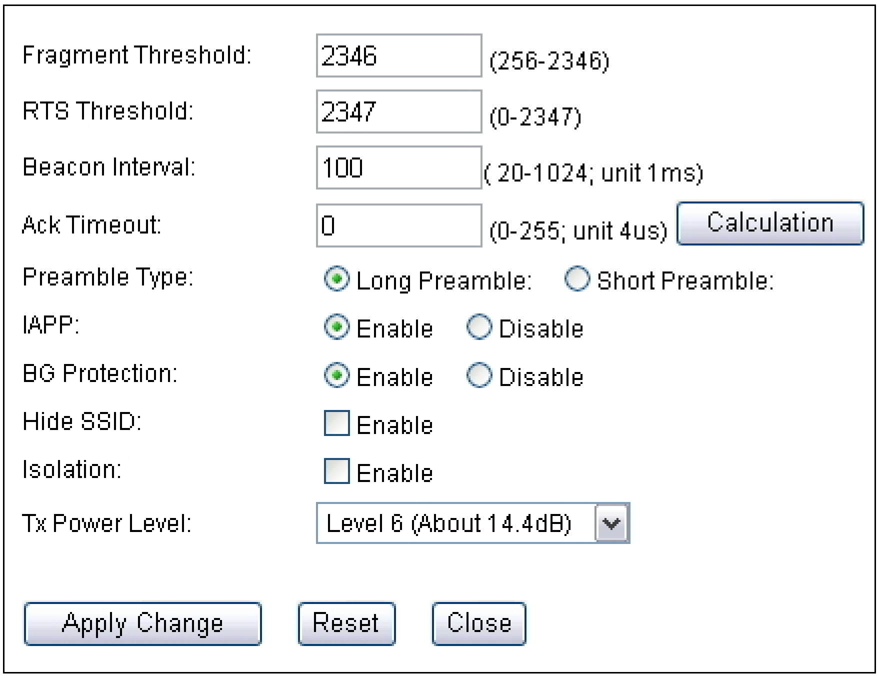
6.3.3 Advance (Wireless Settings)

Operation Mode -> Setup -> Advance



Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024; unit 1ms)

Ack Timeout: 0 (0-255; unit 4us)

Preamble Type: ● Long Preamble: ○ Short Preamble:

IAPP: ● Enable ○ Disable

BG Protection: ● Enable ○ Disable

Hide SSID: □ Enable

Isolation: □ Enable

Tx Power Level: Level 6 (About 14.4dB)

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **Preamble Type**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

- **IAPP:** IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station's security context between current access point (AP) and new AP during handoff period.

- **BG Protection:** The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance..

- **Hide SSID:** Enable Hide SSID will make the AP network's SSID invisible. A device can link with the AP only if correct SSID name is entered.

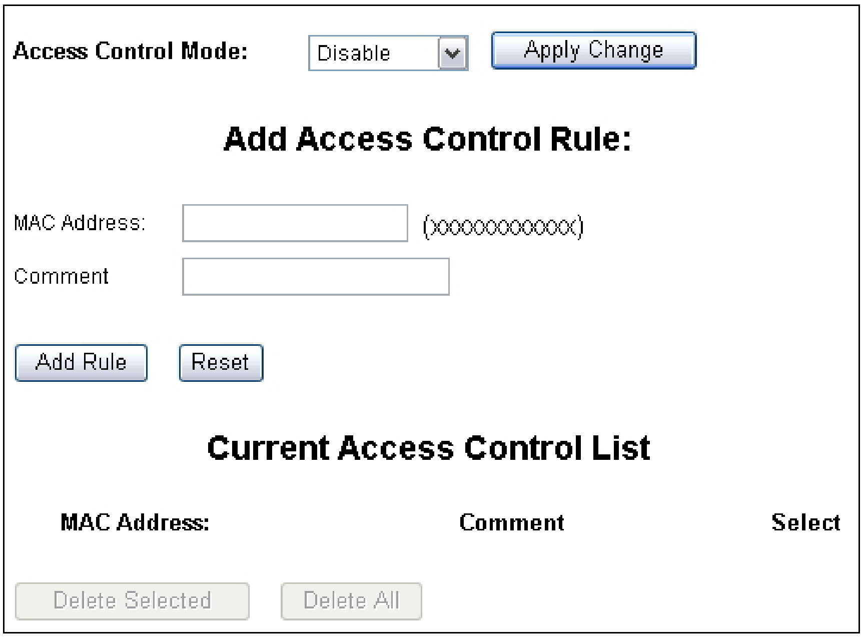
- **Isolation:** Enable Isolation will prevent wireless clients to see each other on the network.

- **TX Power Level:** You can set your TX Output power level here. Please note the maximum allowable TX output power in EU is 20dBm. Please do not exceed your country's legal limit.

6.3.4 Access Control

Operation Mode -> Setup -> Access Control

The G.DUO allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and Gateway modes.



Access Control Mode: Disable

Add Access Control Rule:

MAC Address: (xxxxxxxxxxxx)

Comment

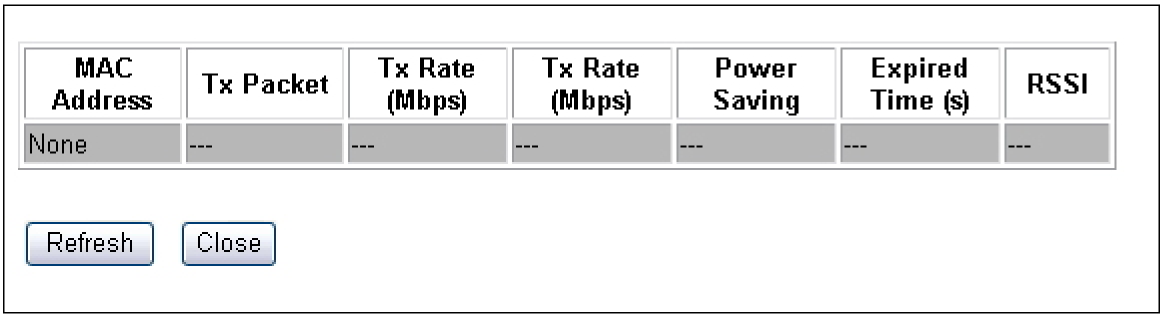
Current Access Control List

MAC Address:	Comment	Select

- **Access Control List**
  - **Disable:** When selected, no MAC address filtering will be performed.
  - **Allow list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.
  - **Deny list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

6.3.5 Associated Clients

Click on this to show the current wireless clients associated to the AP. It will display MAC adderss, Trasmit packet, Tx rate, power saving, expire time, and signal strength.

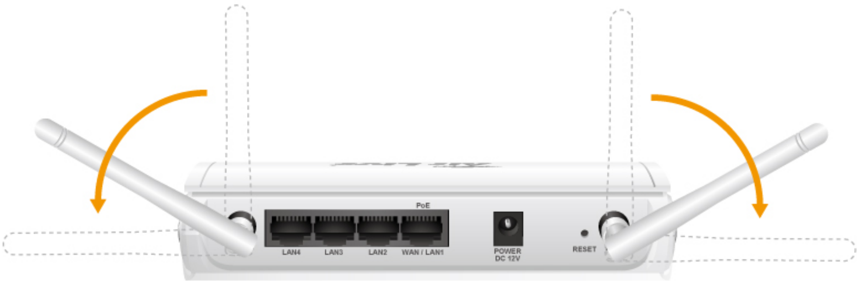


MAC Address	Tx Packet	Tx Rate (Mbps)	Tx Rate (Mbps)	Power Saving	Expired Time (s)	RSSI
None	---	---	---	---	---	---

7 Gateway + AP Mode

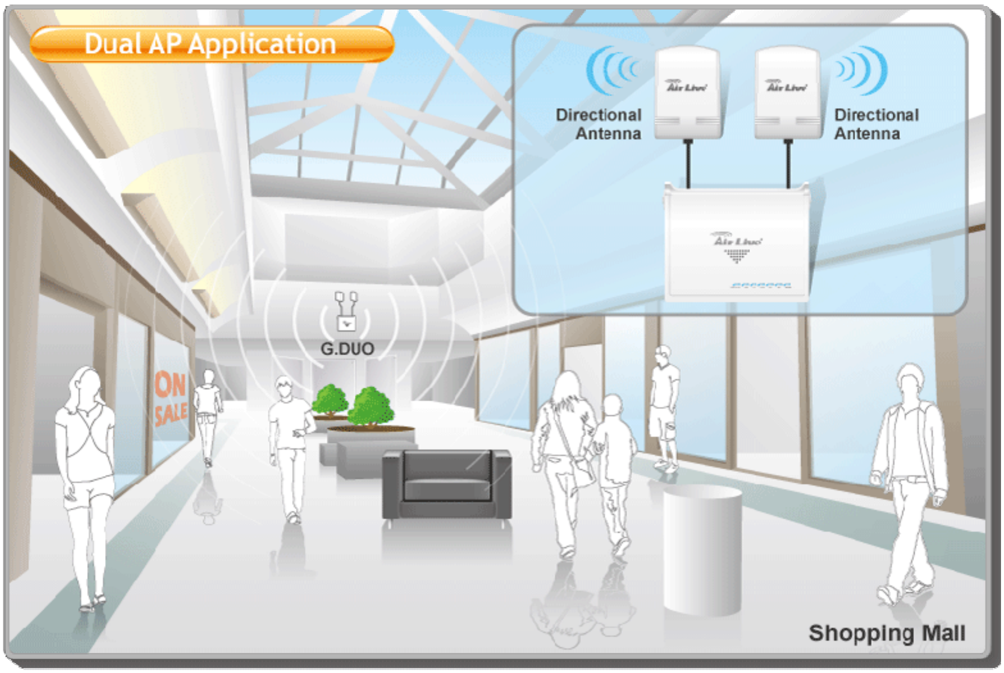
In this chapter, we will explain about the wireless settings for Gateway+AP Mode. Please be sure to read through Chapter 1.4 and Chapter 3's "*Introduction to Web Management"* and *"Initial Configurations"* first.

It is highly recommended that you use 2 directional antennas in this mode to achieve larger coverage and avoid mutual interference. If you need to use the supplied 2dBi Omni antennas, please adjust them according to the diagram below:

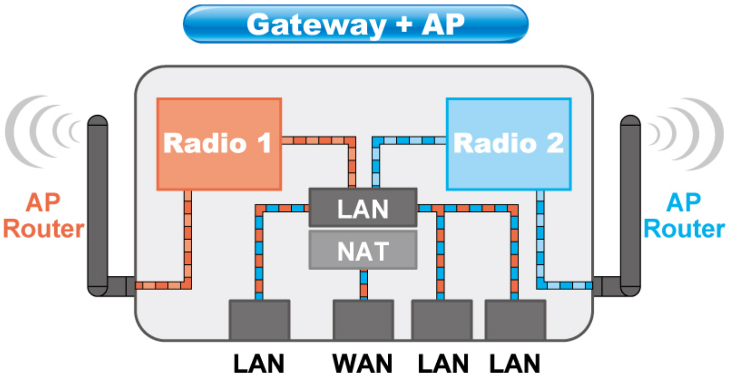


7.1 Application for Gateway +AP Mode

In this mode, both Radio1 and Radio2 are performing as AP Router. This is perfect for shopping mall or office where they can extend the coverage of the wireless IP sharing.



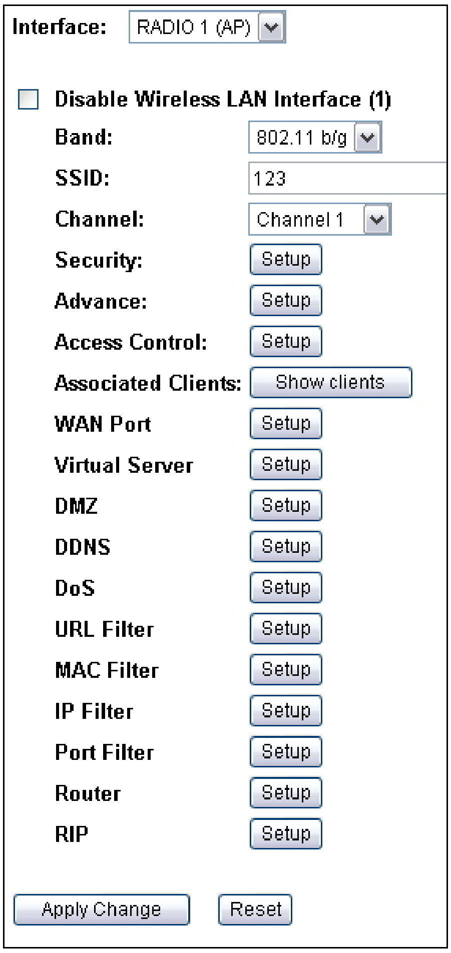
In this mode, the WAN port is in the LAN1. It can be seen as a wireless router with 2 radios.



7.2 Radio1: WISP Router Mode Settings

Although both Radio1 and Radio2 are working as wireless router, the WAN configuration is on the Radio1 side..

When you select “Radio1” as the interface, the following screen will appear.



Interface: RADIO 1 (AP)

□ Disable Wireless LAN Interface (1)

Band:	802.11 b/g
SSID:	123
Channel:	Channel 1

7.2.1 Basic Wireless Settings

- **Band:** You can choose between “802.11g/b”, “802.11g”, or “802.11b”. We recommend to leave the setting at “802.11g/b”.
- **SSID:** The SSID setting of the remote AP. If you are not sure, you can click on “Site Survey” button to scan for AP.
- **Channel**: Wireless Channel used. For EU, it is channel 1~13. For U.S.A., it is channel 1~11.

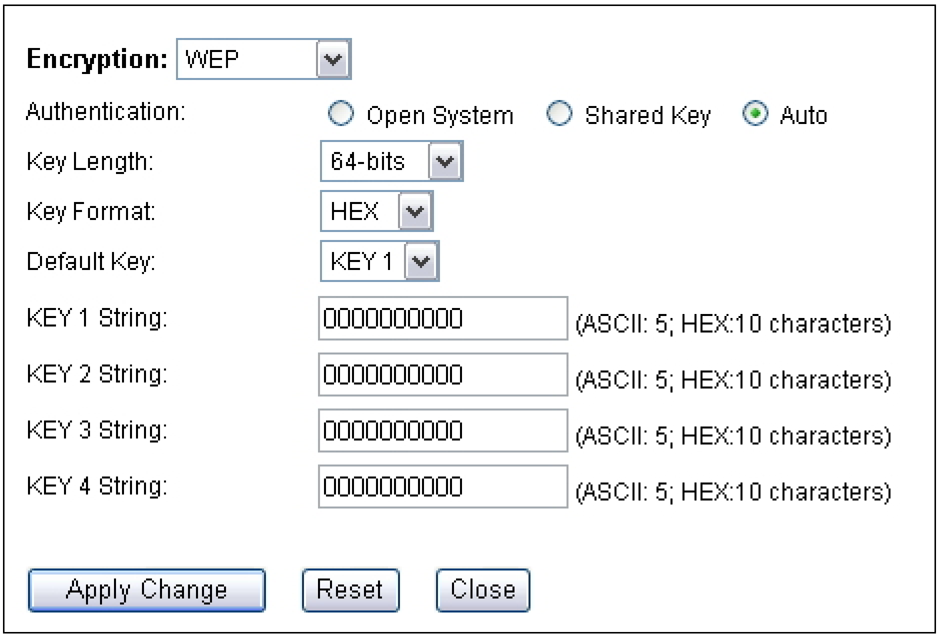
7.2.2 Security Settings

Operation Mode -> Setup -> Security Settings

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The G.DUO features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



Encryption: WEP

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bits

Key Format: HEX

Default Key: KEY 1

KEY 1 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 2 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 3 String: 0000000000 (ASCII: 5; HEX:10 characters)

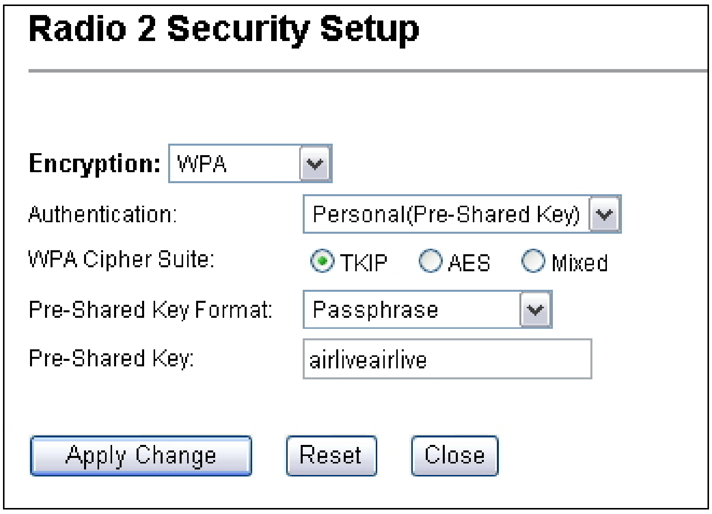
KEY 4 String: 0000000000 (ASCII: 5; HEX:10 characters)

- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

- **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select “Auto”.
- **Key Length:** The G.DUO offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
- **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
- **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, “passw”
- **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
- **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”
- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, “1234567890abcdef1234567890”

WPA-Personal, WPA2-Personal, WPA-Mixed (Pre-Shared Key)

The WPA Personal is also known as “WPA-PSK” encryption. Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.



Radio 2 Security Setup

Encryption: WPA

Authentication: Personal(Pre-Shared Key)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

Pre-Shared Key Format: Passphrase

Pre-Shared Key: airliveairlive

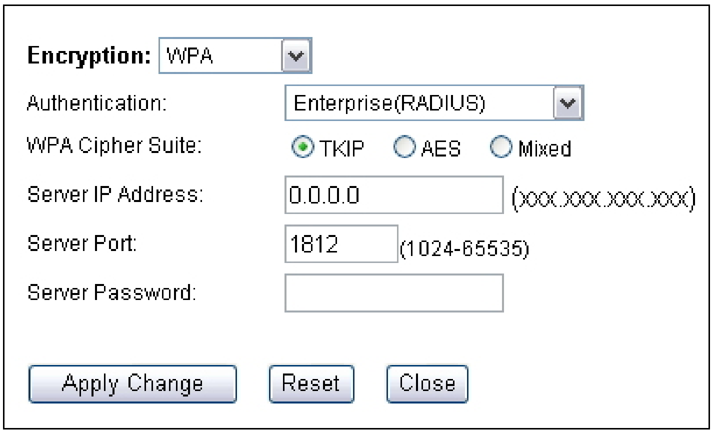
- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While

CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

WPA-Enterprise, WPA2-Enterprise, WPA-Mixed Enterprise (Radius)

Wi-Fi Protected Access (WPA) Enterprise uses Radius Server as the authenticator. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA or WPA2.



Encryption: WPA

Authentication: Enterprise(RADIUS)

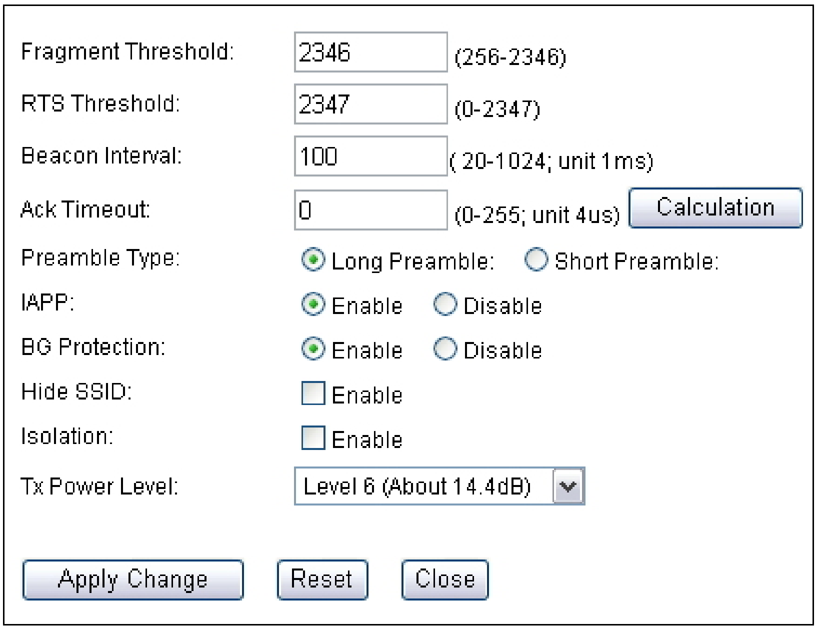
WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

Server IP Address: 0.0.0.0 (xxx.xxx.xxx.xxx)

Server Port: 1812 (1024-65535)

Server Password:

7.2.3 Advance (Wireless Settings)



Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024; unit 1ms)

Ack Timeout: 0 (0-255; unit 4us)

Preamble Type: ● Long Preamble: ○ Short Preamble:

IAPP: ● Enable ○ Disable

BG Protection: ● Enable ○ Disable

Hide SSID: □ Enable

Isolation: □ Enable

Tx Power Level: Level 6 (About 14.4dB)

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **Preamble Type**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

- **IAPP:** IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station’s security context between current access point (AP) and new AP during handoff period.

- **BG Protection:** The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network’s performance..

- **Hide SSID:** Enable Hide SSID will make the AP network’s SSID invisible. A device can link with the AP only if correct SSID name is entered.

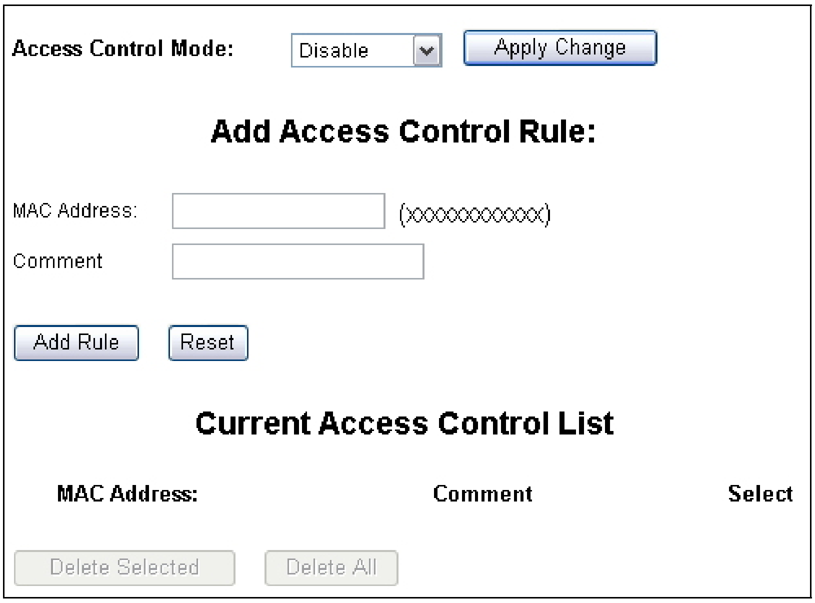
- **Isolation:** Enable Isolation will prevent wireless clients to see each other on the network.

- **TX Power Level:** You can set your TX Output power level here. Please note the maximum allowable TX output power in EU is 20dBm. Please do not exceed your country's legal limit.

7.2.4 Access Control

Operation Mode -> Setup -> Access Control

The G.DUO allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and Gateway modes.



Access Control Mode: Disable

Add Access Control Rule:

MAC Address: (xxxxxxxxxxxx)

Comment

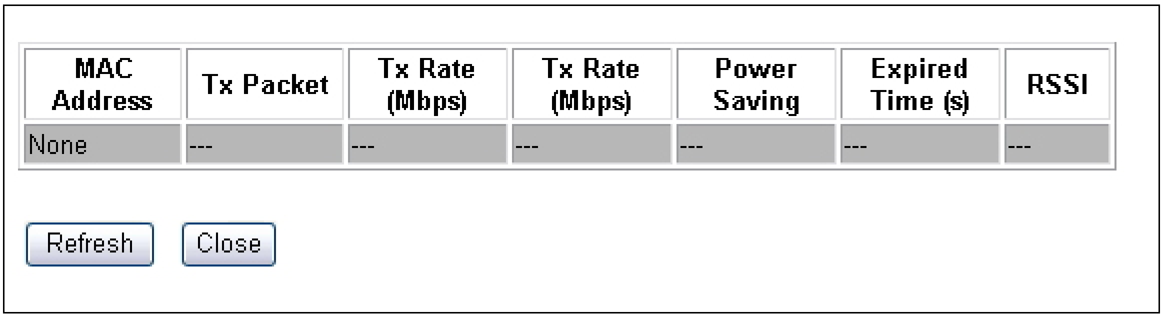
Current Access Control List

MAC Address:	Comment	Select

- **Access Control List**
  - **Disable:** When selected, no MAC address filtering will be performed.
  - **Allow list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.
  - **Deny list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

7.2.5 Associated Clients

Click on this to show the current wireless clients associated to the AP. It will display MAC adderss, Trasmit packet, Tx rate, power saving, expire time, and signal strength.

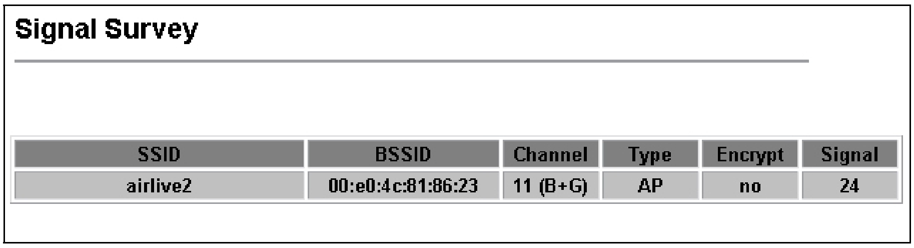


MAC Address	Tx Packet	Tx Rate (Mbps)	Tx Rate (Mbps)	Power Saving	Expired Time (s)	RSSI
None	---	---	---	---	---	---

7.2.6 Signal Survey

Operation Mode -> Setup -> Site Survey -> Signal Survey

The Signal Survey will continuously display the SIGNAL STRENGTH value of the selected SSID for antenna alignment purpose. To use Signal Survey function, please enter the "Site Survey" function first; please refer to the instruction in the above section. Once you select the ESSID and click on the "Signal Survey" button, the following screen will appear.



Signal Survey

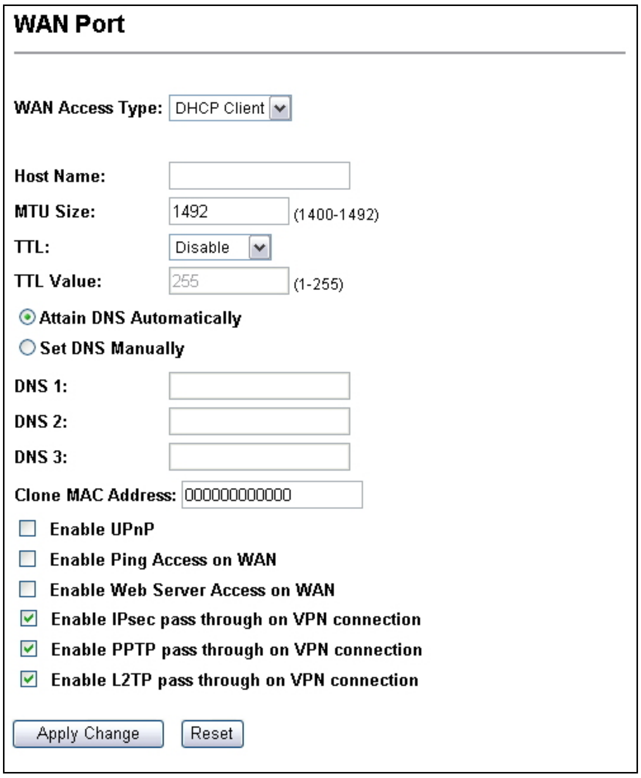
SSID	BSSID	Channel	Type	Encrypt	Signal
airlive2	00:e0:4c:81:86:23	11 (B+G)	AP	no	24

- **BSSID**: This is the remote AP's MAC address.
- **Channel**: The current scanned channel
- **Signal Strength**: This is signal strength number in percentage in 0 to 100 scale. The higher the number, the better signal.

7.2.7 WAN Port

Operation Mode -> Setup -> WAN Port

The G.DUO support different authentication and IP assignment standards for the WAN port. It includes fixed IP, DHCP, PPPoE, PPTP, L2TP, and Big Pond protocols. Please consult with your ISP about what authentication type is used for the WAN port connection.



WAN Port

WAN Access Type: DHCP Client

Host Name:

MTU Size: 1492 (1400-1492)

TTL: Disable

TTL Value: 255 (1-255)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable UPnP

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

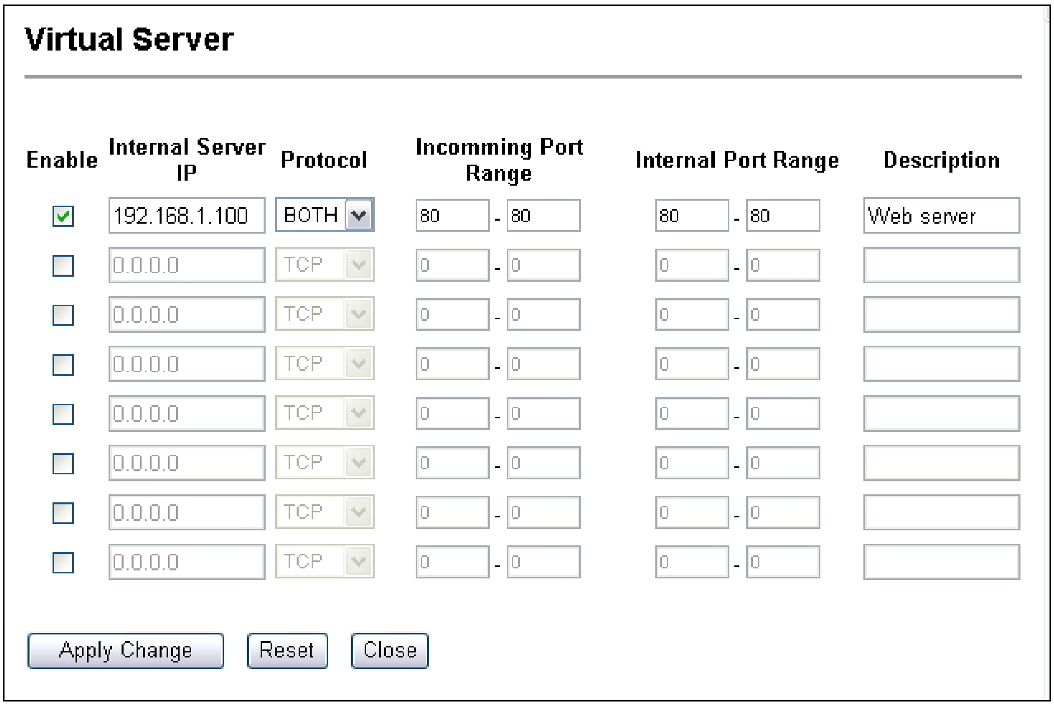
☑ Enable L2TP pass through on VPN connection

- **Clone MAC Address**: In this place, you can assign a MAC address for the WAN port. In case of WISP mode, it is Radio1's MAC address. For Gatway mode, it is the WAN/LAN1 MAC address.
- **Enable UPnP:** Check this field will enable Universal Plug n Play protocol
- **Enable Web Server Access on WAN:** Check this field will enable remote management from WAN side.

7.2.8 Virtual Server Settings

Virtual server allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user. Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.

If you want to allow your web server, ftp server, or email server to be accessible from Internet, you would need to open specific port on the virtual server to your local IP address.



Virtual Server

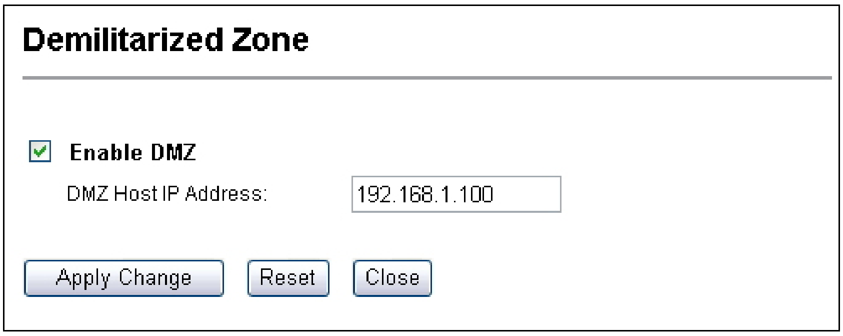
Enable	Internal Server IP	Protocol	Incomming Port Range	Internal Port Range	Description
☑	192.168.1.100	BOTH	80 - 80	80 - 80	Web server
□	0.0.0.0	TCP	0 - 0	0 - 0	
□	0.0.0.0	TCP	0 - 0	0 - 0	
□	0.0.0.0	TCP	0 - 0	0 - 0	
□	0.0.0.0	TCP	0 - 0	0 - 0	
□	0.0.0.0	TCP	0 - 0	0 - 0	
□	0.0.0.0	TCP	0 - 0	0 - 0	
□	0.0.0.0	TCP	0 - 0	0 - 0	

For a list of most frequent used TCP and UDP ports. Please visit http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

7.2.9 DMZ

Advanced Settings >> Multiple DMZ

DMZ opens all TCP/UDP ports to particular IP address on the LAN side. It allows setting up servers behind the G.DUO.



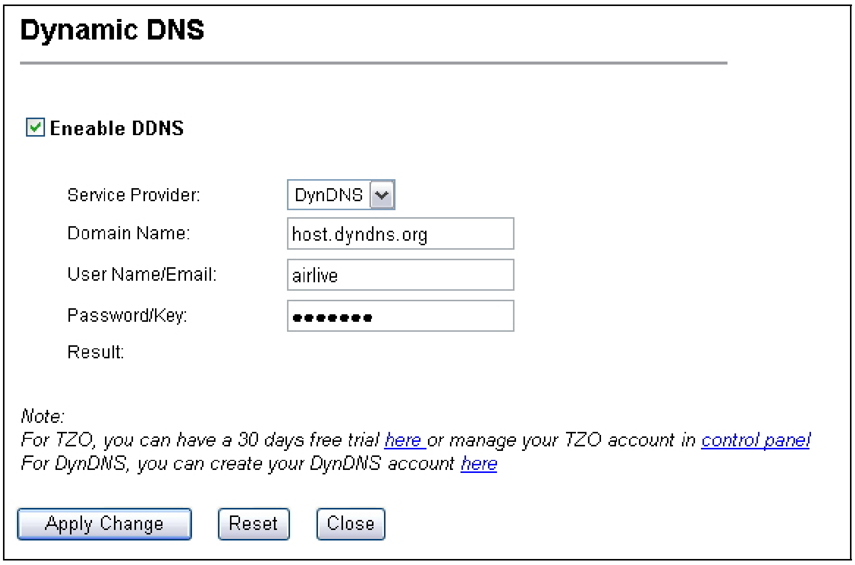
Demilitarized Zone

☑ Enable DMZ

DMZ Host IP Address: 192.168.1.100

7.2.10 DDNS

Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. The G.DUO support “Dyndns” and “TZO” service.



Dynamic DNS

☑ Eneable DDNS

Service Provider: DynDNS
Domain Name: host.dyndns.org
User Name/Email: airlive
Password/Key: ●●●●●●●
Result:

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

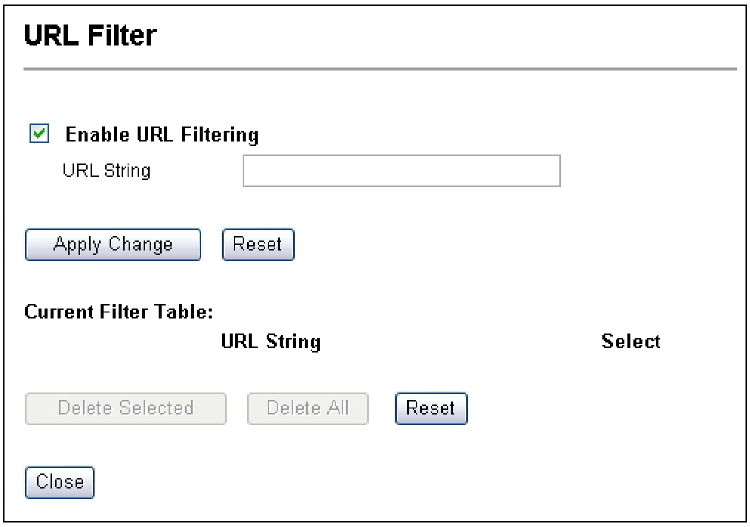
7.2.11 DoS (Denial of Service)

Denial of Service is a type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

The G.DUO provides a list of Firewall grade DoS control that protect your network from hacker attack.

7.2.12 URL Filter

The G.DUO provide URL filter function to stop access to certain website. It is especially useful for parents to stop children from accessing some websites.



URL Filter

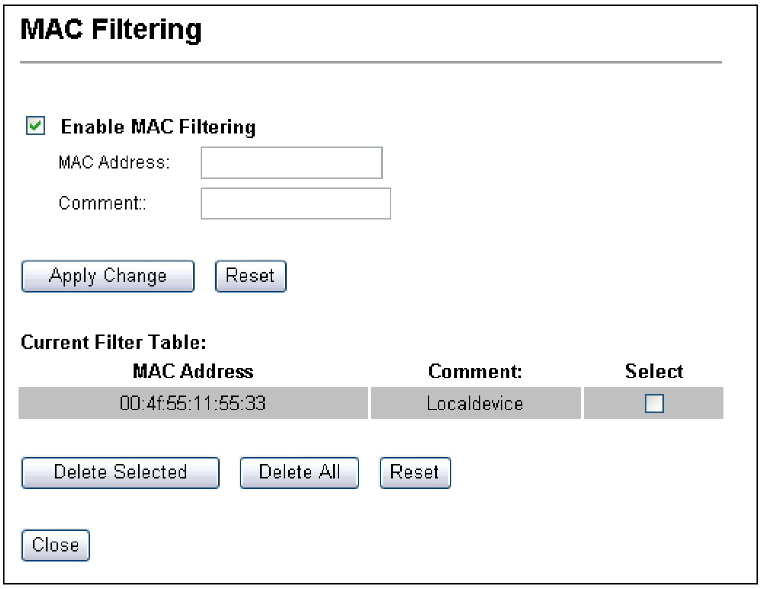
☑ Enable URL Filtering
URL String

Current Filter Table:

URL String	Select

7.2.13 MAC Filter

MAC filter can filter out traffic from certain MAC addresses. It can prevent access to internet from certain station in the local LAN.



MAC Filtering

☑ Enable MAC Filtering

MAC Address:

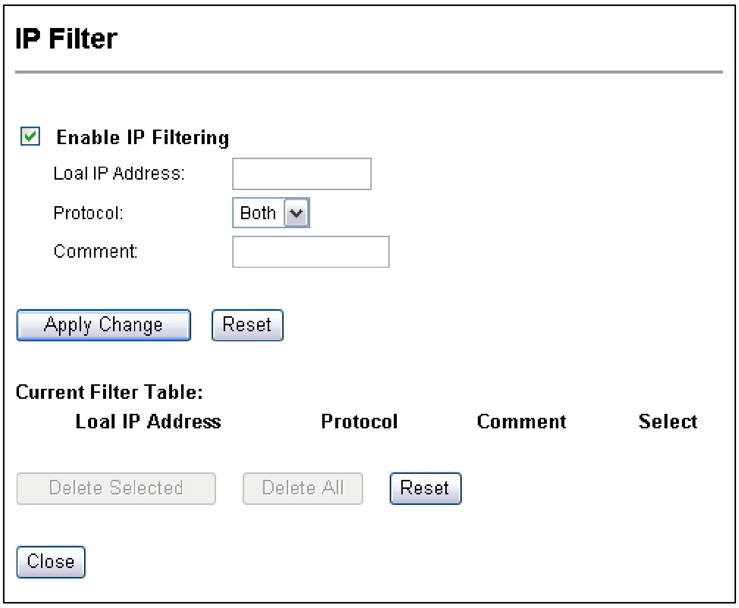
Comment::

Current Filter Table:

MAC Address	Comment:	Select
00:4f:55:11:55:33	Localdevice	□

7.2.14 IP Filter

IP filtering allows you to block certain IP addresses from accessing the network.



IP Filter

☑ Enable IP Filtering

Loal IP Address:

Protocol: Both

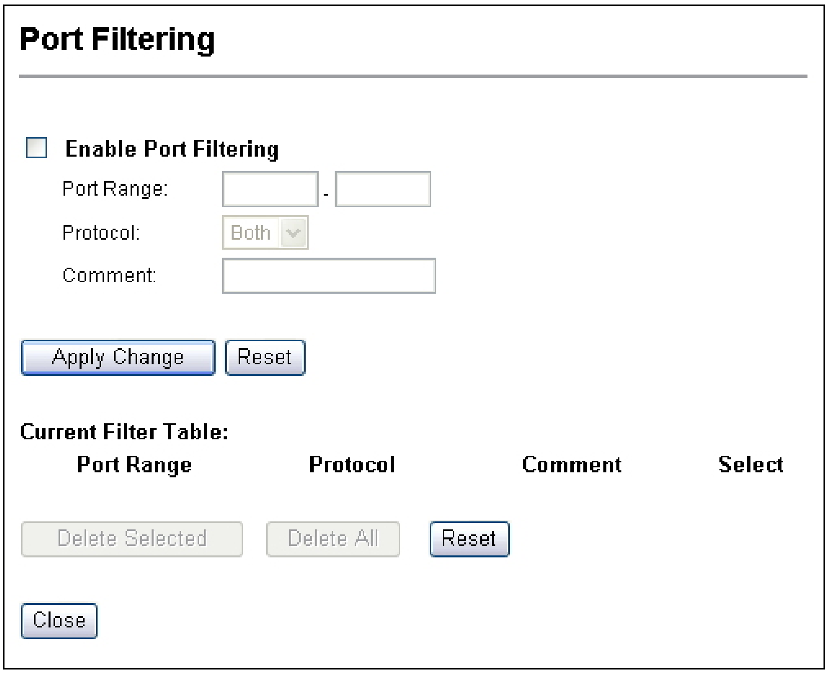
Comment:

Current Filter Table:

Loal IP Address	Protocol	Comment	Select

7.2.15 Port Filter

Port filtering allows you to block certain applications from accessing the network.



Port Filtering

☐ Enable Port Filtering

Port Range: [ ] - [ ]

Protocol: Both

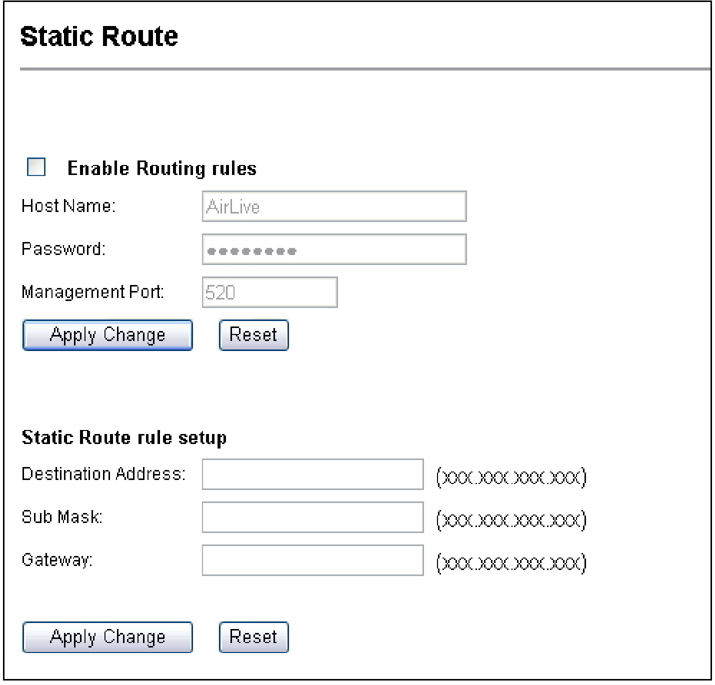
Comment: [ ]

Current Filter Table:

Port Range	Protocol	Comment	Select

7.2.16 Router (Static Route)

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.



Static Route

☐ Enable Routing rules

Host Name: AirLive

Password: ●●●●●●●●●

Management Port: 520

Static Route rule setup

Destination Address: [ ] (xxx.xxx.xxx.xxx)

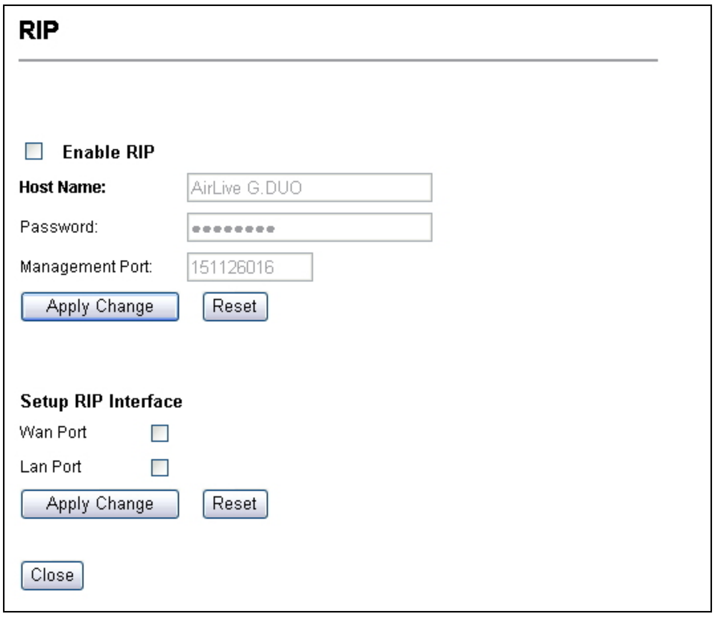
Sub Mask: [ ] (xxx.xxx.xxx.xxx)

Gateway: [ ] (xxx.xxx.xxx.xxx)

7.2.17 RIP (Routing Information Protocol

Operation Mode -> Setup -> Access Control

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks



RIP

☐ Enable RIP

Host Name: AirLive G.DUO

Password: ●●●●●●●●

Management Port: 151126016

Setup RIP Interface

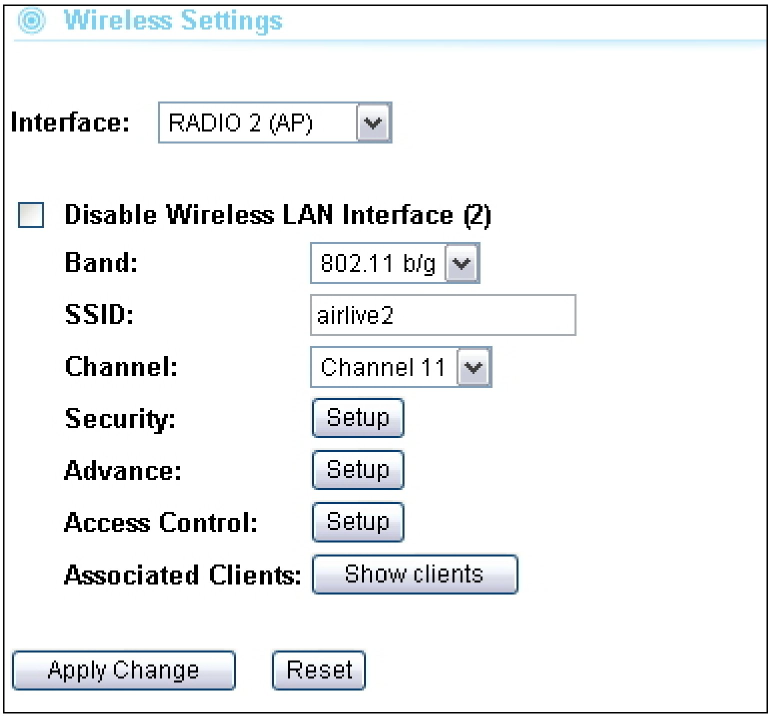
Wan Port ☐

Lan Port ☐

7.3 Radio2: AP Mode Settings

The Radio2 is working in Access Point Mode. The default SSID is “AirLive2”.

When you select “Radio2” as the interface, the following screen will appear:



Wireless Settings

Interface: RADIO 2 (AP)

☐ Disable Wireless LAN Interface (2)

Band: 802.11 b/g

SSID: airlive2

Channel: Channel 11

Security: Setup

Advance: Setup

Access Control: Setup

Associated Clients: Show clients

7.3.1 Basic Wireless Settings

- **Band:** You can choose between “802.11g/b”, “802.11g”, or “802.11b”. We recommend leaving the setting at “802.11g/b”.
- **SSID:** The SSID setting of the remote AP. If you are not sure, you can click on “Site Survey” button to scan for AP.
- **Channel**: Wireless Channel used. For EU, it is channel 1~13. For U.S.A., it is channel 1~11.

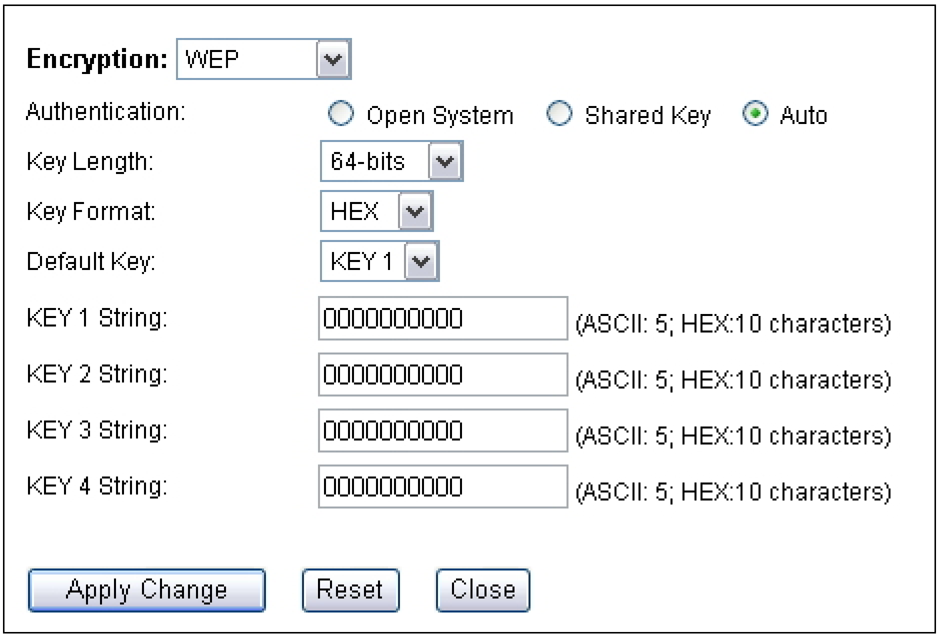
7.3.2 Security Settings

Operation Mode -> Setup -> Security Settings

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The G.DUO features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



Encryption: WEP

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bits

Key Format: HEX

Default Key: KEY 1

KEY 1 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 2 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 3 String: 0000000000 (ASCII: 5; HEX:10 characters)

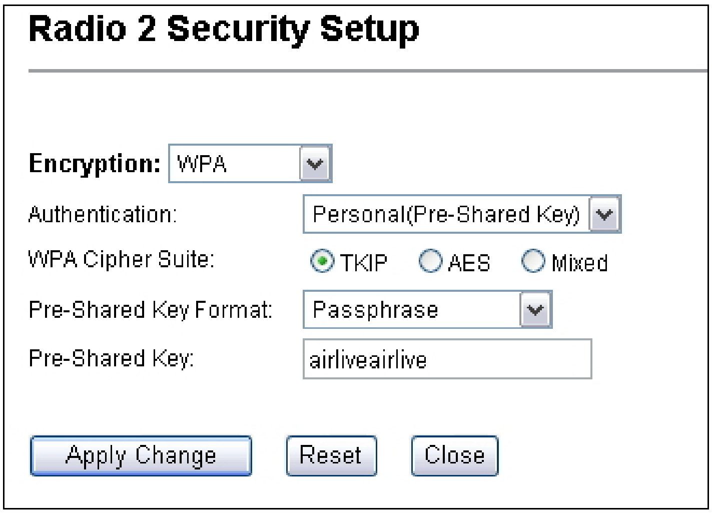
KEY 4 String: 0000000000 (ASCII: 5; HEX:10 characters)

- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

- **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select "Auto".
- **Key Length:** The G.DUO offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
- **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. "airlivepass12"). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
- **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, "passw"
- **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, "12345abcdef"
- **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, "airlivewepkey"
- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, "1234567890abcdef1234567890"

WPA-Personal, WPA2-Personal, WPA-Mixed (Pre-Shared Key)

The WPA Personal is also known as "WPA-PSK" encryption. Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.



Radio 2 Security Setup

Encryption: WPA

Authentication: Personal(Pre-Shared Key)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

Pre-Shared Key Format: Passphrase

Pre-Shared Key: airliveairlive

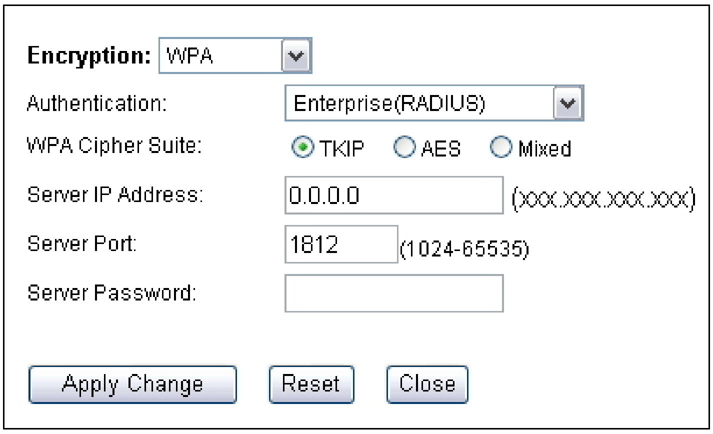
- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While

CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

WPA-Enterprise, WPA2-Enterprise, WPA-Mixed Enterprise (Radius)

Wi-Fi Protected Access (WPA) Enterprise uses Radius Server as the authenticator. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA or WPA2.



Encryption: WPA

Authentication: Enterprise(RADIUS)

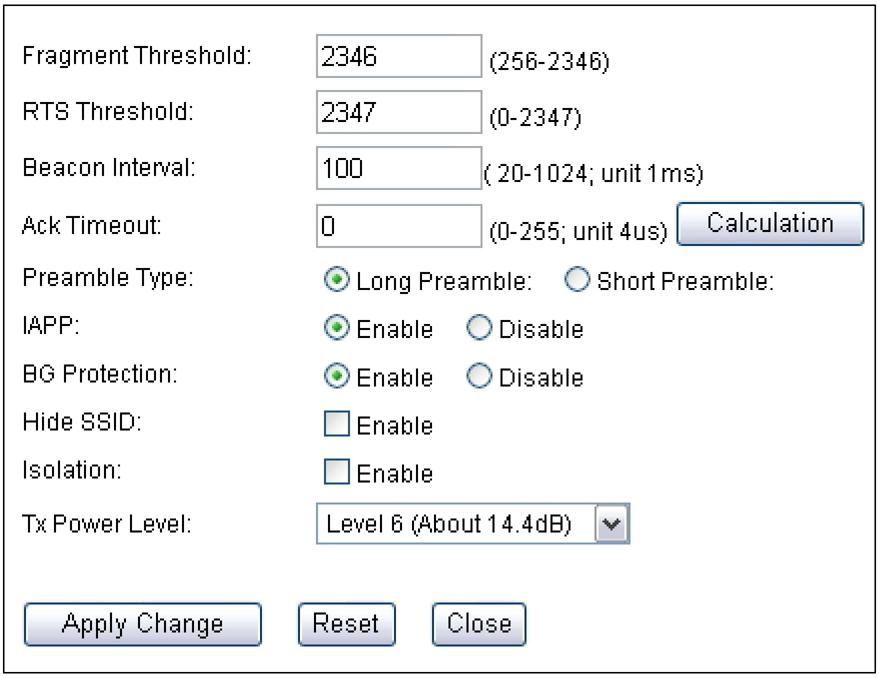
WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

Server IP Address: 0.0.0.0 (xxx.xxx.xxx.xxx)

Server Port: 1812 (1024-65535)

Server Password:

7.3.3 Advance (Wireless Settings)



Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024; unit 1ms)

Ack Timeout: 0 (0-255; unit 4us)

Preamble Type: ● Long Preamble: ○ Short Preamble:

IAPP: ● Enable ○ Disable

BG Protection: ● Enable ○ Disable

Hide SSID: □ Enable

Isolation: □ Enable

Tx Power Level: Level 6 (About 14.4dB)

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **Preamble Type**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

- **IAPP:** IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station’s security context between current access point (AP) and new AP during handoff period.

- **BG Protection:** The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network’s performance..

- **Hide SSID:** Enable Hide SSID will make the AP network’s SSID invisible. A device can link with the AP only if correct SSID name is entered.

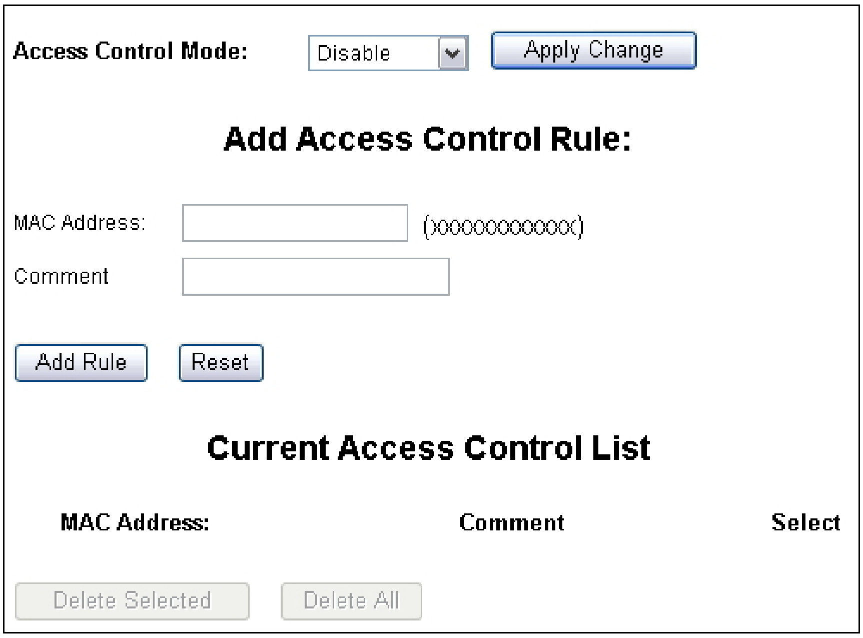
- **Isolation:** Enable Isolation will prevent wireless clients to see each other on the network.

- **TX Power Level:** You can set your TX Output power level here. Please note the maximum allowable TX output power in EU is 20dBm. Please do not exceed your country's legal limit.

7.3.4 Access Control

Operation Mode -> Setup -> Access Control

The G.DUO allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and Gateway modes.



Access Control Mode: Disable

Add Access Control Rule:

MAC Address: (xxxxxxxxxxxx)

Comment

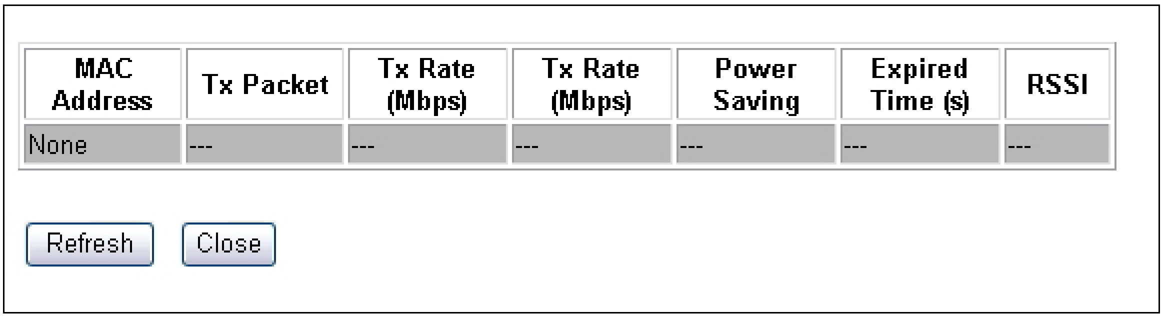
Current Access Control List

MAC Address:	Comment	Select

- **Access Control List**
  - **Disable:** When selected, no MAC address filtering will be performed.
  - **Allow list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.
  - **Deny list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

7.3.5 Associated Clients

Click on this to show the current wireless clients associated to the AP. It will display MAC adderss, Trasmit packet, Tx rate, power saving, expire time, and signal strength.

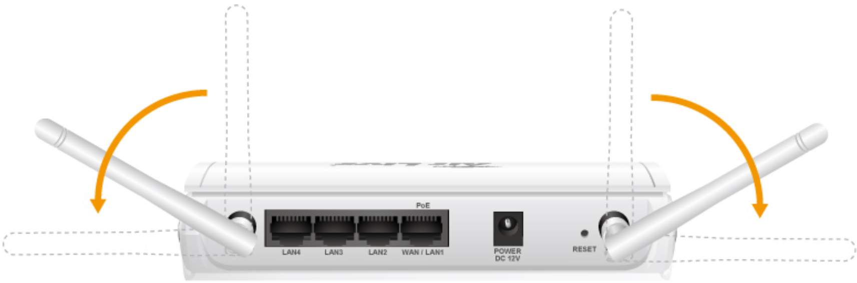


MAC Address	Tx Packet	Tx Rate (Mbps)	Tx Rate (Mbps)	Power Saving	Expired Time (s)	RSSI
None	---	---	---	---	---	---

8 WDS + AP Mode

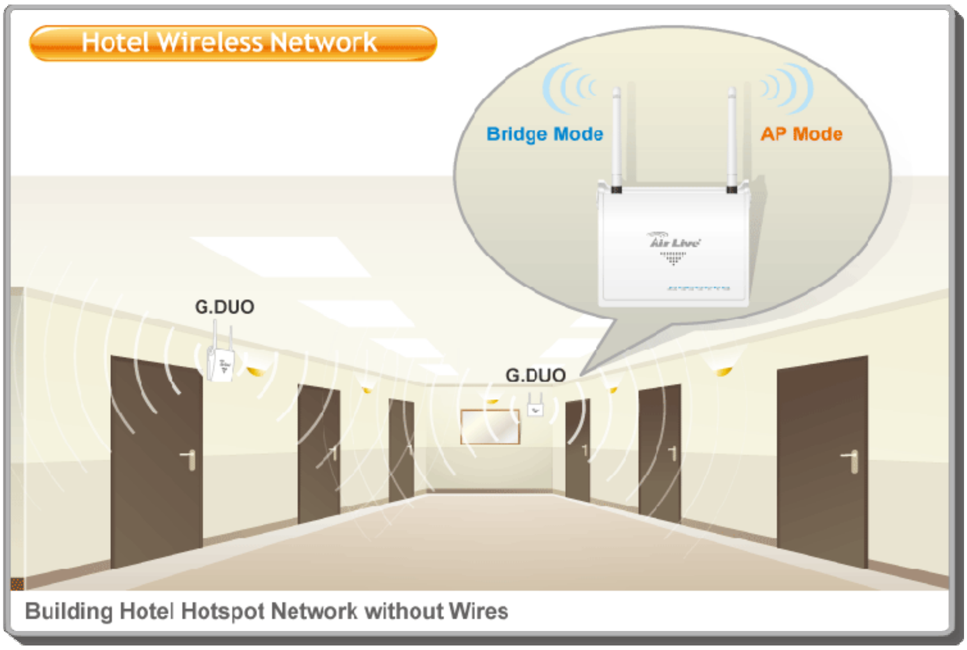
In this chapter, we will explain about the wireless settings for Client + AP Mode. Please be sure to read through Chapter 1.4 and Chapter 3's "*Introduction to Web Management*" and *"Initial Configurations"* first.

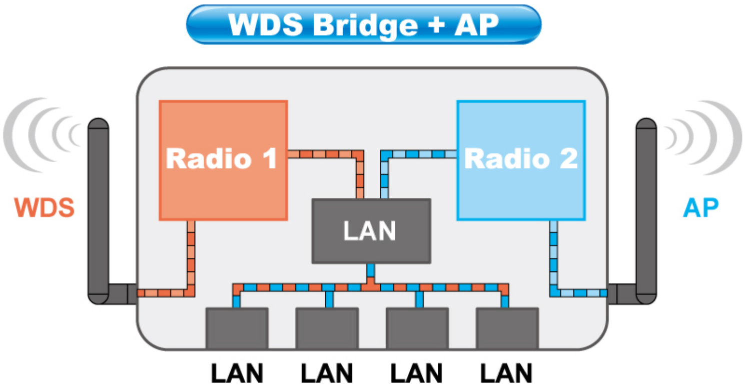
It is highly recommended that you use directional antenna for Radio1 in this mode to achieve larger coverage and avoid mutual interference. If you need to use the supplied 2dBi omni antennas, please adjust them according to the diagram below:



8.1 Application for WDS + AP Mode

In this mode, the Radio1 is working in Bridge mode to connect with another Remote Bridge. Radio2 is performing as an Access Point. The Radio1 can be used to build backbone connection in a hotel hotspot network. Radio2 can be used to provide hotspot service.

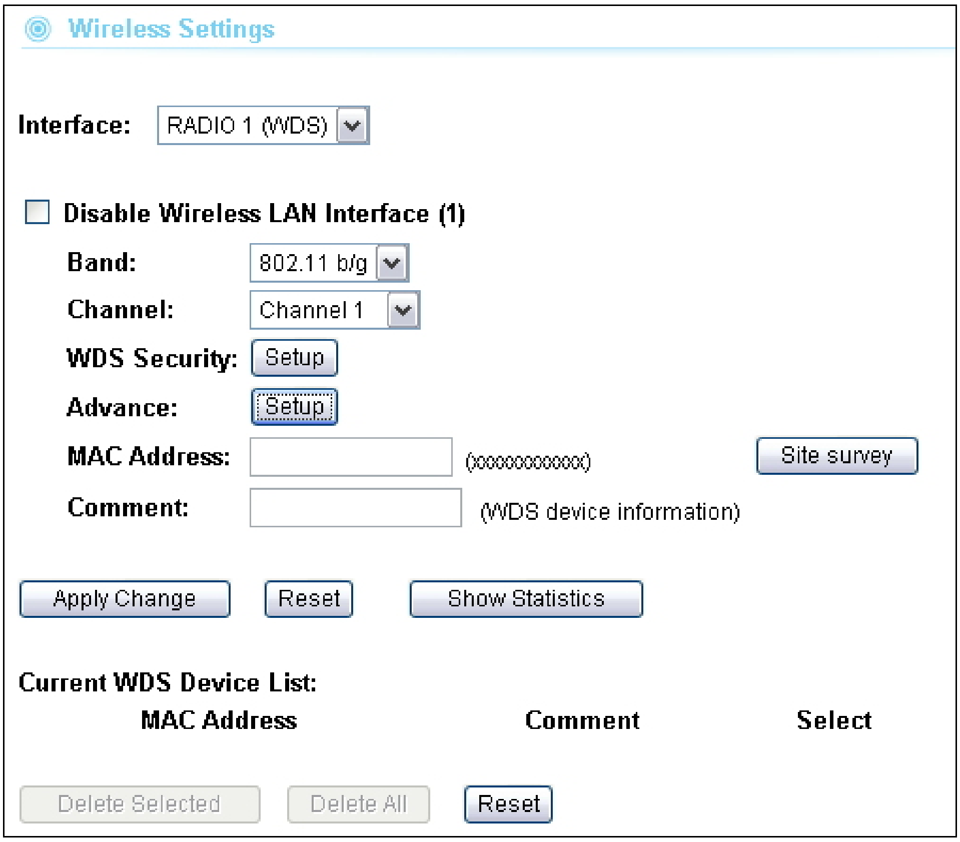




8.2 Radio1: WDS Bridge Settings

The Radio1 is working in WDS Bridge for connection to remote Bridge network.

When you select "Radio1" as the interface, the following screen will appear.



Wireless Settings

Interface: RADIO 1 (WDS)

☐ Disable Wireless LAN Interface (1)

Band: 802.11 b/g

Channel: Channel 1

WDS Security: Setup

Advance: Setup

MAC Address: (xxxxxxxxxxxx) Site survey

Comment: (WDS device information)

Apply Change | Reset | Show Statistics

Current WDS Device List:

MAC Address	Comment	Select

Delete Selected | Delete All | Reset

8.2.1 Basic Wireless Settings

- **Band:** You can choose between "802.11g/b", "802.11g", or "802.11b". We recommend to leave the setting at "802.11g/b".
- **Channel**: Wireless Channel used. For EU, it is channel 1~13. For U.S.A., it is

channel 1~11.

***802.11d Spanning Tree**: Enable this option to prevent network loop from forming. It is highly recommended to turn on this option if you have more than 2 entries in the WDS network. You can find this function in the “**System Configuration”->”LAN Interface Setup**” page.*

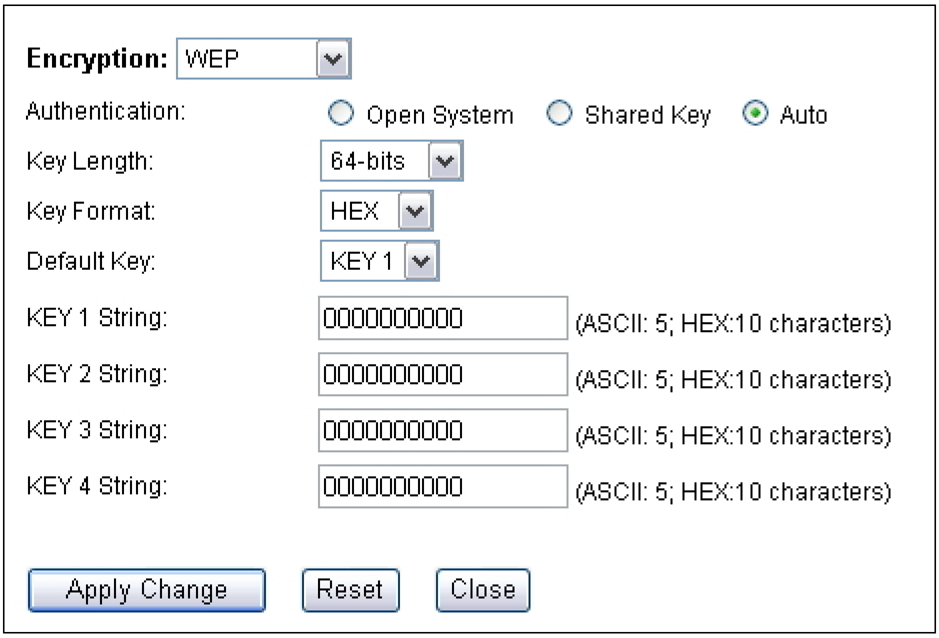
8.2.2 WDS Security

Operation Mode -> Setup -> Security Settings

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The G.DUO features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



Encryption: WEP

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bits

Key Format: HEX

Default Key: KEY 1

KEY 1 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 2 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 3 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 4 String: 0000000000 (ASCII: 5; HEX:10 characters)

- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

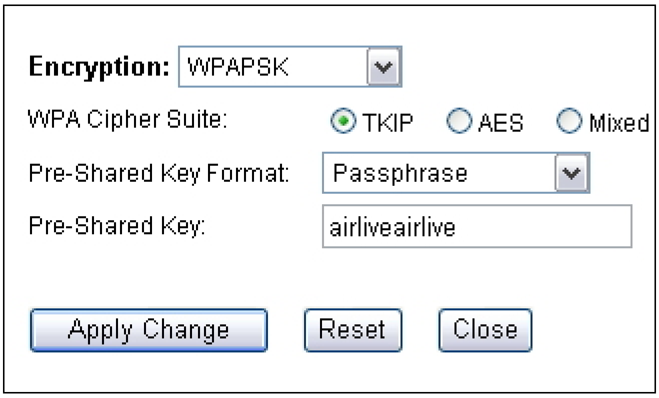
- **Authentication:** 2 types of Authentication are offered. Open system and

Shared key. If you are not sure which one to use, please select "Auto".

- **Key Length:** The G.DUO offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
- **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. "airlivepass12"). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
- **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, "passw"
- **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, "12345abcdef"
- **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, "airlivewepkey"
- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, "1234567890abcdef1234567890"

WPA-PSK, WPA2-PSK

Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.



Encryption: WPAPSK

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

Pre-Shared Key Format: Passphrase

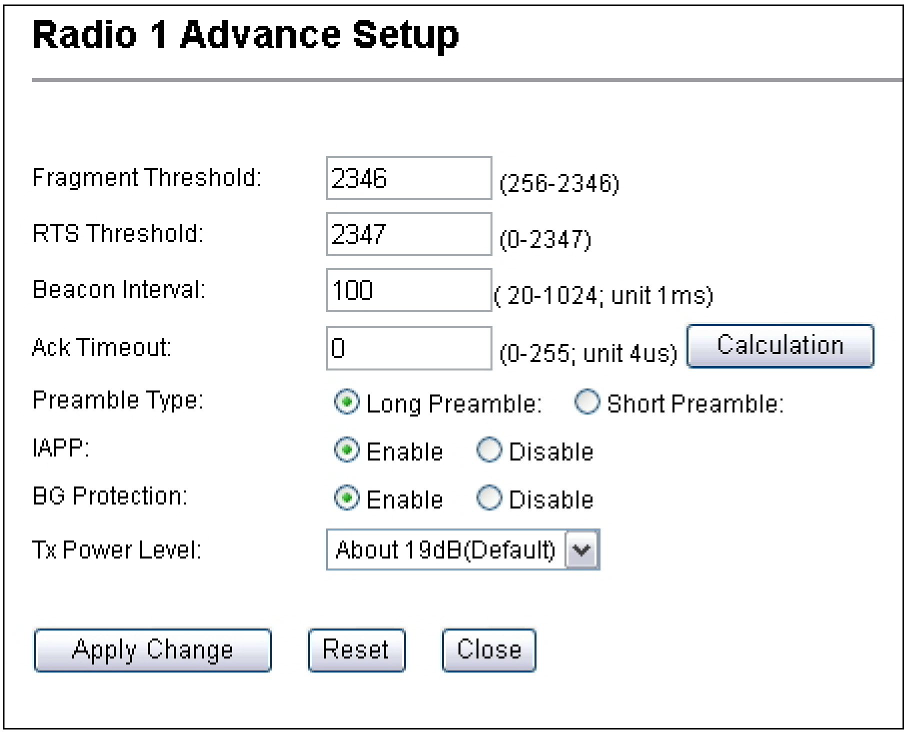
Pre-Shared Key: airliveairlive

- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.

- **Pre-Shared Key**: Enter the password key here..

8.2.3 Advance (Wireless Settings)

Operation Mode -> Setup -> Advance



Radio 1 Advance Setup

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024; unit 1ms)

Ack Timeout: 0 (0-255; unit 4us) Calculation

Preamble Type: ● Long Preamble: ○ Short Preamble:

IAPP: ● Enable ○ Disable

BG Protection: ● Enable ○ Disable

Tx Power Level: About 19dB(Default)

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **Preamble Type**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

- **BG Protection:** The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance..

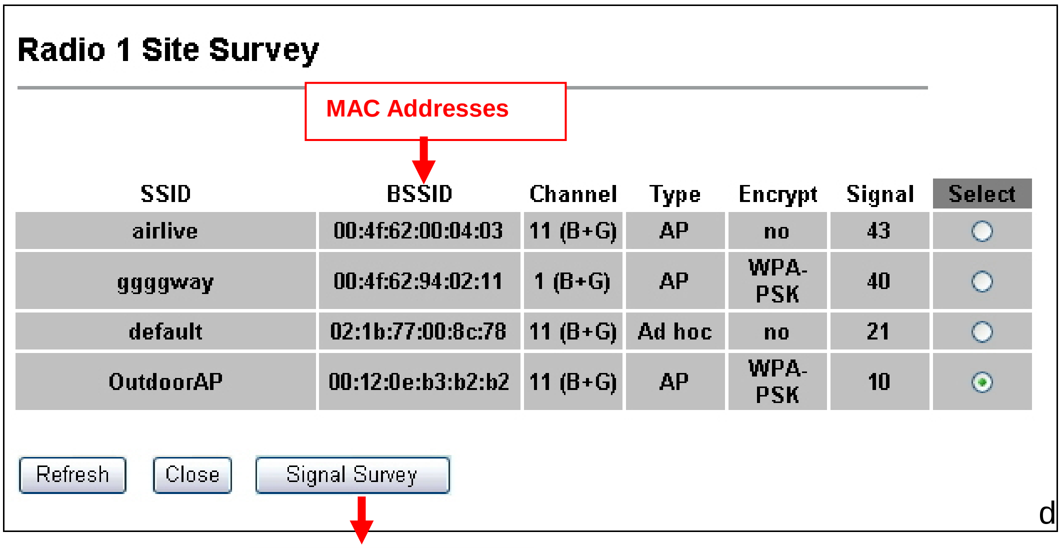
- **TX Power Level:** You can set your TX Output power level here. Please note the maximum allowable TX output power in EU is 20dBm. Please do not exceed your country's legal limit.

8.2.4 Site Survey

Operation Mode -> Setup -> Site Survey

WDS requires you to enter the MAC addresses of other remote bridges in the network. You can scan for wireless networks around your location using the Site Survey function. Then copy the MAC address of the remote Bridge into WDS table.

When you click on Site Survey, the following screen will appear. It might take awhile depending on number of available Bridges in the area.



Radio 1 Site Survey

MAC Addresses

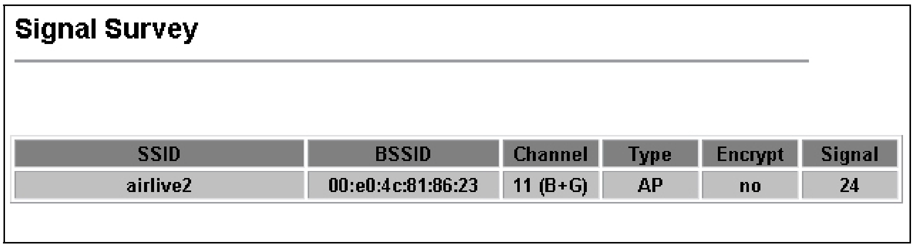
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
airlive	00:4f:62:00:04:03	11 (B+G)	AP	no	43	○
ggggway	00:4f:62:94:02:11	1 (B+G)	AP	WPA-PSK	40	○
default	02:1b:77:00:8c:78	11 (B+G)	Ad hoc	no	21	○
OutdoorAP	00:12:0e:b3:b2:b2	11 (B+G)	AP	WPA-PSK	10	●

For antenna alignment. It will display and update the Signal Strength conitnously

8.2.5 Signal Survey

Operation Mode -> Setup -> Site Survey -> Signal Survey

The Signal Survey will continuously display the Signal Strength of the selected SSID for antenna alignment purpose. To use Signal Survey function, please enter the "Site Survey" function first; please refer to the instruction in the above section. Once you select the ESSID and click on the "Signal Survey" button, the following screen will appear.



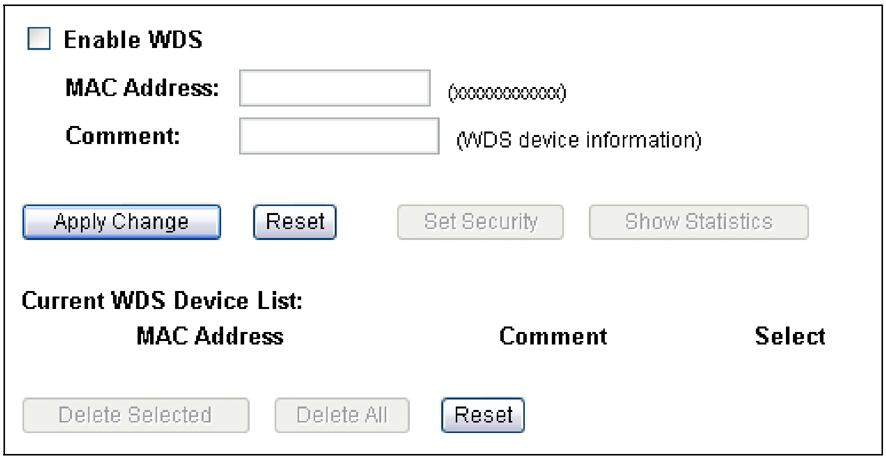
Signal Survey

SSID	BSSID	Channel	Type	Encrypt	Signal
airlive2	00:e0:4c:81:86:23	11 (B+G)	AP	no	24

- **BSSID**: This is the remote AP's MAC address.
- **Channel**: The current scanned channel
- **Signal**: This is signal strength number in percentage in 0 to 100 scale. The higher the number, the better signal.

8.2.6 WDS Settings

For Bridge network, it is required to enter the Wireless MAC address of all remote bridges that is connect directly to your G.DUO. The wireless MAC address is also known as BSSID that is display on your site survey result.

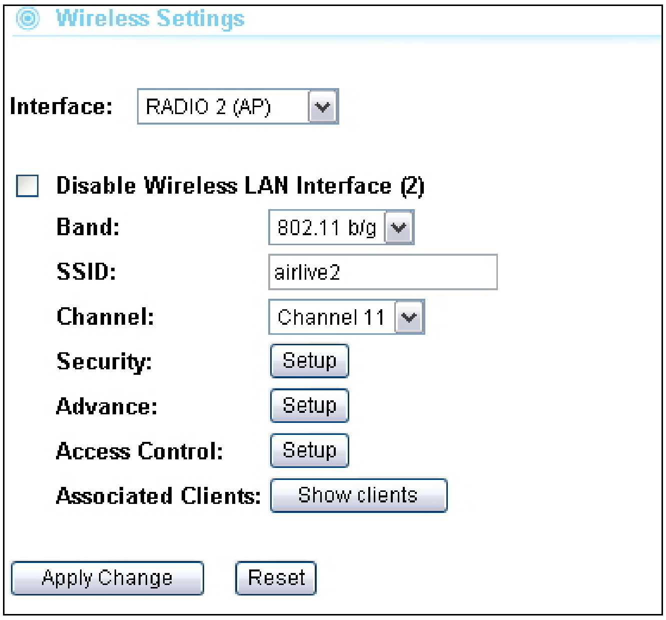


- **MAC Address:** Please enter the Wireless MAC address or BSSID of the remote Bridge. You can usually find it at remote Bridge's device label.
- **Comment:** If you input anything that will help remind you about which remote Bridge it is.

8.3 Radio2: AP Mode Settings

The Radio2 is working in Access Point Mode. The default SSID is "AirLive2".

When you select "Radio2" as the interface, the following screen will appear:



Wireless Settings

Interface: RADIO 2 (AP)

□ Disable Wireless LAN Interface (2)

Band: 802.11 b/g

SSID: airlive2

Channel: Channel 11

8.3.1 Basic Wireless Settings

- **Band:** You can choose between "802.11g/b", "802.11g", or "802.11b". We recommend leaving the setting at "802.11g/b".
- **SSID:** The SSID setting of the remote AP. If you are not sure, you can click on "Site Survey" button to scan for AP.
- **Channel**: Wireless Channel used. For EU, it is channel 1~13. For U.S.A., it is channel 1~11.

8.3.2 Security Settings

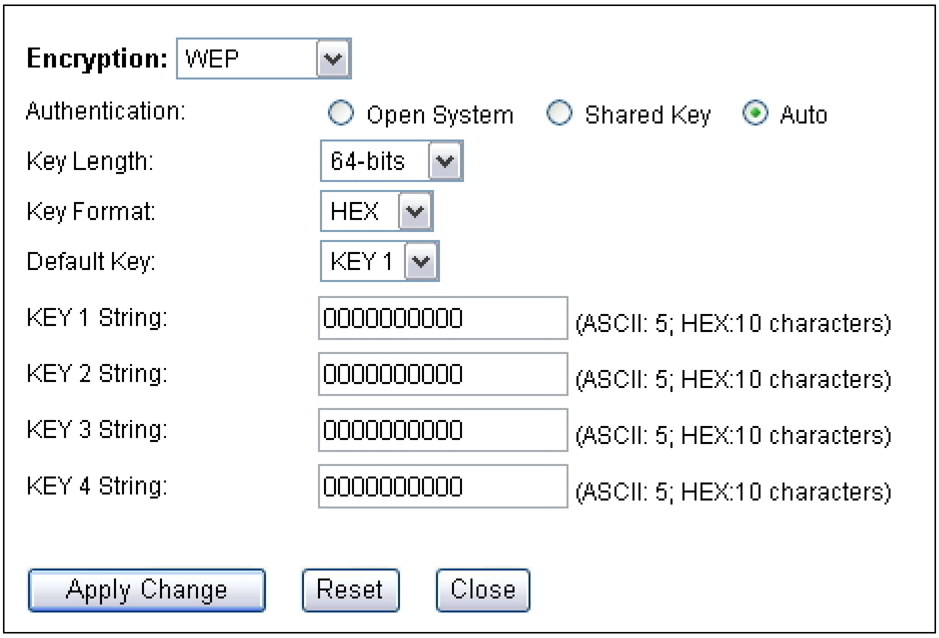
Operation Mode -> Setup -> Security Settings

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The G.DUO features various security policies including WEP, 802.1x, WPA,

WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



Encryption: WEP

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bits

Key Format: HEX

Default Key: KEY 1

KEY 1 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 2 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 3 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 4 String: 0000000000 (ASCII: 5; HEX:10 characters)

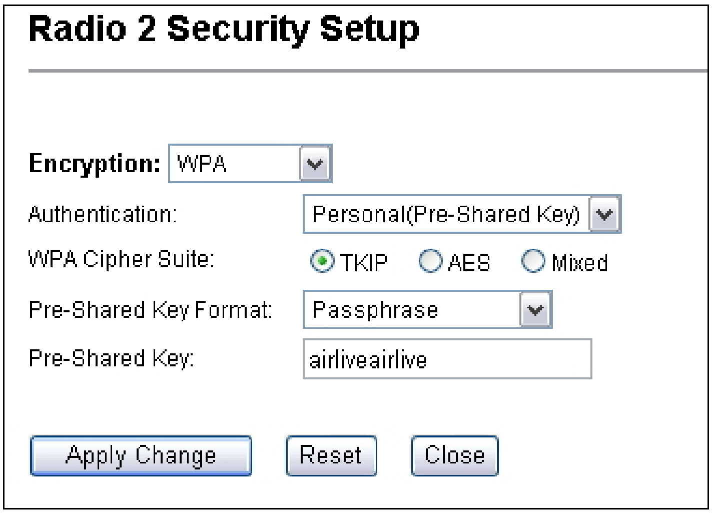
- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

  - **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select “Auto”.
  - **Key Length:** The G.DUO offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
  - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
  - **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, “passw”
  - **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
  - **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”

- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, “1234567890abcdef1234567890”

WPA-Personal, WPA2-Personal, WPA-Mixed (Pre-Shared Key)

The WPA Personal is also known as “WPA-PSK” encryption. Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.



Radio 2 Security Setup

Encryption: WPA

Authentication: Personal(Pre-Shared Key)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

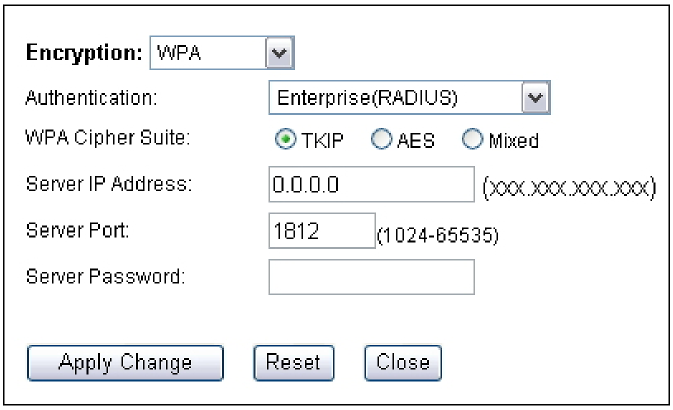
Pre-Shared Key Format: Passphrase

Pre-Shared Key: airliveairlive

- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

WPA-Enterprise, WPA2-Enterprise, WPA-Mixed Enterprise (Radius)

Wi-Fi Protected Access (WPA) Enterprise uses Radius Server as the authenticator. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA or WPA2.



Encryption: WPA

Authentication: Enterprise(RADIUS)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

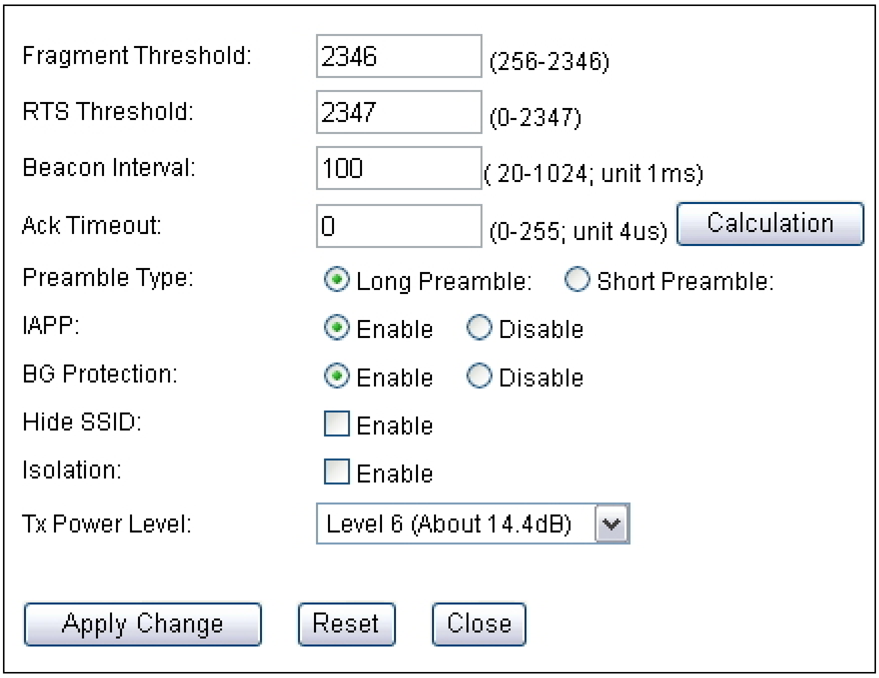
Server IP Address: 0.0.0.0 (xxx.xxx.xxx.xxx)

Server Port: 1812 (1024-65535)

Server Password:

8.3.3 Advance (Wireless Settings)

Operation Mode -> Setup -> Advance



Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024; unit 1ms)

Ack Timeout: 0 (0-255; unit 4us)

Preamble Type: ● Long Preamble: ○ Short Preamble:

IAPP: ● Enable ○ Disable

BG Protection: ● Enable ○ Disable

Hide SSID: □ Enable

Isolation: □ Enable

Tx Power Level: Level 6 (About 14.4dB)

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346.   If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **Preamble Type**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

- **IAPP:** IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station’s security context between current access point (AP) and new AP during handoff period.

- **BG Protection:** The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network’s performance**..**

- **Hide SSID:** Enable Hide SSID will make the AP network’s SSID invisible. A device can link with the AP only if correct SSID name is entered.

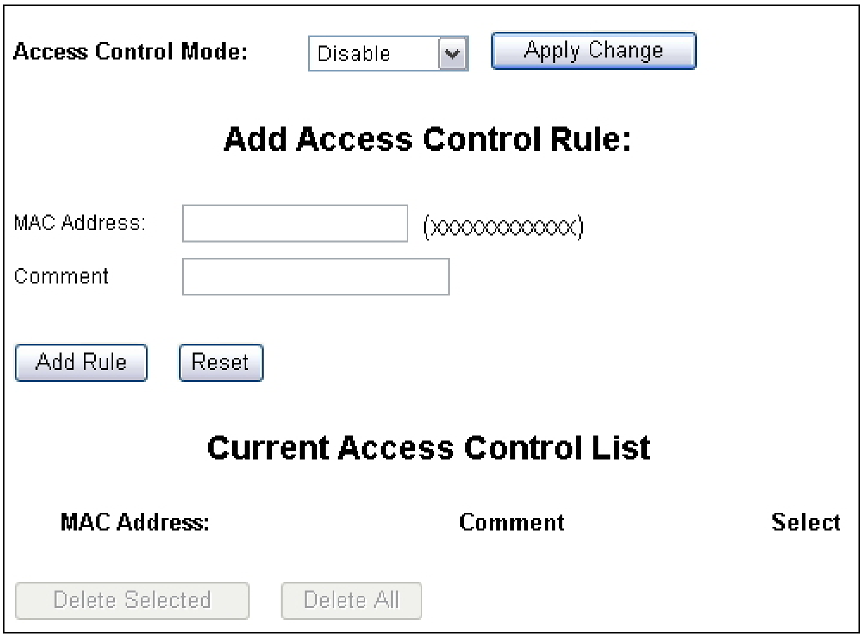
- **Isolation:** Enable Isolation will prevent wireless clients to see each other on the network.

- **TX Power Level:** You can set your TX Output power level here. Please note the maximum allowable TX output power in EU is 20dBm. Please do not exceed your country’s legal limit.

8.3.4 Access Control

Operation Mode -> Setup -> Access Control

The G.DUO allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and Gateway modes.



Access Control Mode: Disable

Add Access Control Rule:

MAC Address: (xxxxxxxxxxxx)

Comment

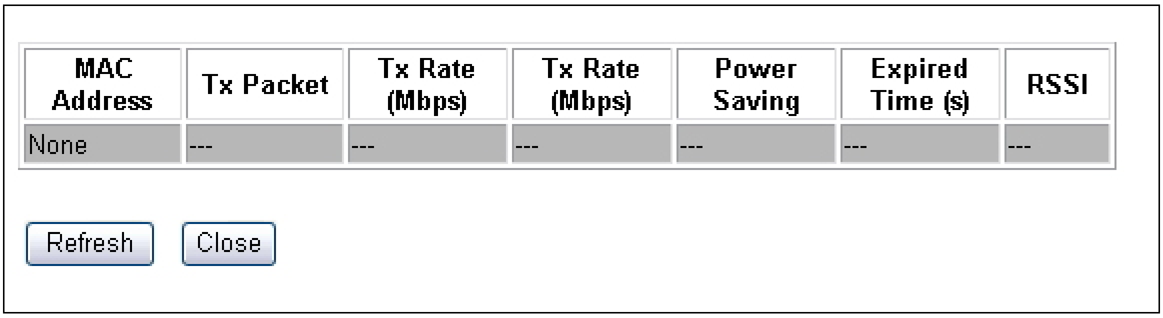
Current Access Control List

MAC Address:	Comment	Select

- **Access Control List**
  - **Disable:** When selected, no MAC address filtering will be performed.
  - **Allow list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.
  - **Deny list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

8.3.5 Associated Clients

Click on this to show the current wireless clients associated to the AP. It will display MAC adderss, Trasmit packet, Tx rate, power saving, expire time, and signal strength.



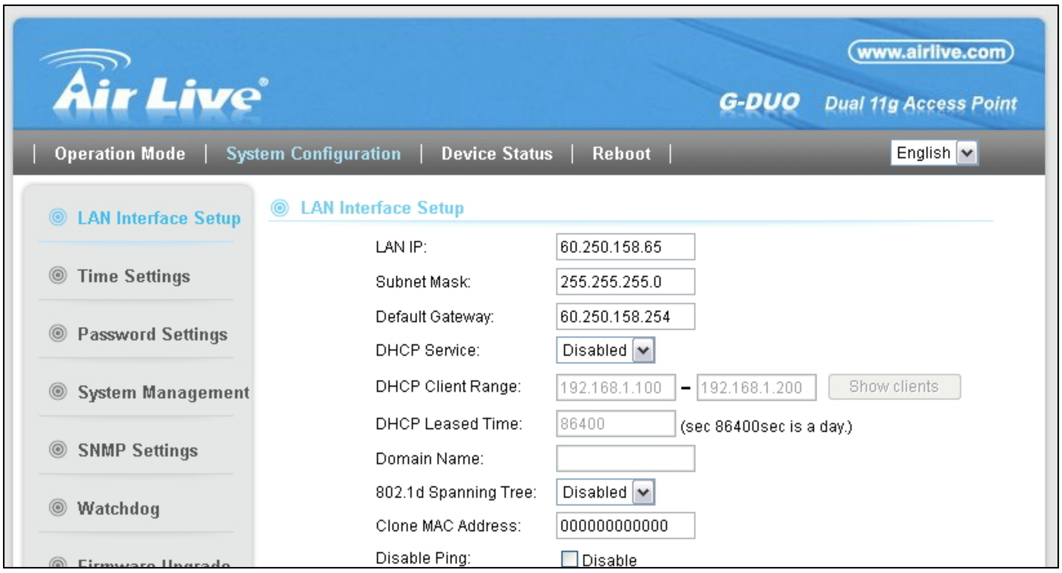
MAC Address	Tx Packet	Tx Rate (Mbps)	Tx Rate (Mbps)	Power Saving	Expired Time (s)	RSSI
None	---	---	---	---	---	---

9 System Configuration Menu

In this chapter, we will explain about *System Configurations* in web management interface. Please be sure to read through Chapter 3's "*Introduction to Web Management*" and *"Initial Configurations"* first. .

9.1 Menu Structure

When you click on the "System Configuration" menu on the top menu bar, the following screen will appear. The system configuration includes all non-wireless settings. We will explain their functions here.



LAN Interface Setup

LAN IP: 60.250.158.65

Subnet Mask: 255.255.255.0

Default Gateway: 60.250.158.254

DHCP Service: Disabled

DHCP Client Range: 192.168.1.100 – 192.168.1.200

DHCP Leased Time: 86400 (sec 86400sec is a day.)

Domain Name:

802.1d Spanning Tree: Disabled

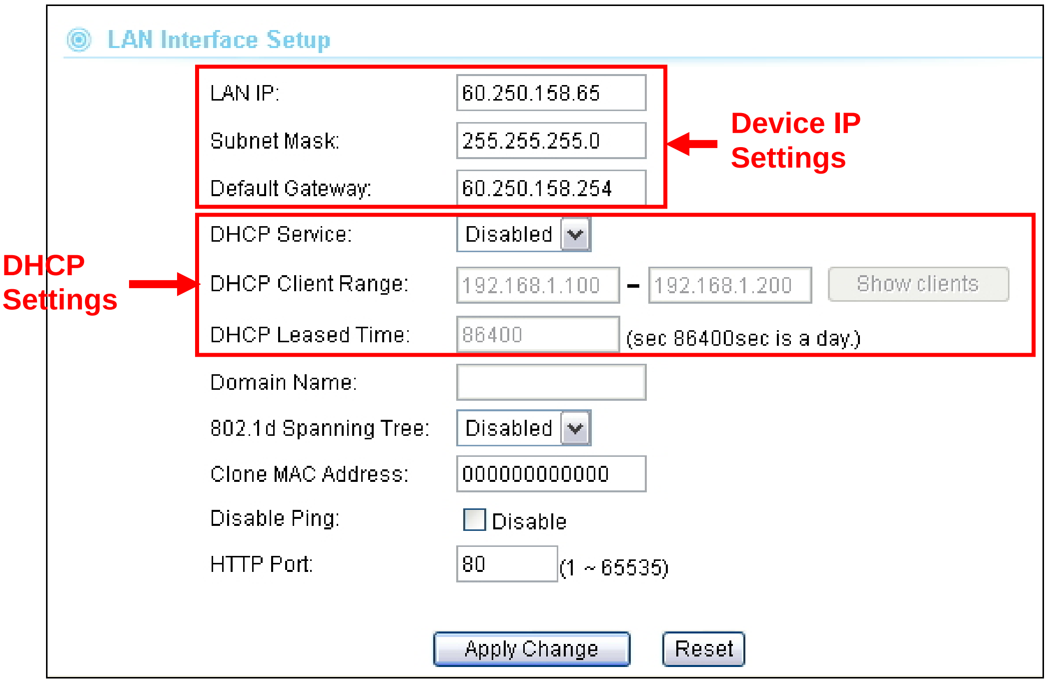
Clone MAC Address: 000000000000

Disable Ping: □ Disable

9.2 LAN Interface Setup

System Configurations>> LAN Interface Setup

This menu is where you can configuration all the aspect about LAN interface including IP address, DHCP server settings..etc.



LAN Interface Setup

LAN IP: 60.250.158.65

Subnet Mask: 255.255.255.0

Default Gateway: 60.250.158.254

DHCP Service: Disabled

DHCP Client Range: 192.168.1.100 – 192.168.1.200

DHCP Leased Time: 86400 (sec 86400sec is a day.)

Domain Name:

802.1d Spanning Tree: Disabled

Clone MAC Address: 000000000000

Disable Ping: □ Disable

HTTP Port: 80 (1 ~ 65535)

Device IP Settings

DHCP Settings

9.2.1 DHCP Settings

- **DHCP Service:** You can enable or disable DHCP server here.
  - **Disable**: Disable DHCP server
  - **Client:** The LAN interface will get IP address from DHCP server
  - **Server(default)**; The G.DUO will act as DHCP server to provide IP addresses to the clients on the LAN/Wireless interface. By default, the DHCP server is on.

- **DHCP Client Range**: You can define the IP pool from which the DHCP clients can get IP address.. Click on “Show Clients” to see the current DHCP client table.

- **DHCP Release Time:** You can define how long the G.DUO will reserve IP address for a particular PC or Device here.

9.2.2 802.1d Spanning Tree

Enable this will prevent forming of network loop.

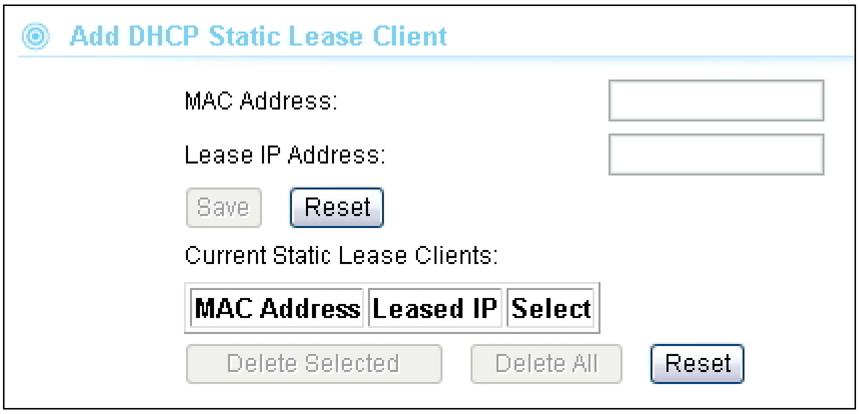
9.2.3 Clone MAC Address

You can change the MAC address of your LAN port to other value here.

9.2.4 Disable PING

If you do not wish the G.DUO to respond to remote PING command, please disable it here.

9.2.5 Add DHCP Static Lease Client



Add DHCP Static Lease Client

MAC Address:

Lease IP Address:

Current Static Lease Clients:

MAC Address	Leased IP	Select

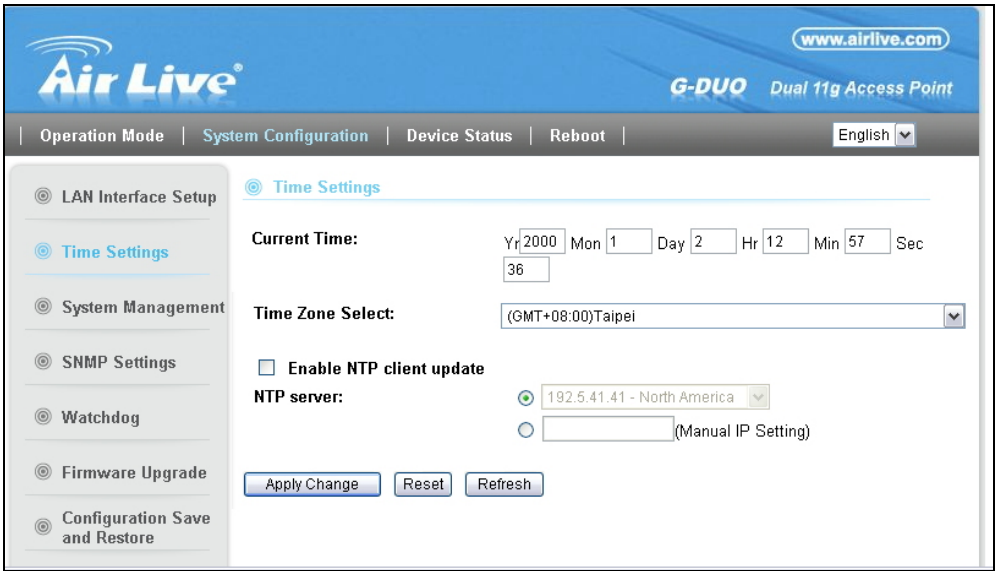
If you want to lock IP address to a MAC address, you should add DHCP clients to the “Static Lease Client”. Up to 40 entries can be entered. Below is the procedure for adding an entry:

1. Enter the MAC address of the device
2. Enter the IP address of the device
3. Click on the “Add” button

9.3 Time Settings

System Configuration ->Time Settings

You can set the NTP Time Server for your G.DUO’s internal clock here. You can use NTP server function so your G.DUO will check with NTP to set time automatically upon each startup. Thus, it prevents the clock losing track of time during reboot or power outage.



Time Settings

Current Time: Yr 2000 Mon 1 Day 2 Hr 12 Min 57 Sec 36

Time Zone Select: (GMT+08:00)Taipei

□ Enable NTP client update

NTP server: ● 192.5.41.41 - North America
○ (Manual IP Setting)

Below is the procedure to set your NTP server

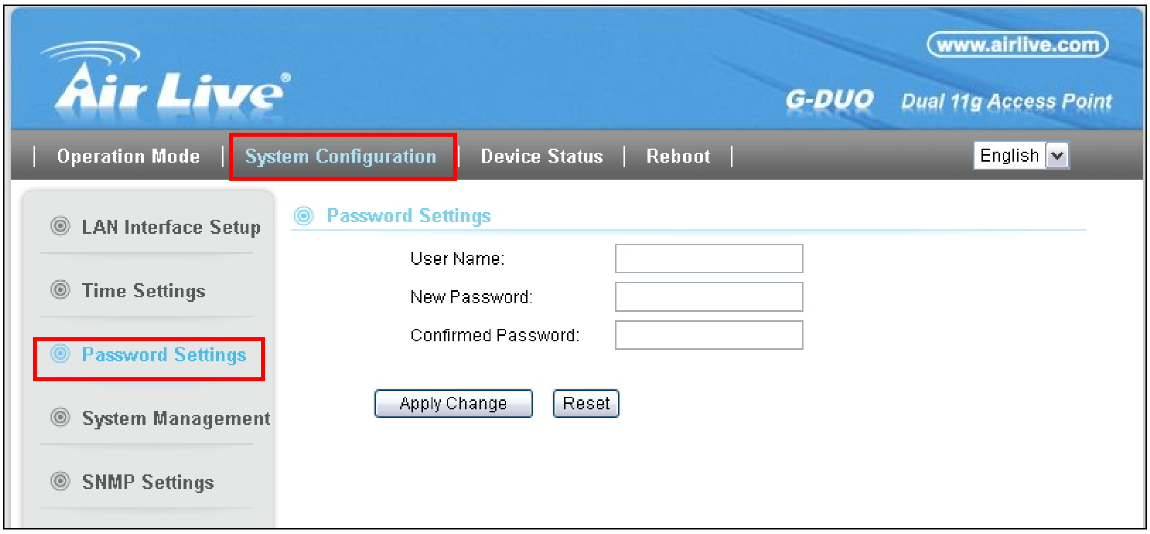
1. Check the “Enable NTP Client Update”

2. Select your time Zone
3. Select your NTP server
4. Click on “Apply Change”

9.4 Password Settings

System Configuration -> Password Settings

The G.DUO’s password protection is turned off by default. To enable password protection or change password, just enter your username and password, and click on “Apply Change” button.



Password Settings

User Name:

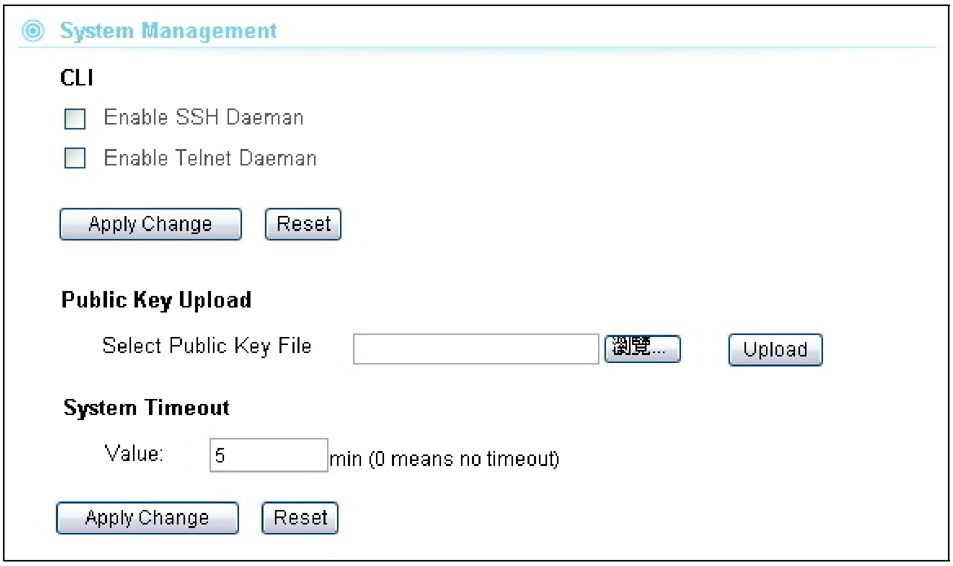
New Password:

Confirmed Password:

9.5 System Management

System Configuration -> System Management

In this page, administrator can change the management parameters and disable/enable management interface.



System Management

CLI

□ Enable SSH Daeman

□ Enable Telnet Daeman

Public Key Upload

Select Public Key File

System Timeout

Value: 5 min (0 means no timeout)

CLI (Command Line Interface):

You can enable or disable Telnet and SSH management interface from here.

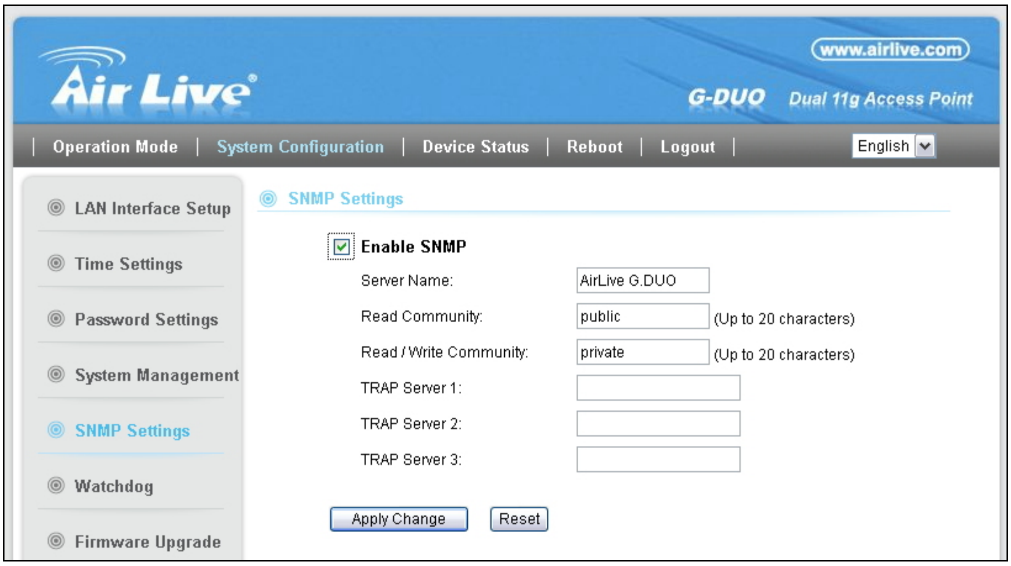
Public Key Upload: You can upload your public for the SSH authentication here.

System Timeout Value: This is the time the AP will wait when there is no configuration activity, then it will log out the user. We strongly recommend to leave the value at zero.

9.6 SNMP Settings

System Configuration -> SNMP Settings

The G.DUO's SNMP management is OFF by default. You should come to this page to enable the SNMP management. The G.DUO supports RFC-1213MIB and SNMPv2 MIB.



☑ Enable SNMP

Server Name:	AirLive G.DUO	
Read Community:	public	(Up to 20 characters)
Read / Write Community:	private	(Up to 20 characters)
TRAP Server 1:		
TRAP Server 2:		
TRAP Server 3:		

- **System Name:** A name that you assign to your G.DUO. It is an alphanumeric string of up to 30 characters.

- **Read Community:** If you intend the router to be managed from a remote SNMP management station, you need to configure a read-only "community string" for read-only operation. The community string is an alphanumeric string of up to 15 characters.

- **Read/Write Community:** For read-write operation, you need to configure a write "community string".

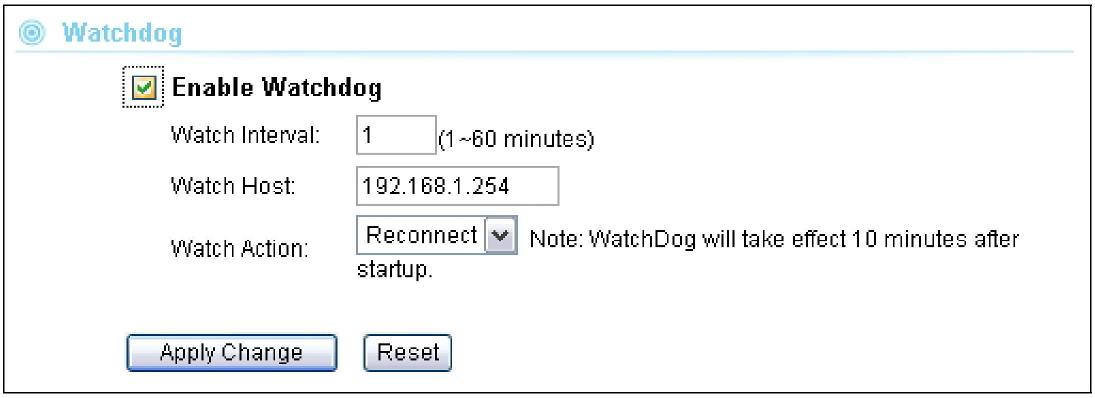
- **Trap Server:**
  A trap server is a remote SNMP management station where special SNMP trap

messages are generated (by the router) and sent to in the network. You can define up to 3 trap servers in the system.

9.7 Watchdog

System Configuration -> Watchdog

The Ping Watchdog will ping remote IP addresses to make sure the wireless connection is active, if not, it can either reconnect or reboot. To prevent the AP from power recycling, the PING watchdog will start 10 minutes after power up to prevent power recycle problem.



Watchdog

☑ Enable Watchdog

Watch Interval: 1 (1~60 minutes)

Watch Host: 192.168.1.254

Watch Action: Reconnect Note: WatchDog will take effect 10 minutes after startup.

- **Watch Interval:** means: "How often the CPE will PING". For example, it will PING once every "1" minute.

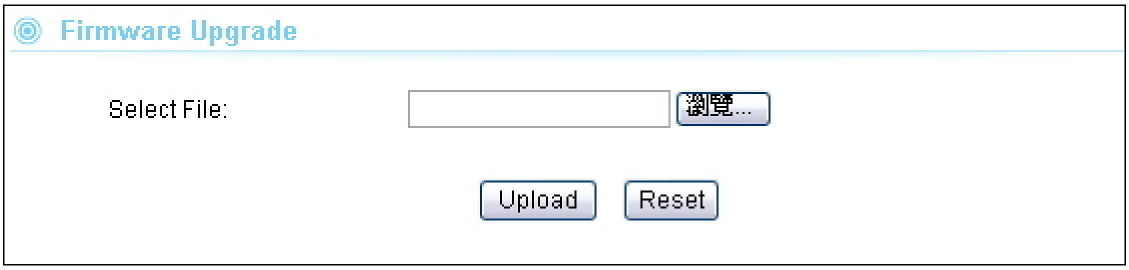
- **Watch Host:** This is the IP address for which the Watchdog will ping.

- **Watchdog Actions:** if the Watch Host fail to respond to PING. Then one of the action below will be taken.
  - Reconnect: the G.DUO will attempt to re-establish the connection.
  - Reboot: the G.DUO will do a power recycle.

9.7.1 Firmware Upgrade

System Configuration -> Firmware Upgrade

You can upgrade the firmware of your G.DUO (the software that controls your G.DUO’s operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have encountered with the current version.



■ **Upgrade Firmware:**

To update the G.DUO firmware, first download the firmware from AirLive web site to your local disk. ***Please do not use the firmware for Emergency Upgrade, it might damage your AP!.*** Then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

The new firmware will be loaded to your G.DUO. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.

> ⚠ Do not power off the device while upgrading the firmware.
> It is recommended that you do not upgrade your G.DUO unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

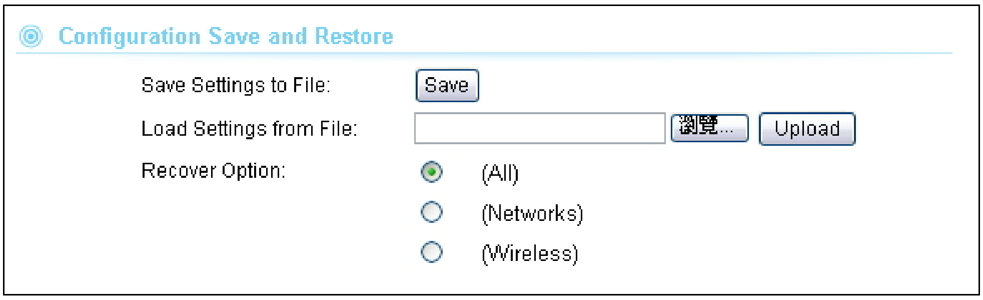
9.7.2 Configuration Save and Restore

System Configuration -> Configuration Save and Restore

The G.DUO can save and restore the settings to a file. In addition, it has the unique capability to restore only the network or wireless settings. This makes changes of wireless settings across the entire network of AP much easier.

You can save system configuration settings to a file, and later download it back to the G.DUO by following the steps.

Step 1 Select *Configuration Save and Restore* from the *System Configurations* menu.



Step 2 Click on “Save to” and Enter the path of the configuration file to save-to.

Restore Setting:

Step 1: Choose the Recovery Options

- All: Restore all settings
- Networks: Only restore the network parameters, not including wireless
- Wireless: Only restore the wireless settings.

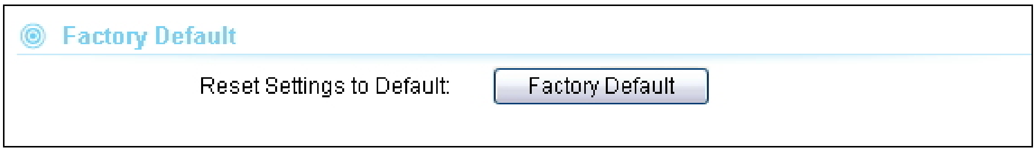
Step 2: Enter the file name in the “Load Settings from File” field. Or click on “Browse” button to location the location of the file.

Step3: Click on “Upload” button to restore settings.

9.8 Factory Default

System Configuration -> Factory Default

You can reset the configuration of your G.DUO to the factory default settings.



Factory Default

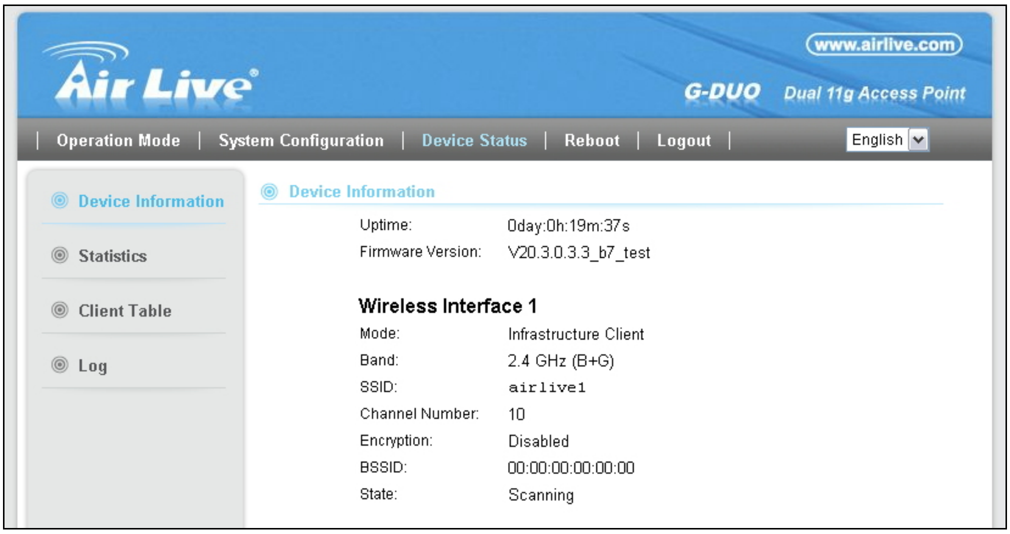
Reset Settings to Default: Factory Default

10 Device Status Menu

In this chapter, we will explain the “Device Status” menu in the web management interface. Before you read this chapter, please make sure to read through chapter 3 on “Introduction to Web Management Interface.

10.1 Menu Structure

When you click on the “Device Status” on the top menu bar, the sub menu for device status will appear.


www.airlive.com
G-DUO Dual 11g Access Point
Operation Mode | System Configuration | Device Status | Reboot | Logout
English
Device Information
Statistics
Client Table
Log

Device Information

Uptime: 0day:0h:19m:37s
Firmware Version: V20.3.0.3.3_b7_test

Wireless Interface 1
Mode: Infrastructure Client
Band: 2.4 GHz (B+G)
SSID: airlive1
Channel Number: 10
Encryption: Disabled
BSSID: 00:00:00:00:00:00
State: Scanning

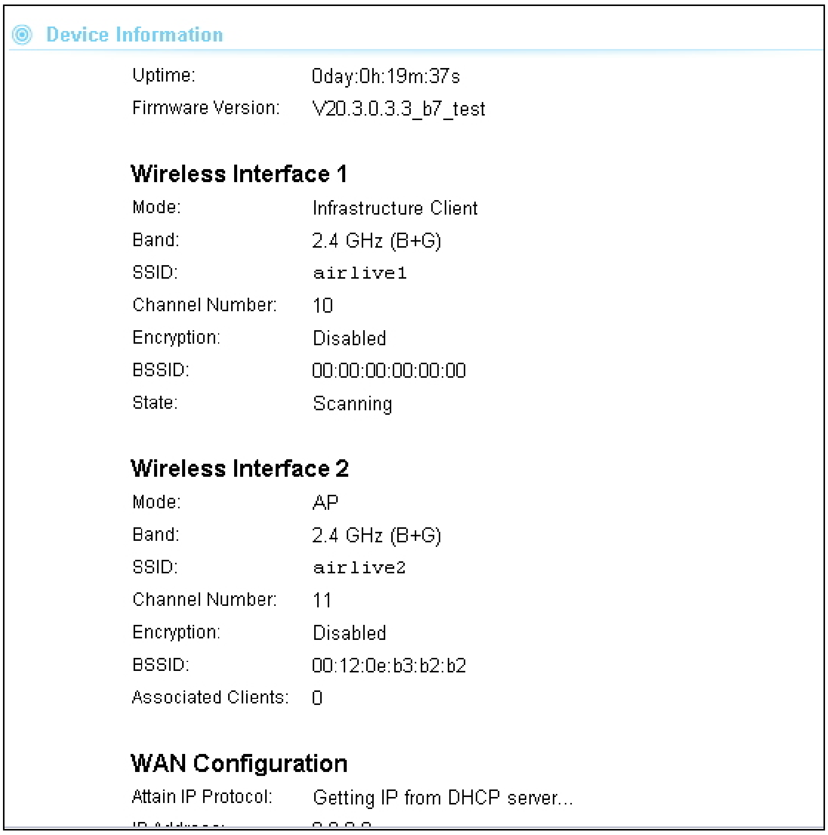
10.2 Device Information

This page shows the general information about G.DUO such as Uptime, Firmware version, Wireless Interface…etc. Below are some additional explanations on some status information of this page:

- **Uptime** This displays the time since system last boot up. This is a good indication for how long the system has been alive.
- **Firmware version**: The first G.DUO firmware release is 1.00e10. In general, AirLive will refer to its firmware as exx (such as e10) version on the release note
- **Wireless Interface 1**: This page displays the current settings and status of the Radio 1. It include the BSSID and connection status. The BSSID is also the wireless MAC address that is needed for the WDS entry.
- **Wireless Interface 1**: This page displays the current settings and status of the Radio 2. It include the BSSID and connection status. It also indicates the number of wireless

clients in AP

- **WAN Configuration:** WAN configuration tells you the current status of WAN port such as IP address and connection status.



Device Information

Uptime: 0day:0h:19m:37s
Firmware Version: V20.3.0.3.3_b7_test

Wireless Interface 1

Mode: Infrastructure Client
Band: 2.4 GHz (B+G)
SSID: airlive1
Channel Number: 10
Encryption: Disabled
BSSID: 00:00:00:00:00:00
State: Scanning

Wireless Interface 2

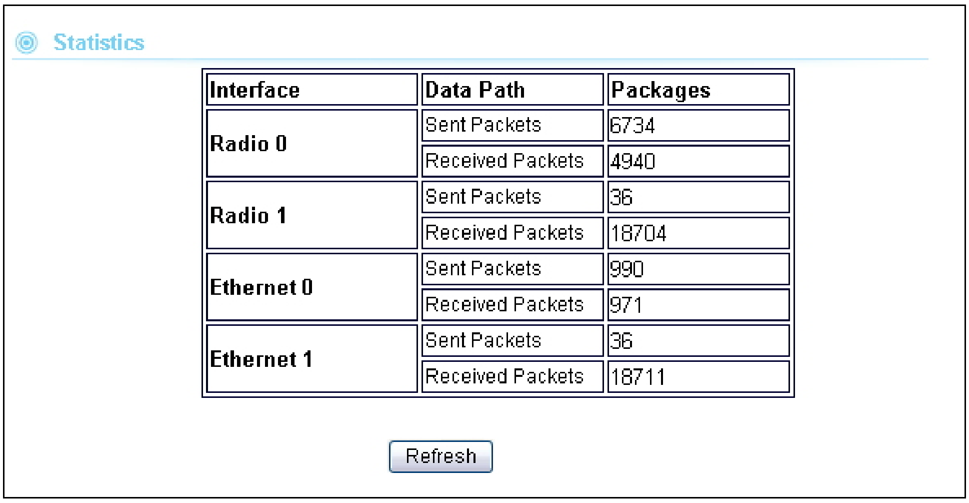
Mode: AP
Band: 2.4 GHz (B+G)
SSID: airlive2
Channel Number: 11
Encryption: Disabled
BSSID: 00:12:0e:b3:b2:b2
Associated Clients: 0

WAN Configuration

Attain IP Protocol: Getting IP from DHCP server...

10.3 Statistic

This page shows the sent and received packet information for Radio1, Radio2, LAN, and WAN interface.

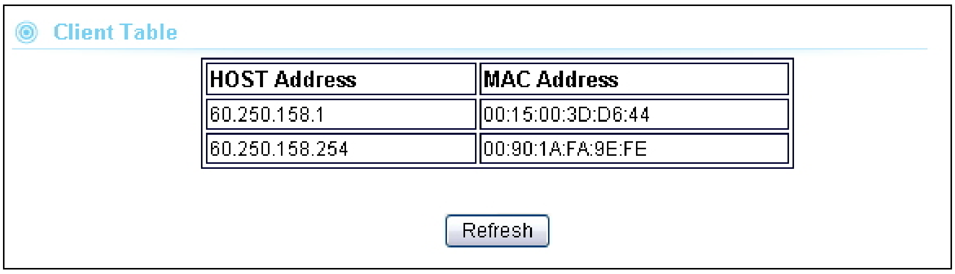


Statistics

Interface	Data Path	Packages
Radio 0	Sent Packets	6734
	Received Packets	4940
Radio 1	Sent Packets	36
	Received Packets	18704
Ethernet 0	Sent Packets	990
	Received Packets	971
Ethernet 1	Sent Packets	36
	Received Packets	18711

10.4 Client Table (ARP Table)

This table is also known as ARP table. It will show all wireless and wired device connected to the G.DUO. If you want to look at the wireless clients only, you can go to the "Wireless Settings" page in AP or Gateway mode for "Show Client" button.

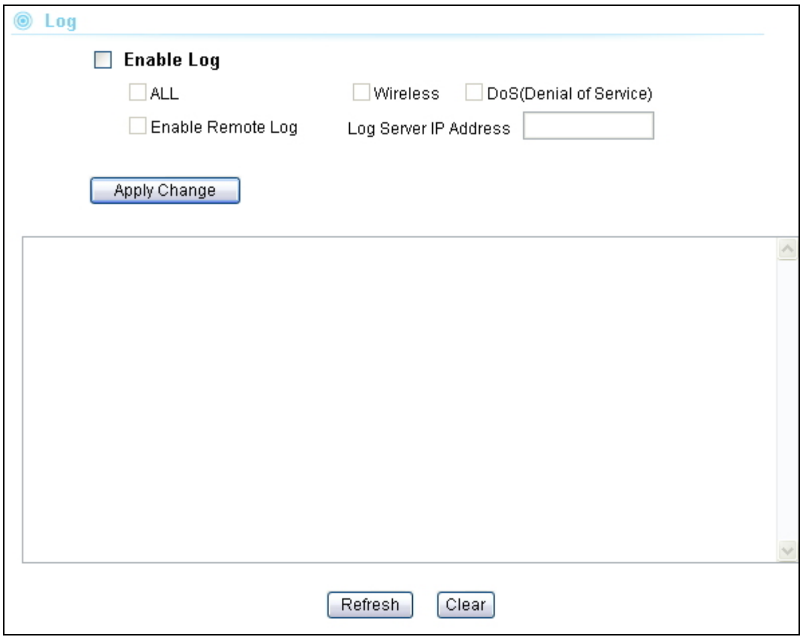


Client Table

HOST Address	MAC Address
60.250.158.1	00:15:00:3D:D6:44
60.250.158.254	00:90:1A:FA:9E:FE

10.5 Log

The log function is where you can check for error messages for diagnostic purpose.



Log

□ Enable Log

□ ALL □ Wireless □ DoS(Denial of Service)

□ Enable Remote Log Log Server IP Address

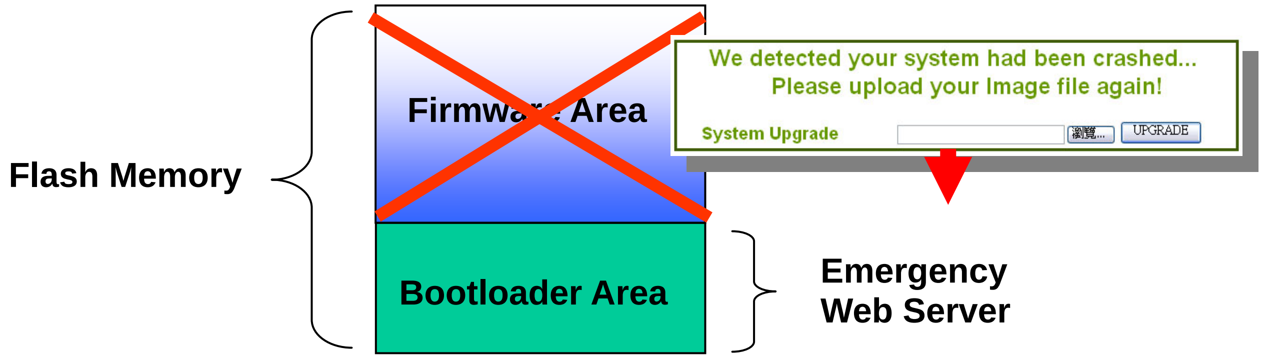
- **Enable Log**: Check this box to enable log function.
  - **All**: register all logs
  - **Wireless**: register wireless log only
  - **DoS**: register DoS attack log only
- **Enable Remote Log**: This will enable the Syslog function. All logs will be sent to the Syslog server
  - **Log Server IP address**: Enter the Syslog server IP address.

11 Emergency Firmware Recovery

The G.DUO features emergency firmware upgrade function that can restore your AP from a firmware crashed. If you can't access your AP anymore, please first try to restore the setting to default by holding the RESET button (in the back) for more than 7 seconds. You should be able to find the AP at 192.168.1.254. If you can't find it, then please perform the emergency upgrade. ***The Emergency Upgrade requires special G.DUO firmware***, please visit www.airlive.com->support->download and type "G.DUO" to the download page.

How Emergency Upgrade Works?

G.DUO's flash memory is divided into "firmware" and "bootloader" area. The bootloader area is protected from writing and has a built-in emergency web server. Therefore, the AP can be recovered from emergency web server after a firmware crash. The emergency web server is enabled when AP is forced into emergency upgrade mode, it's IP will be changed to ***192.168.1.6***.



We detected your system had been crashed...
Please upload your Image file again!

Procedure to Restore the AP using Emergency Upgrade

1. Please connect your PC directly to the ***LAN 2, LAN3, or LAN4 port*** of the AP. Do not connect to LAN1.

2. set your PC's IP address to 192.168.1.50

3. Before connecting the power, please press and holding the "Reset" button(in the back of the AP). Then plug in the power. Keep press and hold the Reset button until the "Power" LED goes off(about10 seconds)

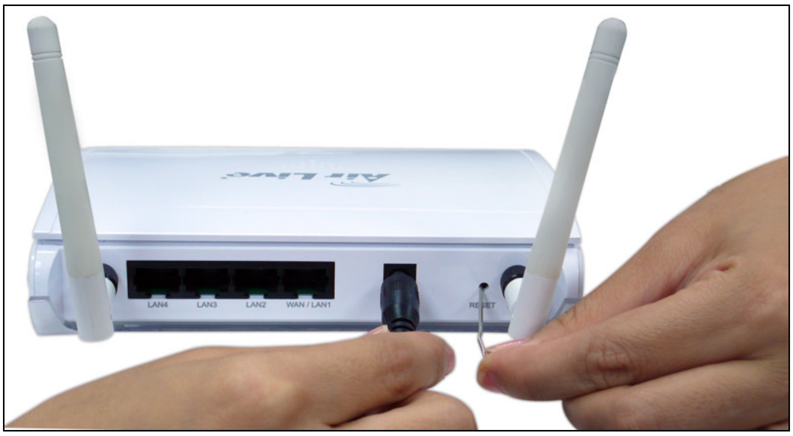
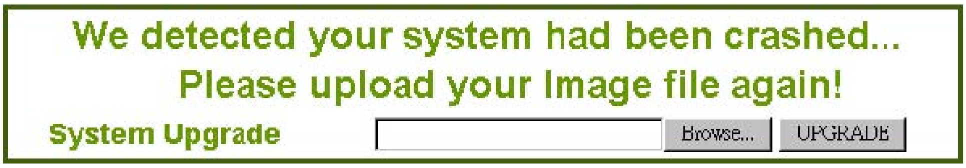


Fig 1-2 : Press and hold the reset button while plugging in the power.

6. Open a browser; type “192.168.1.6” for the website address. The following screen should show up



We detected your system had been crashed...
Please upload your Image file again!
System Upgrade

7. Click the “Browse” button, select and open the correct firmware file. This firmware file is different from the Web upgradeable firmware. Please go to www.airlive.com to G.DUO’s support page and download the special firmware for emergency upgrade.

8. Click on “UPGRADE” button. Do not touch the AP or PC until the upgrade is completed.

9. Wait for AP to finish reboot. Open the web browser, and type “192.168.1.254”. You should be able to login into the normal Web UI.

12 Frequent Asked Questions

In this chapter, we will address some frequent asked questions about G.DUO

Question: Why is there no password protection for G.DUO?

Answer: By default, the password protection is turned off for G.DUO. Please go to “System Configuration -> Password Settings”, then enter a new set of username and password to turn it on.

===

Question: I forgot my password or the IP address of G.DUO.

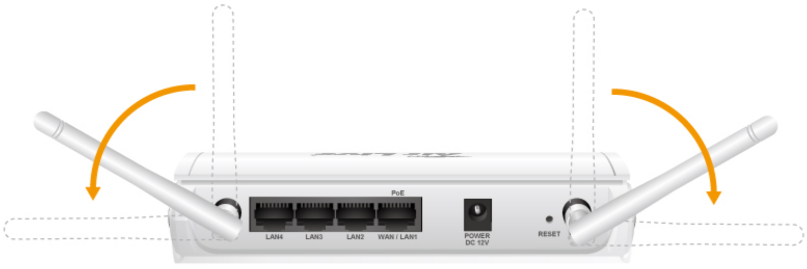
Answer: Please restore your settings to default by press the reset button for more than 7 seconds. You should be able to find your G.DUO at 192.168.1.254 with password “airlive”.

==

Question: Why am I not getting good performance when I am running 2 radios at the same time?

Answer: G.DUO’s 2 radios system require special attention in regards to mutual interference. It is recommended that you take the following steps to ensure best performance for a 2-radio system

1. Please make sure the 2 radios’ channels are set as far apart as possible. For example, one at channel 1 and one at channel 11
2. Please adjust the angle of the antenna or the orientation of the AP to get the best performance. The best performance is about 30 degree from horizontal as indicated in the graph below.



3. Do not increase the TX output power unless one or both radio are using directional antenna.

===

Question: When I wan to use “Site Survey” tool to connect with a AP that has no encryption, why does the G.DUO report “encryption type mismatch!” and ask me to configure the wireless security settings?

Answer: When you press “Connect” from site survey, the G.DUO will first check if the current wireless encryption setting is correct. If not, it will ask you to modify the setting. Therefore, if your current wireless settings has encryption and the new AP you want to associate does not use encryption, then the G.DUO will report the mismatch. In this case, simple select “Disable” in the encryption field and press “Apply Change”.

===

Question: When I change my wireless operation mode, why can’t I find my AP anymore?

Answer: This situation can have 2 possibilities..

1. By Default, the DHCP server is turned on in WISP+AP and Gateway+AP mode. In other modes, the DHCP server is turned off. If you get your IP address automatically, then when you change to Dual AP, Client+AP, or WDS+AP modes. Your PC will not be able to get IP address from DHCP server anymore, therefore, you should set the IP address manually.
2. When you change the mode to WISP+AP or Gateway+AP mode, the GDUO’s IP address might change to 192.168.1.254. Therefore; if you can’t find the device’s IP in these modes, please set your PC’s IP address to automatically get from DHCP server, then you should find the G.DUO at 192.168.1.254.

===

Question: Why can’t I get Telnet or SSH access?

Answer: The Telnet or SSH interface are turned off by default. Please go to “System Configuration-> System Management” menu to enable them.

===

Question: Why can't I get SNMP access?

Answer: The SNMP management interface is turned off by default. Please go to "System Configuration-> SNMP Management" menu to enable it.

===

Question: Where is the POE port for G.DUO?

Answer: The PoE system used for G.DUO is 12V Passive PoE. LAN1 is also used as the passive PoE port.

===

Question: Where is the signal survey function that displays the signal strength continuously for antenna alignment?

Answer: The "Signal Survey" function is inside the Site Survey function. After the site survey, please select a SSID and press the "Signal Survey" button. ***The signal strength is indicated by percentage, not by SIGNAL STRENGTH***. The higher the number, the stronger the signal.

===

Question: Why can't I perform emergency upgrade correctly?

Answer:

1. Please make sure you are connecting your PC to LAN2, LAN3, or LAN4. Do not connect to LAN 1.

2. You need special firmware for emergency upgrade. Please visit www.airlive.com to download the file.

13 Specifications

The specification of G.DUO is subject to change without notice. Please use the information with caution.

13.1 Hardware Features

13.1.1 General Hardware Feature

- Realtek Dual 11g/b Chipset
- 4MB Flash, 32MB SDRAM
- RoHS compliant
- 4 10/100 Mbps Ethernet Port with Auto MDI/MDI-X support
- 12V Passive PoE Port (LAN1)
- WAN Port (LAN1)
- Radio1: 26dBm(South America) or 20dBm(EU) TX output power
- Radio2: 24dBm(South America) or 20dBm(EU) TX output power
- 7 LED indicators
- Wall Mount Screw Holes
- Switching DC12V Power adapter
- Reset Button
- 2 x R-SMA antenna conectors

13.2.1 Power Supply

- Power Adapter Voltage : input 100~240Vac/50~60Hz , output 12V/1A
- Advance Passive PoE (Accept 12 to 24 volts)

13.2.2 Dimension and Weight

- Dimension: 154 x 130 x 316 mm
- AP Unit Weight(Approximate): 280g
- Package Weight(Approximate): 686g

13.2 Radio Specifications

13.2.1 Frequency Band

- USA (FCC) 11 Channels: 2.412GHz~2.462GHz
- Europe (ETSI) 13 Channels : 2.412GHz~2.472GHz d

13.2.3 Rate and Modulation

- Data Rate: 54, 48, 36, 24, 18,11, 5.5, 2, 1 Mbps
- Modulation
  - 11g Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK, BPSK)
  - 11b Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK)

13.2.4 TX Output Power

Radio1:

- South America: 26dBm (11b)
- South America: 20dBm (11g)
- EU: 20dBm(11b)
- EU: 20dBm(11g)

Radio2:

- South America: 24dBm (11b)
- South America: 20dBm (11g)
- EU: 20dBm(11b)
- EU: 20dBm(11g)

13.2.5 Receiver Sensitivity

- **RF1**

Data Rate	SIGNAL STRENGTH (dB)
1 Mbps	-92
2 Mbps	-91
5.5 Mbps	-88
6 Mbps	-86

9 Mbps	-86
11 Mbps	-85
12 Mbps	-85
18 Mbps	-84
24 Mbps	-80
36 Mbps	-78
48 Mbps	-73
54 Mbps	-72

- **RF2**

Data Rate	SIGNAL STRENGTH (dB)
1 Mbps	-90
2 Mbps	-88.5
5.5 Mbps	-88
6 Mbps	-83
9 Mbps	-83
11 Mbps	-84
12 Mbps	-83
18 Mbps	-82
24 Mbps	-81
36 Mbps	-77
48 Mbps	-74
54 Mbps	-71

13.2.6 Supported WLAN Mode

- WISP + AP Mode
- Dual AP Mode
- Client + AP Mode
- Gateway + AP Mode
- WDS + AP Mode

13.3 Software Features

Operation Modes

- WISP + AP Mode
- Dual AP Mode
- Client + AP Mode

- Gateway + AP Mode
- WDS + AP Mode

Management Interface

- Web HTTP
- Secured Web (HTTPS)
- Telnet (CLI)
- SSH/SSH2 (Secured Shell)
- SNMP v1/v2 Support
  - SNMP Read/Write Community String
  - SNMP Trap support
  - RFC-1213 MIB Support
  - SNMPv2 MIB

Advance Functions

- Site Survey with Signal Strength Indicator
- Bandwidth Control / Traffic Shaping
- Wi-Fi, WPA compatible interoperability
- WPA with PSK/TKIP/AES support ,WPA2 support
- Privacy Separator support
- Hide SSID Support
- Support adjustable output power
- ACK Timeout Adjustment
- Bootloader Protection and Emergency Firmware Upload Code
- Radius Supported
- Up to 40 Static DHCP entries
- Firmware upgrade and configuration backup via Web
- Partial Configuration Backup and Restore

14 Wireless Network Glossary

The wireless network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

802.3ad

802.3ad is an IEEE standard for bonding or aggregating multiple Ethernet ports into one virtual port (also known as trunking) to increase the bandwidth.

802.3af

This is the PoE (Power over Ethernet) standard by IEEE committee.   803.af uses 48V POE standard that can deliver up to 100 meter distance over Ethernet cable.

802.11b

International standard for wireless networking that operates in the 2.4 GHz frequency band (2.4 GHz to 2.4835 GHz) and provides a throughput up to 11 Mbps.

802.1d STP

Spanning Tree Protocol.   It is an algorithm to prevent network from forming.   The STP protocol allows net work to provide a redundant link in the event of a link failure.   It is advise to turn on this option for multi-link bridge network.

802.11d

Also known as "Global Roaming".   802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

802.11e

The IEEE QoS standard for prioritizing traffic of the VoIP and multimedia applications. The WMM is based on a subset of the 802.11e.

802.11g

A standard provides a throughput up to 54 Mbps using OFDM technology. It also operates in the 2.4 GHz frequency band as 802.11b. 802.11g devices are backward compatible with 802.11b devices.

802.11i

The IEEE standard for wireless security. 802.11i standard includes TKIP, CCMP, and AES encryption to improve wireless security. It is also know as WPA2.

802.1x

802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

Adhoc

A Peer-to-Peer wireless network. An Adhoc wireless network do not use wireless AP or router as the central hub of the network. Instead, wireless client are connected directly to each other. The disadvantage of Adhoc network is the lack of wired interface to Internet connections. It is not recommended for network more than 2 nodes.

Access Point (AP)

The central hub of a wireless LAN network. Access Points have one or more Ethernet ports that can connect devices (such as Internet connection) for sharing. Multi-function Access Point can also function as an Ethernet client, wireless bridge, or repeat signals from other AP. Access Points typically have more wireless functions comparing to wireless routers.

ACK Timeout

Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the Ack Window to timeout on lost packets. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks. Setting the correct ACK timeout value need to consider 3 factors: distance, AP response time, and interference. The G.DUO provide ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the G.DUO will automatically calculate the correct ACK timeout value.

Bandwidth Management (Traffic Control)

Bandwidth Management controls the transmission speed of a port, user, IP address, and application. Router can use bandwidth control to limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address - a crucial feature of QoS (Quality of Service) function.

Bootloader

Bootloader is the under layering program that will start at the power-up before the device loads firmware. It is similar to BIOS on a personal computer. When a firmware crashed, you might be able to recover your device from bootloader.

Bridge

A product that connects 2 different networks that uses the same protocol. Wireless bridges are commonly used to link network across remote buildings. For wireless application, there are 2 types of Bridges. WDS Bridge can be used in Point-to-Point or Point-to-Multipoint topology. Bridge Infrastructure works with AP mode to form a star topology.

Cable and Connector Loss: During wireless design and deployment, it is important to factor in the cable and connector loss. Cable and connector loss will reduce the output power and receiver sensitivity of the radio at connector end. The longer the cable length is, the more the cable loss. Cable loss should be subtracted from the total output power during distance calculation. For example, if the cable and connector loss is 3dBm and the output power is 20dBm; the output power at the cable end is only 17dBm.

Client

Client means a network device or utility that receives service from host or server. A client device means end user device such as wireless cards or wireless CPE.

CPE Devices

CPE stands for Customer Premises Equipment. A CPE is a device installed on the end user's side to receive network services. For example, on an ADSL network, the ADSL modem/router on the subscriber's home is the CPE device. Wireless CPE means a complete Wireless (usually an AP with built-in Antenna) that receive wireless broadband access from the WISP. The opposite of CPE is CO.

CTS

Clear To Send. A signal sent by a device to indicate that it is ready to receive data.

DDNS

Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. A router with DDNS capability has a built-in DDNS client that updates the IP address information to DDNS service provider whenever there is a change. Therefore, users can build website or other Internet servers even if they don't have fixed IP connection.

DHCP

Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it by DHCP server. A DHCP server can either be a designated PC on the network or another network device, such as a router.

DMZ

Demilitarized Zone. When a router opens a DMZ port to an internal network device, it opens all the TCP/UDP service ports to this particular device. The feature is used commonly for setting up H.323 VoIP or Multi-Media servers.

DNS

A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers.

Domain Name

The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. In www.airlive.com, the "airlive.com" is the doman name.

DoS Attack

Denial of Service. A type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

Encryption

Encoding data to prevent it from being read by unauthorized people. The common wireless encryption schemes are WEP, WPA, and WPA2.

ESSID (SSID)

The identification name of an 802.11 wireless network. Since wireless network has no physical boundary liked wired Ethernet network, wireless LAN needs an identifier to distinguish one network from the other. Wireless clients must know the SSID in order to associate with a WLAN network. Hide SSID feature disable SSID broadcast,
so users must know the correct SSID in order to join a wireless network.

Firewall

A system that secures a network and prevents access by unauthorized users. Firewalls can be software, router, or gateway. Firewalls can prevent unrestricted access into a network, as well as restricting data from flowing out of a network.

Firmware

The program that runs inside embedded device such as router or AP. Many network devices are firmware upgradeable through web interface or utility program.

FTP

File Transfer Protocol. A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Fragment Threshold

Frame Size larger than this will be divided into smaller fragment. If there are interferences in your area, lower this value can improve the performance. If there are not, keep this parameter at higher value. The default size is 2346. You can try 1500, 1000, or 500 when there are interference around your network.

Gateway

In the global Internet network, the gateways are core routers that connect networks in different IP subnet together. In a LAN environment with an IP sharing router, the gateway is the router. In an office environment, gateway typically is a multi-function device that integrates NAT, firewall, bandwidth management, and other security functions.

Hotspot

A place where you can access Wi-Fi service. The term hotspot has two meanings in wireless deployment. One is the wireless infrastructure deployment, the other is the Internet access billing system. In a hotspot system, a service provider typically need an authentication and account system for billing purposes, and a wireless AP network to provide access for customers.

IGMP Snooping

Internet Group Management Protocol (IGMP) is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP snooping is a feature that allows an Ethernet switch to "listen in" on the IGMP conversation between hosts and routers. A switch support IGMP snooping has the possibility to avoid multicast traffic being treated as broadcast traffic; therefore, reducing the overall traffic on the network.

Infrastructure Mode

A wireless network that is built around one or more access points to provide wireless clients access to wired LAN / Internet service. The opposite of Infrastructure mode is Adhoc mode.

IP address

IP (Internet Protocol) is a layer-3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

IPsec

IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

LACP (802.3ad) Trunking

The 802.3ad Link Aggregation standard defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both device must set the trunking feature to work.

MAC

Media Access Control. MAC address provides layer-2 identification for Networking Devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each manufacturer. When a network device have MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps

Megabits Per Second. One million bits per second; a unit of measurement for data transmission

MESH

Mesh is an outdoor wireless technology that uses Spanning Tree Protocol (STP) and Wireless Distribution system to achieve self-forming, self-healing, and self-configuring outdoor network. MESH network are able to take the shortest path to a destination that does not have to be in the line of site.

MIMO

Multi In Multi Out. A Smart Antenna technology designed to increase the coverage and performance of a WLAN network. In a MIMO device, 2 or more antennas are used to increase the receiver sensitivity and to focus available power at intended Rx.

NAT

Network Address Translation. A network algorithm used by Routers to enables several PCs to share single IP address provided by the ISP. The IP that a router gets from the ISP side is called Real IP, the IP assigned to PC under the NAT environment is called Private IP.

Node

A network connection end point, typically a computer.

Packet

A unit of data sent over a network.

Passphrase

Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for the company products.

POE

Power over Ethernet. A standard to deliver both power and data through one single Ethernet cable (UTP/STP). It allows network device to be installed far away from power ource. A POE system typically compose of 2 main component: DC Injector (Base Unit) and Splitter(Terminal Unit). The DC injector combines the power and data, and the splitter separates the data and power back. A PoE Access Point or CPE has the splitter built-in to the device. The IEEE 802.3af is a POE spec that uses 48 volt to deliver power up to 100 meter distance.

Port

This word has 2 different meaning for networking.

- The hardware connection point on a computer or networking device used for plugging in a cable or an adapter.
- The virtual connection point through which a computer uses a specific application on a server.

PPPoE

Point-to- Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.

PPTP

Point-to-Point Tunneling Protocol: A VPN protocol developed by PPTP Forum. With PPTP, users can dial in to their corporate network via the Internet. If users require data encryption when using the Windows PPTP client, the remote VPN server must support MPPE (Microsoft Point-To-Point Encryption Protocol) encryption. PPTP is also used by some ISP for user authentication, particularly when pairing with legacy Alcatel / Thomson ADSL modem.

Preamble Type

Preamble are sent with each wireless packet transmit for transmission status. Use the long preamble type for better compatibility. Use the short preamble type for better performance

Rate Control

Ethernet switches' function to control the upstream and downstream speed of an individual port. Rate Control management uses "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

RADIUS

Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Radius typically uses port 1812 and port 1813 for authentication and accounting port. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Receiver Sensitivity

Receiver sensitivity means how sensitive is the radio for receiving signal. In general; the slower the transmission speed, the more sensitive the radio is. The unit for Receiver Sensitivity is in dB; the lower the absolute value is, the higher the signal strength. For example, -50dB is higher than -80dB.

RJ-45

Standard connectors for Twisted Pair copper cable used in Ethernet networks. Although they look similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Router

An IP sharing router is a device that allows multiple PCs to share one single broadband connection using NAT technology. A wireless router is a device that combines the functions of wireless Access Point and the IP sharing router.

SIGNAL STRENGTH

Receiver Sensitivity Index. SIGNAL STRENGTH is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher SIGNAL STRENGTH values. For SIGNAL STRENGTH value, the smaller the absolute value is, the stronger the signal. For example, “-50db” has stronger signal than “-80dB”. For outdoor connection, signal stronger than -60dB is considered as a good connection.

RTS

Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

RTS Threshold

RTS (Request to Send). The RTS/CTS(clear to send) packet will be send before a frame if the packet frame is larger than this value. Lower this value can improve the performance if there are many clients in your network. You can try 1500, 1000 or 500 when there are many clients in your AP’s network.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. The SNMP network contains 3 key elements: managed devices, agents, and network-management systems (NMSs). Managed devices are network devices that content SNMP agents. SNMP agents are programs that reside SNMP capable device's firmware to provide SNMP configuration service. The NMS typically is a PC based software such as HP Openview that can view and manage SNMP network device remotely.

SSH
Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL
Secure Sockets Layer. It is a popular encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session. SSL VPN is also known as Web VPN. The HTTPS and SSH management interface use SSL for data encryption.

Subnet Mask
An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

Subnetwork or Subnet
Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

TCP
A layer-4 protocol used along with the IP to send data between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through
the Internet.

TX Output Power

Transmit Output Power. The TX output power means the transmission output power of the radio. Normally, the TX output power level limit for 2.4GHz 11g/b is 20dBm at the antenna end. The output power limit for 5GHz 802.11a is 30dBm at the antenna end..

UDP

User Datagram Protocol. A layer-4 network protocol for transmitting data that does not require acknowledgement from the recipient of the data.

Upgrade

To replace existing software or firmware with a newer version.

Upload

To send a file to the Internet or network device.

URL

Uniform Resource Locator. The address of a file located on the Internet.

VPN

Virtual Private Network. A type of technology designed to increase the security of information transferred over the Internet. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate network.

WAN

Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. A WAN port on the network device means the port (or wireless connection) that is connected to the Internet side of the network topology.

WEP

Wired Equivalent Privacy. A wireless encryption protocol. WEP is available in 40-bit (64-bit), 108-bit (128-bit) or 152-bit (Atheros proprietary) encryption modes.

Wi-Fi

Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the IEEE 802.11 standards. The governing body for Wi-Fi is called Wi-Fi Alliance (also known as WECA).

WiMAX

Worldwide Interoperability for Microwave Access. A Wireless Metropolitan Network technology that complies with IEEE 802.16 and ETSI Hiperman standards. The orginal 802.16 standard call for operating frequency of 10 to 66Ghz spectrum. The 802.16a amendment extends the original standard into spectrum between 2 and 11 Ghz. 802.16d increase data rates to between 40 and 70 Mbps/s and add support for MIMO antennas, QoS, and multiple polling technologies. 802.16e adds mobility features, narrower bandwidth (a max of 5 mhz), slower speed and smaller antennas. Mobility is allowed up to 40 mph.

WDS

Wireless Distribution System. WDS defines how multiple wireless Access Point or Wireless Router can connect together to form one single wireless network without using wired uplinks. WDS associate each other by MAC address, each device

WLAN

Wireless Local Area Network. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. The most popular standard for WLAN is the 802.11 standards.

WMM

Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM prioritize traffic\ on Voice-over-IP (VoIP), audio, video, and streaming media as well as traditional IP data over the AP.

WMS

Wireless Management System. An utility program to manage multiple wireless AP/Bridges.

WPA

Wi-Fi Protected Access. It is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption. The WPA-PSK utilizes pre-share key for encryption/authentication.

WPA2

Wi-Fi Protected Access 2. WPA2 is also known as 802.11i. It improves on the WPA security with CCMP and AES encryption. The WPA2 is backward compatible with WPA. WPA2-PSK utilizes pre-share key for encryption/authentication.