Button.

7. The “**About**” Tab, it is the trademark and USB configuration utility version.

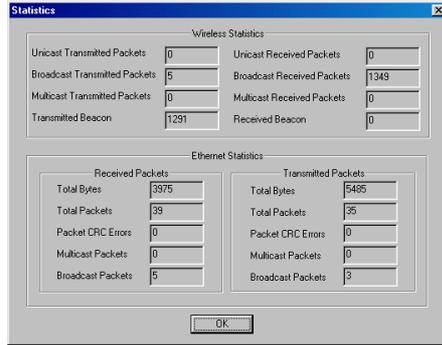


Stations: Thru this option the user can know how many stations are connecting with this Access Point.

The connected stations’ MAC Addresses will be indicated in the list.



Statistics: The submenu reports the statistics concerning the unit’s Wireless / Ethernet Activity.



TrapLog: This option provides information from the trap message. From which the user can see additional information for every Trap Message.

Appendix A Network Configuration

A-1 Network Topology

Ad-Hoc Mode

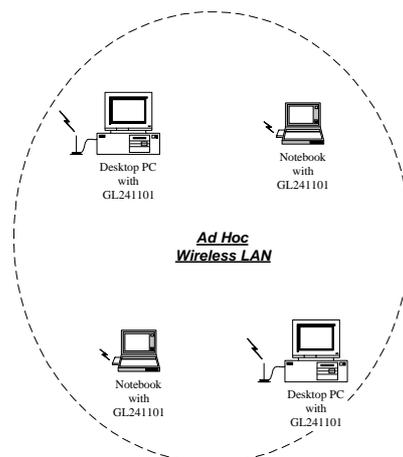


Fig. 1 - Ad-Hoc Wireless LAN

An Ad-Hoc wireless LAN is a group of computers, each equipped with one LAN adapter, connected as an independent wireless LAN. Computers in a specific Ad-Hoc wireless LAN must be configured at the same radio channel and ESSID.

Ad-Hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

Infrastructure

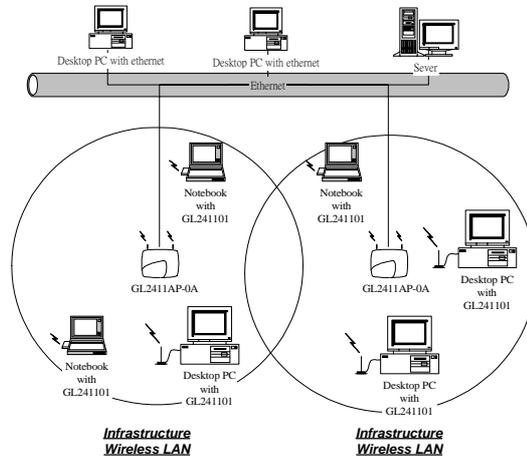


Fig. 2 An Example of Infrastructure Wireless LAN

GL2411AP-0A provides access to a wired LAN for wireless workstations. An integrated wireless and wired LAN is called an Infrastructure configuration. A group of LAN PC users and a GL2411AP-0A Access Point construct a Basic Service Set (BSS). Each LAN PC in the BSS can talk to any computer in the wired LAN infrastructure via the GL2411AP-0A Access Point.

Infrastructure configuration not only extends the accessibility of a LAN PC to the wired LAN, but also doubles the effective wireless transmission range for 2 LAN PCs. Since GL2411AP-0A is able to forward data within its BSS, the effective transmission range in an infrastructure LAN is **doubled**.

BSS ID is, in essence, the ID of each independent GL2411AP-0A. All LAN PCs configured without roaming options in the independent BSS must be configured with the BSS ID of the GL2411AP-0A.

Infrastructure is applicable in an enterprise scale for wireless access to central databases, or wireless access for mobile workers.

A-2 Roaming

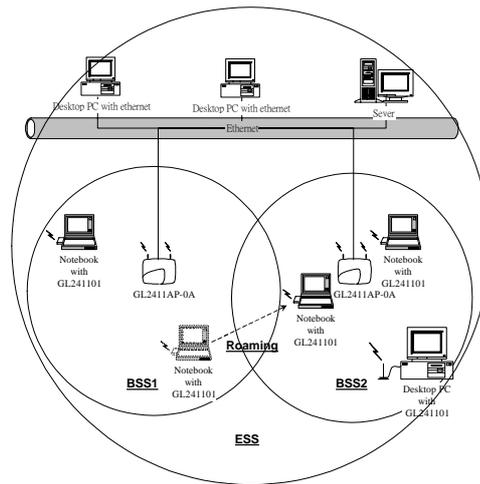


Fig. 3 Roaming in an Extended Service Set (ESS)

An Infrastructure configuration also supports roaming capability for mobile workers. More than one BSS can be configured to be an Extended Service Set (ESS). On account of a continuous connection to the network, users **within an ESS** can roam freely. All LAN PCs and GL2411AP-0As within one ESS must be configured with the same ESS ID and at the same radio channel.

Appendix B Specifications

GL2411AP-0A Access Point	
Wired Interface	Ethernet, 10/100 BaseT
Wireless Interface	IEEE 802.11b standard Wireless LAN
Frequency Band	2.412~2.462 GHz (FCC, Canada) 2.412~2.472 GHz (ETSI) 2.412~2.472 GHz (Japan STD-T66) 2.484 GHz (Japan STD-33) (Customized)
RF Technology	Spread Spectrum Direct Sequence (DSSS)
Channels	FCC : 1-11 channels ETSI : 1-13 channels Japan STD-T66 : 1-13 channels Japan STD-33 : 14 th channel only

Appendix C Glossary

Access Point — An internetworking device that seamlessly connects wired and wireless networks.

Ad-Hoc — An Ad-Hoc wireless LAN is a group of computers each with LAN adapters, connected as an independent wireless LAN.

Authentication Type — Indication of an authentication algorithm which can be supported by this node:

1. Open System : Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any station that requests authentication with this algorithm may become authenticated if dot11AuthenticationType at the recipient station is set to Open System authentication.
2. Shared Key : Shared Key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not.
Open System authentication is the default authentication algorithm.

Backbone — The core infrastructure of a network. The portion of the network transports information from one central location to another central location where it is unloaded onto a local system.

Basic Rate — the data rate of the AP with the value 1,2,5.5 or 11 Mbps for your selection.

Bridge — An internetworking function that incorporates the lowest 2 layers of the OSI network protocol model.

BSS — BSS stands for “Basic Service Set”. It is an Access Point and all the LAN PCs that associated with it.

Channel — The AP and the with it associated stations will work in this channel. You must set the channel by consulting Appendix B from violating the Specifications.

DSSS — direct sequence spread spectrum

ESS — ESS stands for “Extended Service Set”. More than one BSS is configured to become Extended Service Set. LAN mobile users can roam between different BSSs in an ESS.

ESSID — In infrastructure association , the stations will link to the AP with the same ESSID as they have.

Ethernet — A popular local area data communications network, originally developed by Xerox Corp., that accepts transmission from computers and terminals. Ethernet operates on a 10 Mbps baseband transmission rate, using a shielded coaxial cable or over shielded twisted pair telephone wire.

Ethernet IP Address and SubMask — Please setup them to match your network environment.

For example : If your IP address is 192.168.99.127 and your SubMask is 255.255.255.0. Please set the IP address of the AP to 192.168.99.xx which will not have conflict with other IP address

and set the SubMask of the AP to 255.255.255.0.

Ethernet Mac Address — Don't change it, as this will disable the AP.

Infrastructure — An integrated wireless and wired LAN is called an Infrastructure configuration.

PLCP — physical layer convergence protocol

PPDU — PLCP protocol data unit

Preamble Type — During transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. Two different preambles and headers are defined : the mandatory supported long preamble and header which interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999, and an optional short preamble and header. At the receiver, the PLCP preamble and header are processed to aid in demodulation and delivery of the PSDU. The optional short preamble and header is intended for application where maximum throughput is desired and interoperability with legacy and non short preamble capable equipment is not consideration. That is, it is expected to be used only in networks of like equipment that can all handle the optional mode. (IEEE 802.11b standard)

PSDU — PLCP service data unit

Roaming — A LAN mobile user moves around an ESS and enjoys a continuous connection to the Infrastructure network.

RTS Threshold — Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “ Hidden Node Problem”. If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

WEP — Wired Equivalent Privacy (WEP) is an encryption scheme used to protect wireless data communication.

To enable the icon will prevent other stations without the same WEP key from linking with the AP.