stations. All the communication is done from Client to Client without any Access Point involved. Ad Hoc networking must use the same SSID and channel for establishing the wireless connection.



In client mode, the device can't support the Router mode function include Firewall and WAN settings.

3. WDS

Wireless Distribution System, this mode serves as a wireless repeater, only devices with WDS function supported can connect to it, all the wireless clients can't survey and connect the device when the mode is selected.

4. AP+WDS

Support both AP and WDS functions, the wireless clients and devices with WDS function supported can survey and connect to it.

SSID:

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access point/bridges on a network or sub-network can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID.

Channel Number

Channel No.	Frequency	Country Domain	
1	2412	Americas, EMEA, Japan, and China	
2	2417	Americas, EMEA, Japan, and China	
3	2422	Americas, EMEA, Japan, Israel, and China	
4	2427	Americas, EMEA, Japan, Israel, and China	
5	2432	Americas, EMEA, Japan, Israel, and China	
6	2437	Americas, EMEA, Japan, Israel, and China	
7	2442	Americas, EMEA, Japan, Israel, and China	
8	2447	Americas, EMEA, Japan, Israel, and China	
9	2452	Americas, EMEA, Japan, Israel, and China	
10	2457	Americas, EMEA, Japan, and China	
11	2462	Americas, EMEA, Japan, and China	
12	2467	EMEA and Japan only	
13	2472	EMEA and Japan only	

The following table is the available frequencies (in MHz) for the 2.4-GHz radio:

14	2484	Japan only

When set to "Auto", the device will find the least-congested channel for use.

Associated Client

Show the information of active wireless client stations that connected to the device.

Advanced Settings

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your device. The default setting is optimized for the normal operation. For specific application, setting configuration will required highly attention to reach optimistic condition.

<u>Note</u>: Any unreasonable value change to default setting will reduce the throughput of the device.

	Wireless	LAN Series			
	Wireless Adv	anaod Sattings			
	WIRELESS Advanced Settings These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.				
 ➡ Wizard ➡ Operation Mode ➡ Wireless ➡ Basic Settings 					
실 ····································	Authentication Type:	○ Open System ○ Shared Key			
WDS settings	Fragment Threshold:	2346 (256-2346)			
Site Survey	RTS Threshold:	2347 (0-2347)			
Tirewall	Beacon Interval:	100 (20-1024 ms)			
- 🛄 Management 	Data Rate:	Auto 🐱			
	Preamble Type:	Ostant Preamble ○ Short Preamble			
	Broadcast SSID:	Enabled O Disabled			
	IAPP:	Enabled Obisabled			
	802.11g Protection:	Enabled Obisabled			
	Block WLAN Relay:	○ Enabled ⊙ Disabled			
	Transmit Power(OFDM)	⊙ 100mW(20dBm) ○ 50mW(17dBm)			
	Transmit Power(CCK):	⊙ 250mW(24dBm)			
		○200mW(23dBm)			
		○150mW(21dBm)			
		○ 100mW(20dBm)			

Authentication Type

The device supports two Authentication Types "Open system" and "Shared Key". When you select "Share Key", you need to setup "WEP" key in "Security" page (See the next section). The default setting is "Auto". The wireless client can associate with the device by using one of the two types.

Fragment Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. This function will help you to improve the network performance.

RTS Threshold

The RTS threshold determines the packet size at which the radio issues a request to send (RTS) before sending the packet. A low RTS Threshold setting

can be useful in areas where many client devices are associating with the device, or in areas where the clients are far apart and can detect only the device and not each other. You can enter a setting ranging from 0 to 2347 bytes.

Data Rate

The standard IEEE 802.11b/11g supports 1, 2, 5.5,11/6, 9, 12, 18, 24, 36, 48 and Mbps data rates. You can choose the rate that the device uses for data transmission. The default value is "auto". The device will use the highest possible selected transmission rate.

Beacon Interval

The beacon interval is the amount of time between access point beacons in microseconds. The default beacon interval is 100.

Broadcast SSID

Broadcasting the SSID will let your wireless clients find the device automatically. If you are building a public Wireless Network, disable this function can provide better security. Every wireless stations located within the coverage of the device must connect this device by manually configure the SSID in your client settings.

Int. Roaming

This function will let Wireless Stations roam among a network environment with multiple devices. Wireless Stations are able to switch from one device to another as they move between the coverage areas. Users can have more wireless working range. An example as the following figure

You should comply with the following instructions to roam among the wireless coverage areas.

Note :	For implementing the roaming function, the setting MUST comply the		
	foll	owing two items.	
	•	All the devices must be in the same subnet network and the SSID must be the same.	
	•	If you use the 802.1x authentication, you need to have the user profile in these devices for the roaming station.	



Block WLAN Relay (Isolate Client)

The device supports isolation function. If you are building a public Wireless Network, enable this function can provide better security. The device will block packets between wireless clients (relay). All the wireless clients connected to the device can't see each other.

Transmit Power

The device supports four transmission output power levels 250, 200, 150 and 100mW for CCK (802.11b) mode and two transmission output power levels 100 and 50mW for OFDM (802.11g) mode. User can adjust the power level to change the coverage of the device. Every wireless stations located within the coverage of the device also needs to have the high power radio. Otherwise the wireless stations only can survey the device, but can't establish connection with device.

Configuring Wireless Security

This device provides complete wireless security function include WEP, 802.1x, WPA-TKIP, WPA2-AES and WPA2-Mixed in different mode (see the Security Support Table).

The default security setting of the encryption function is disabled. Choose your preferred security setting depending on what security function you need.

	Wireless LAN Series
Site contents: Wizard Operation Mode Wireless Advanced Settings Security Control WDS settings Site Survey TCP/IP Firewall Management Reboot	Wireless Security Setup This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
	Encryption: None SetWEP Key Use 802.1x Authentication Enable MAC Authentication WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key) Pre-Shared Key Format: Passphrase Pre-Shared Key: Enable Pre- Authentication
	Authentication RADIUS Server: Port 1812 IP address Password Note: When encryption WEP is selected, you must set WEP key value. Apply Changes Reset

WEP Encryption Setting

Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. The WEP setting must be as same as each client in your wireless network. For more secure data transmission, you can change encryption type to "WEP" and click the "Set WEP Key" button to open the "Wireless WEP Key setup" page.

Encryption:	WEP	~	SetWEP	Key				
Use 802.7	Ix Authentic IAC Authent	ation tication	VVEP 64b	its OW	EP 128	3bits		
WPA Auther	ntication Mo	de:	Enterprise	(RADIUS) 💿	Personal	l (Pre-S	hared Key)
Pre-Shared	Key Format	: [^D assphrase		2			
Pre-Shared	Key:							
Enable I Authenticati	Pre- on							
Authenticati Server:	on RADIUS	F	ort 1812	IP addr	ess		F	assword

When you decide to use the WEP encryption to secure your WLAN, please

refer to the following setting of the WEP encryption:

- 64-bit WEP Encryption : 64-bit WEP keys are as same as the encryption method of 40-bit WEP. You can input 10 hexadecimal digits (0~9, a~f or A~F) or 5 ACSII chars.
- 128-bit WEP Encryption : 128-bit WEP keys are as same as the encryption method of 104-bit WEP. You can input 26 hexadecimal digits (0~9, a~f or A~F) or 10 ACSII chars.
- The Default Tx Key field decides which of the four keys you want to use in your WLAN environment.

IEP Key Setup - Microsoft	Internet Explorer	
Wireless WE	P Key Setup	
This page allows you setup key, and select ASCII or H	o the WEP key value. You could choose use 64-bit or 128-bit as the encryption lex as the format of input value.	
Key Length:	64-bit 🗸	
Key Format:	Hex (10 characters)	
Default Tx Key:	Key 1 🐱	
Encryption Key 1:	******	
Encryption Key 2:	*****	
Encryption Key 3:	******	
Encryption Key 4:	*****	
Apply Changes	Close Reset	

WEP Encryption with 802.1x Setting

The device supports external RADIUS Server that can secure networks against unauthorized access. If you use the WEP encryption, you can also use the RADIUS server to check the admission of the users. By this way every user must use a valid account before accessing the Wireless LAN and requires a RADIUS or other authentication server on the network. An example is shown as following.



You should choose WEP 64 or 128 bit encryption to fit with your network environment first. Then add user accounts and the target device to the RADIUS server. In the device , you need to specify the IP address Password (Shared Secret) and Port number of the target RADIUS server.

Encryption: WEP	Set WEP Key			
Use 802.1x Authentication WEP 64bits WEP 128bits 				
Enable MAC Authenticatio	n			
WPA Authentication Mode:	Enterprise (RADIUS)			
Pre-Shared Key Format:	Passphrase			
Pre-Shared Key:				
Enable Pre- Authentication				
Authentication RADIUS Server:	Port 1812 IP address 192.168.2.205 Password			

WPA Encryption Setting

WPA feature provides a high level of assurance for end-users and administrators that their data will remain private and access to their network restricted to authorized users. You can choose the WPA encryption and select the Authentication Mode.

WPA Authentication Mode

This device supports two WPA modes. For personal user, you can use the Pre-shared Key to enhance your security setting. This mode requires only an access point and client station that supports WPA-PSK. For Enterprise, authentication is achieved via WPA RADIUS Server. You need a RADIUS or other authentication server on the network.

• Enterprise (RADIUS):

When WPA Authentication mode is Enterprise (RADIUS), you have to add user accounts and the target device to the RADIUS Server. In the device, you need to specify the IP address

Password (Shared Secret) and Port number of the target RADIUS server.

• Pre-Share Key:

This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8~63 ACSII chars. When Key format is Hex, the key value should have 64 hexadecimal digits (0~9, a~f or A~F).

Configuring as WLAN Client Adapter

This device can be configured as a wireless Ethernet adapter. In this mode, the device can connect to the other wireless stations (Ad-Hoc network type) or Access Point (Infrastructure network type) and you don't need to install any driver.

Quick start to configure

Step 1. In "Basic Settings" page, change the Mode to "Client" mode. And key in the SSID of the AP you want to connect then press "Apply Changes" button to apply the change.

Wireless LAN Series				
Site contents: Wizard Operation Mode Wireless Security Advanced Settings Security Access Control WDS settings Ste Survey TCP/IP Firewall Management E Reboot	Wireless Basic Settings This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters. Disable Wireless LAN Interface Band: 2.4 GHz (B+G) • Mode: 2.1 Client • Network Type: Infrastructure • SSID: 3. Target-AP-SSID Channel Number: 11 • Associated Clients: Show Active Clients Imable Mac Clone (Single Ethernet Client) Apply Changes			

Step 2. Check the status of connection in "Status" web page

	Wireles	s LAN Series
Site contents: Wizard Operation Mode Wireless TCP/IP Firewall Status Status DDNS DDNS Log Log Save/Reload Setting Password Reboot	System Uptime Free Memory Firmware Version Webpage Version Wireless Configuratio Mode Band SSID Channel Number Encryption BSSID State RSSI TCP/IP Configuration Attain IP Protocol IP Address Subnet Mask Default Gateway DHCP Server	Oday:1h:13m:5s 2292 kB v1.2.1 v1.2.1 Infrastructure Client - Bridge 2.4 GHz (B+G) Target-AP-SSID 5 Disabled 09-09-09-09-09-09 Scanning 0 Fixed IP 192.168.2.254 265.265.265.0 192.188.2.254 Enabled 09.01.01.01.01.01
	inde duuless	00.00.00.00.01

The alternative way to configure as following:

Step 1. In "Wireless Site Survey" page, select one of the SSIDs you want to connect and then press "Connect" button to establish the link.

	Wirele	ess LAN Ser	ies				
Site contents:	Wireless S This page provides to found, you could cho	ite Survey ol to scan the wireless ose to connect it manu	network. ally when	lf any A client r	Access Po node is er	int or IE nabled.	3SS is
Advanced Settings	SSID	BSSID	Channel	Туре	Encrypt	Signal	Select
Access Control	Mercy_CA_SSID	00:0d:14:00:80:18	9 (B+G)	AP	no	100	0
VDS settings	ZPlus-G192-DEV1	00:00:00:04:27:28	11 (B+G)	AP	no	120	۲
	ZPlus-G192-DEV2	00:00:00:04:26:92	11 (B+G)	AP	no	81	0
Firewall Management	Zinwell	00:05:9e:80:01:f8	1 (B)	AP	no	80	0
E Reboot	linksys	00:06:25:d7:c3:97	6 (B+G)	AP	no	73	0
	ZPlus-G192	00:aa:ee:ff:99:01	11 (B+G)	AP	no	67	0
	DFC-test	00:05:9e:80:46:3b	1 (B)	AP	no	32	0
	Refresh 3. Con	nect					

Step 2. If the linking is established successfully. It will show the message "Connect successfully". Then press "OK".



Step 3. Then you can check the linking information in "Status" page.

	Wireles	s LAN Series
Site contents: Vizard Operation Mode Vireless TCP/IP Firewall Status Status Statistics DDNS CDNS Content Status DDNS Content Content	System Uptime Free Memory Firmware Version Webpage Version Wireless Configuratio Mode Band SSID Channel Number Encryption	Oday:1h:24m:22s 1932 kB v1.2.1 v1.2.1 Infrastructure Client - Bridge 2.4 GHz (B+G) ZPlus-G192-DEV1 11 Disabled
Password	BSSID	00:00:00:04:27:28
Reboot	State RSSI	Connected 100
	TCP/IP Configuration	
	Attain IP Protocol IP Address Subnet Mask Default Gateway DHCP Server	Fixed IP 192.168.2.254 255.255.255.0 192.168.2.254 Enabled
	MAC Address	00:00:aa:bb:dd:91

Note :

If the available network requires authentication and data encryption, you need to setup the authentication and encryption before step1 and all the settings must be as same as the Access Point or Station. About the detail authentication and data encryption settings, please refer the security section.

Authentication Type

In client mode, the device also supports two Authentication Types "Open system" and "Shared Key". Although the default setting is "Auto", not every Access Points can support "Auto" mode. If the authentication type on the Access Point is knew by user, we suggest to set the authentication type as same as the Access Point.

Data Encryption

In client mode, the device supports WEP and WPA Personal/Enterprise except WPA2 mixed mode data encryption. About the detail data encryption settings, please refer the security section.

Chapter 3 - Configuring WDS

Wireless Distribution System (WDS) uses wireless media to communicate with the other devices, like the Ethernet does. This function allows one or more remote LANs connect with the local LAN. To do this, you must set these devices in the same channel and set MAC address of other devices you want to communicate with in the WDS AP List and then enable the WDS.

When you decide to use the WDS to extend your WLAN, please refer the following instructions for configuration.

- The bridging devices by WDS must use the same radio channel.
- When the WDS function is enabled, all wireless stations can't connect the device.
- If your network topology has a loop, you need to enable the 802.1d Spanning Tree function.
- You don't need to add all MAC address of devices existed in your network to WDS AP List. WDS AP List only needs to specify the MAC address of devices you need to directly connect to.
- The bandwidth of device is limited, to add more bridging devices will split the more bandwidth to every bridging device.

WDS network topology

In this section, we will demonstrate the WDS network topologies and WDS AP List configuration. You can setup the four kinds of network topologies: bus, star, ring and mesh.

In this case, there are five devices with WDS enabled: WDS1, WDS2, WDS3, WDS4 and WDS5.



Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Address of WDS2	No
WDS2	The MAC Addresses of WDS1 and WDS3	No
WDS3	The MAC Addresses of WDS2 and WDS4	No
WDS4	The MAC Addresses of WDS3 and WDS5	No
WDS5	The MAC Address of WDS4	No

Bus topology :

Star topology :



Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4	Νο
	and WDS5	
WDS2	The MAC Address of WDS1	Νο
WDS3	The MAC Address of WDS1	Νο
WDS4	The MAC Address of WDS1	Νο
WDS5	The MAC Address of WDS1	Νο

Ring topology :



Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2 and WDS5	Yes
WDS2	The MAC Addresses of WDS1 and WDS3	Yes
WDS3	The MAC Addresses of WDS2 and WDS4	Yes
WDS4	The MAC Addresses of WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS4 and WDS1	Yes

Mesh topology :



Device	Entries of WDS AP List	Spanning Tree
		Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	Yes
WDS2	The MAC Addresses of WDS1, WDS3, WDS4 and WDS5	Yes
WDS3	The MAC Addresses of WDS1, WDS2, WDS4 and WDS5	Yes
WDS4	The MAC Addresses of WDS1, WDS2, WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS1, WDS2, WDS3 and WDS4	Yes

WDS Application

Wireless Repeater

Wireless Repeater can be used to increase the coverage area of another device (Parent AP). Between the Parent AP and the Wireless Repeater, wireless stations can move among the coverage areas of both devices. When you decide to use the WDS as a Repeater, please refer the following instructions for configuration.

- In AP mode, enable the WDS function.
- You must set these connected devices with the same radio channel and SSID.
- Choose "WDS+AP" mode.
- Using the bus or star network topology.



Description	Entries of WDS AP List	Spanning Tree Protocol Required
Access Point	The MAC Address of Repeater	Yes
Repeater	The MAC Address of Access Point	Yes

Wireless Bridge

Wireless Bridge can establish a wireless connection between two or more Wired LANs. When you decide to use the WDS as a Wireless Bridge, please refer the following instructions for configuration.

- In AP mode, enable the WDS function.
- You must set these connected devices with the same radio channel, but you may use different SSID.
- Choose "WDS" mode for only wireless backbone extension purpose.
- You can use any network topology, please refer the WDS topology section.

Chapter 4 - Advanced Configurations

Configuring LAN to WAN Firewall

Filtering function is used to block packets from LAN to WAN. The device supports three kinds of filter Port Filtering, IP Filtering and MAC Filtering. All the entries in current filter table are used to restrict certain types of packets from your local network to through the device. Use of such filters can be helpful in securing or restricting your local network.

Port Filtering

When you enable the Port Filtering function, you can specify a single port or port ranges in current filter table. Once the source port of outgoing packets match the port definition or within the port ranges in the table, the firewall will block those packets from LAN to WAN.

Wireless LAN Series					
Site contents: Wizard Operation Mode Wireless Firswall Firswall Firswall MAC Filtering MAC Filtering MAC Filtering DMZ VPN Management Reboot	Port Filtering Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network. Enable Port Filtering Port Range: - Port Range: - Apply Changes Reset				
	Current Filter Table: Port Range Protocol Comment Select				
	Delete Selected Delete All Reset				

IP Filtering

When you enable the IP Filtering function, you can specify local IP Addresses in current filter table. Once the source IP address of outgoing packets match the IP Addresses in the table, the firewall will block this packet from LAN to WAN.

	Wireless LAN Series
Site contents: Vizard Operation Mode Vireless TCP/IP Port Filtering Port Filtering Port Forwarding Port Forwarding Port Forwarding DMZC Filtering DMZC Filtering Content MAC Filtering Port Forwarding Content Port Forwarding Reboot	IP Filtering Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network. Image:

MAC Filtering

When you enable the MAC Filtering function, you can specify the MAC Addresses in current filter table. Once the source MAC Address of outgoing packets match the MAC Addresses in the table, the firewall will block this packet from LAN to WAN.

	Wireless LAN Series
Site contents: Wizard Operation Mode Wireless FIFewall Port Filtering Port Filtering Port Filtering Port Forwarding DMZ DMZ VPN Management Reboot	MAC Filtering Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network. Enable MAC Filtering MAC Address: Comment: Apply Changes Reset Current Filter Table: Comment Delete Selected Delete All

Configuring Port Forwarding (Virtual

Server)

This function allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind the device's NAT firewall.

	Wireless LAN Series
Site contents: Wizard Operation Mode Wireless TCP/IP Frewall Port Filtering Port Filtering Port Forwarding Port Port Port Port Port Port Port Port	Port Forwarding Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall. Enable Port Forwarding IP Address: Protocol: Both Port Range: . Comment: . <t< th=""></t<>

The most often used port numbers are shown in the following table.

Services	Port Number	
ECHO	7	

FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer Protocol)	80
POP3 (Post Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
SIP (Session Initiation Protocol)	5060
PPTP (Point-to-Point Tunneling Protocol)	1723

Multiple Servers behind NAT Example:

In this case, there are two PCs in the local network accessible for outside users.



Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.2.1	TCP+UDP	80	Web Server	
192.168.2.2	TCP+UDP	21	FTP Server	
Delete Selected	Delete All R	eset		

Configuring DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. So that all inbound packets will be redirected to the computer you set. It also is useful while you run some applications (ex. Internet game) that use uncertain incoming ports.

	Wireless LAN Series
Site contents: Wizard Geration Mode Wireless TCP/IP Firewall Firewall Firewall Fort Filtering Firewall Fort Fortwarding Fort Forwarding Fort Forwarding Forwarding Fort Forwarding Fort Forwarding Forwarding Fort Forwarding	A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. Enable DMZ DMZ Host IP Address: Apply Changes Reset

Enable DMZ:

Enable the "Enable DMZ", and then click "Apply Changes" button to save the changes.

DMZ Host IP Address:

Input the IP Address of the computer that you want to expose to Internet.



DNS Host

Device with Router Mode enabled

Configuring WAN Interface

The device supports four kinds of IP configuration for WAN interface, including Static IP, DHCP Client, PPPoE and PPTP. You can select one of the WAN Access Types depend on your ISP required. The default WAN Access Type is "Static IP".

Wireless LAN Series			
Site contents: Wizard Wireless LAN Interface WAN Interface Kirwall Management Reboot	WAN Interface This page is used to cor port of your Access Poin PPPoE or PPTP by clicit WAN Access Type: IP Address: Subnet Mask: Default Gateway: DNS 1: DNS 2: DNS 3: Clone MAC Address:	Static IP 172.1.1.1 255.255.0 172.1.1.254 000000000000	
	Enable Web Serv Apply Changes	Reset	

Static IP

You can get the IP configuration data of Static-IP from your ISP. And you will need to fill the fields of IP address, subnet mask, gateway address, and one of the DNS addresses.

	Wireless LAN Series
Site contents:	WAN Interface Setup
→ 🗳 Wizard – 🗳 Operation Mode – ● Wireless – ● TCP/IP	This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
LAN Interface	WAN Access Type: Static IP
Management	IP Address: 172.1.1.1
Reboot	Subnet Mask: 255.255.255.0
	Default Gateway: 172.1.1.254
	DNS 1:
	DNS 2:
	DNS 3:
	Clone MAC Address: 00000000000
	Enable uPNP
	Enable Web Server Access on WAN
	Apply Changes Reset
IP Address: Subnet Mask:	Ine Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier besides your local network. The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached
Default Gateway:	through a gateway. The IP address of Default Gateway provided by your ISP or MIS. Default Gateway is the intermediate network device that has knowledg of the network IDs of the other networks in the Wide Area Network, so can forward the packets to other gateways until they are delivered to the one connected to the specified destination
DNS 1~3:	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses ar map the domain names in your Internet requests to other servers on th Internet until the specified web site is found.
Clone MAC Address: Enable uPnP:	Clone device MAC address to the specify MAC address required by yo ISP Enable uPnP, this function allows the device to be found and configure

DHCP Client (Dynamic IP)

All IP configuration data besides DNS will obtain from the DHCP server when DHCP-Client WAN Access Type is selected.

	Wireless LAN Series
Site contents: Wirzard Operation Mode Wireless LAN Interface LAN Interface Firewall Management Reboot	WAN Interface Setup This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Prover you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type. WAN Access Type: DHCP Client Attain DNS Automatically • Set DNS Manually DNS 1: DNS 2: DNS 3: Clone MAC Address: 0000000000 Enable uPNP Clonel Web Server Access on WAN
DNS1~3:	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to I addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet request to other servers on the Internet until the specified web site is found.
Clone MAC Address:	Clone device MAC address to the specify MAC address require by your ISP
Enable uPnP:	Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

PPPoE

When the PPPoE((Point to Point Protocol over Ethernet) WAN Access Type is selected, you must fill the fields of User Name, Password provided by your ISP. The IP configuration will be done when the device successfully authenticates with your ISP.

	Wireless LAN Series
Site contents:	
Wizard Operation Mode Wireless	This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
TCP/IP	WAN Access Type: PPPoE
Firewall	User Name:
E Reboot	Password:
	Connection Type: Continuous Connect Disconnect
	Idle Time: 5 (1-1000 minutes)
	MTO Size: (1400-1492 bytes)
	© Set DNS Manually
	DNS 1:
	DNS 2:
	DNS 3:
	Clone MAC Address: 0000000000
	Enable uPNP
Jser Name:	The account provided by your ISP
assword:	The password for your account.
Connect Type:	"Continuous " : connect to ISP permanently
	"Manual" : Manual connect/disconnect to ISP
	"On-Demand" : Automatically connect to ISP when user access the Internet.
Idle Time:	The number of inactivity minutes to disconnect from ISP setting is only available when "Connect on Demand" cor
	type is selected.
MTU Size:	Maximum Transmission Unit, 1412 is the default setting need to change the MTU for optimal performance with yo ISP.
DNS1~3:	The IP addresses of DNS provided by your ISP.
	DNS (Domain Name Server) is used to map domain nar addresses. DNS maintain central lists of domain name/l addresses and map the domain names in your Internet other servers on the Internet until the specified web site
Clone MAC Address:	Clone device MAC address to the specify MAC address by your ISP.
Enable uPnP:	Enable uPnP, this function allows the device to be found configured automatically by the system. (Ex. Window XF

PPTP

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only

Site contents:	This page is used to cor port of your Access Poir PDPDE or PDTP by slice	The second secon
- ≌ Wizard - ≌ Operation Mode - ■ Wireless - ■ TCP/IP	WAN Access Type:	
LAN Interface	IP Address:	172.1.1.2
- Firewall	Subnet Mask:	255.255.255.0
Management	Server IP Address:	172.1.1.1
	User Name:	
	Password:	
	MTU Size:	1412 (1400-1492 bytes)
	O Attain DNS Autom	atically
	Set DNS Manually	
	DNS 1:	
	DNS 2:	
	DNS 3:	
	Clone MAC Address:	0000000000
	Enable uPNP	
	Enable Web Sen	ver Access on WAN

IP Address:	The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier besides your local network.
Subnet Mask:	The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.
Server IP Address:	The IP address of PPTP server
(Default Gateway)	
User Name:	The account provided by your ISP
Password:	The password of your account
MTU Size:	Maximum Transmission Unit, 1412 is the default setting, you may need to change the MTU for optimal performance with your specific ISP.
DNS1~3:	The IP addresses of DNS provided by your ISP.
	DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
Clone MAC Address:	Clone device MAC address to the specify MAC address required by your ISP.
Enable uPnP:	Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

Configuring Clone MAC Address

The device provides MAC address clone feature to fit the requirement of some ISP need to specify the client MAC address.

Physical WAN interface MAC Address clone

1. Clone MAC address for DHCP Client WAN access type

	Wireless LAN Series
Site contents:	WAN Interface Setup This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type. WAN Access Type: DHCP Client O Attain DNS Automatically Set DNS Manually DNS 1:

2. Clone MAC address for Static IP WAN access type

	Wireles	ss LAN Series
Site contents: Wizard Operation Mode Wireless TCP/IP LAN Interface	WAN Interfa This page is used to cc port of your Access Po PPPoE or PPTP by clin	ace Setup onfigure the parameters for Internet network which connects to the WAN int. Here you may change the access method to static IP, DHCP, ck the item value of WAN Access type.
📑 WAN Interface	WAN Access Type:	Static IP
Management	IP Address:	172.1.1.1
- B Kepool	Subnet Mask:	255.255.255.0
	Default Gateway:	172.1.1.254
	DNS 1:	
	DNS 2:	
	DNS 3:	
	Clone MAC Address:	001122334455
	Enable uPNP Enable Web Ser Apply Changes	ver Access on WAN

3. Clone MAC address for PPPoE WAN access type

	Wireless	s LAN Series
Site contents: Wizard Operation Mode Wireless TCP/IP LAN Interface	WAN Interface This page is used to conf port of your Access Point PPPoE or PPTP by click	se Setup figure the parameters for Internet network which connects to the WAN t. Here you may change the access method to static IP, DHCP, k the item value of WAN Access type.
 ➡ Firewall ➡ Management ➡ Reboot 	WAN Access Type: User Name: 87 Password: • Connection Type: C Idle Time: 5 MTU Size: 14	PPPoE
	Attain DNS Automa Set DNS Manually DNS 1: DNS 2: DNS 3: Clone MAC Address: Enable uPNP	(1400-1402 b)(85)

4. Clone MAC address for PPTP WAN access type

Site contents:	This page is used to co port of your Access Poi PPPoE or PPTP by clic	nfigure the parameters for Internet network which connects to the WA nt. Here you may change the access method to static IP, DHCP, ck the item value of WAN Access type.
■ Operation Mode ■ Wireless ■ CCP/IP	WAN Access Type:	PPTP
LAN Interface	IP Address:	172.1.1.2
Firewall	Subnet Mask:	255.255.255.0
E Reboot	Server IP Address:	172.1.1.1
	User Name:	
	Password:	
	MTU Size:	1412 (1400-1492 bytes)
	Attain DNS Autom	atically
	○ Set DNS Manually	
	DNS 1:	
	DNS 2:	
	DNS 3:	
	Clone MAC Address:	001122334455

Site contents: Wizard Operation Mode Wireless TCPJIP	LAN Interfac This page is used to con the device. Here you may etc	e Setup figure the parameters for local area network which connect _y change the setting for IP addresss, subnet mask, DHCP
WAN Interface ► WAN Interface Firewall Management Reboot	IP Address: Subnet Mask: Default Gateway: DHCP: DHCP Client Range: 802.1d Spanning Tree Clone MAC Address:	192.168.3.254 255.255.255.0 0.0.0 Server 192.168.3.1 ■ 192.168.3.253 Show Client 001122334455

5. Physical LAN interface MAC address clone

Configuring DHCP Server

- 1. To use the DHCP server inside the device, please make sure there is no other DHCP server existed in the same network as the device.
- 2. Enable the DHCP Server option and assign the client range of IP addresses as following page.

Wireless LAN Series		
Site contents:	LAN Interface Setup This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP addresss, subnet mask, DHCP, etc	
	IP Address: Subnet Mask: Default Gateway: DHCP: DHCP Client Range: 802.1d Spanning Tree: Clone MAC Address:	192.168.3.254 255.255.05 0.0.0 Server 192.168.3.1 Disabled 001122334455

3. When the DHCP server is enabled and also the device router mode is enabled then the default gateway for all the DHCP client hosts will set to the IP address of device.

Using CLI Menu

Start a SSH(Secure Shell) client session to login the device

The SSH server daemon inside device uses well-known TCP port 22. User must use SSH client utility such like Putty to login the device. The default password for user "root" is "qwert", once user login the device then can change the password by CLI command.

Execute CLI program

This program won't execute automatically when user login the device. User must manually execute it by typing the case-sensitive command "cli". Please note that any modified settings won't save permanently until user "Apply Changes to Flash" or reboot it. The new settings modified by CLI will take effect after rebooting the device.

Menu Tree List

	A. Basic Settings		
	B. Advanced Settings		
	C. Security Settings		
	D. Access Control Settings		
	E WDS Settings		
	0 Fxit		
	A ID Address :102 168 2 2		
	P. Sylwast Mode 255 255 0		
	C. Default Cataman 102 168 2 2		
A. Operation Mode	D. DUCD Excelled		
	D. DHCP :Enabled		
B. Wireless Setting	E. DHCP Client Range :192.168.2.100 ~~ 192.168.2.200		
	F. 802.1d Spanning Tree:Disabled		
C. TCP/IP-LAN Setting	G. Clone MAC Address :00000000000		
	0. Exit		
D. TCP/IP-WAN Setting	A WAN Tupo DDDoE		
	A. WAIN Type		
E. Firewall Setting	D. Osei Ivaille .87043009@illitet.itet		
J	C. Password :2xsssssd		
G. Management	D. Connection Type : Continous		
	E. MTU Size :1412 (1400-1492 bytes)		
H Apply Changes to Flash	F. DNS Mode :Auto		
II. rippiy changes to I hash	Y. Clone MAC Address :00000000000		
L Deheet to take offect	Z. uPNP :Disabled		
I. Reboot to take effect	0. Exit		
0			
0. Exit	A. Port Filtering: Disabled		
	B. IP Filtering: Disabled		
	C MAC Filtering Disabled		
	D. Port Forwarding: Disabled		
	E DMZ:Disabled		
	U. LAR		
	A. Access Point Status		
	B Password		
	0 Exit		
	U. LAR		

The System Management

Password Protection

Both Web-Browser and SSH configuration interfaces have password protection.

Wireless LAN Series				
Site contents: Wizard Operation Mode Wireless Firewall Management Status Statistics DDNS DDNS DDNS Upgrade Firmware Save/Reload Setting Password Behont	Password Setup This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection. User Name: New Password: Confirmed Password: Apply Changes Reset			

To disable the Web-Browser password protection just leave the "User Name" field to blank then click "Apply Changes" button.



To change the password of user "root" for SSH session, please use the CLI menu item G. System Setting \rightarrow A. Root Password

About SNMP Agent

This device is compatible with SNMP v1/v2c and provide standard MIB II. Currently only the "public" community string is available and the modified settings by SNMP SET request will be lost after rebooting the device.

Firmware Upgrade

Firmware Types

The firmware for this device is divided into 2 parts, one is web pages firmware the other is application firmware, and the naming usually are g192webpage.bin and g192linux.bin. To upgrade firmware, we suggest user first upgrade the application firmware then web pages firmware. Upgrading Firmware

The Web-Browser upgrading interface is the simplest and safest way for user, it will check the firmware checksum and signature, and the wrong firmware won't be accepted. After upgrading, the device will reboot and please note that depends on the version of firmware, the upgrading may cause the device configuration to be restored to the factory default setting, and the original configuration data will be lost! To upgrade firmware, just assign the file name with full path then click "Upload" button as the following page.

Memory Limitation

To make sure the device have enough memory to upload firmware, the system will check the capacity of free memory, if the device lack of memory to upload firmware, please temporarily turn-off some functions then reboot the device to get enough memory for firmware uploading.

	Wireless LAN Series
Site contents: Site contents:	Upgrade Firmware This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system. If free memory is not enough for uploading, please temporarily turn off some functions such like Log/IPsec Select File: c:\img\g192linux.bin Browse Upload Reset

Configuration Data Backup & Restore

Rest Setting to Factory Default Value

Since the device is designed for outdoor used, there is no interface outside the housing to reset the configuration value to the factory default value. The device provides the Web-Browser interface to rest the configuration data. After resetting it, the current configuration data will be lost and restored to factory default value.

Saving & Restoring Configuration Data

Wireless LAN Series				
Site contents:	Save/Reload	Settings		
Viizard Viizard Operation Mode Vireless TCP/IP	This page allows you save which was saved previousl factory default.	current settings to a file or reload the settings from the file y. Besides, you could reset the current configuration to		
Management Status Estatistics	Save Settings to File: Load Settings from File:	Save Browse Upload		
- 딸 Time Zone - 딸 Log - 안 Upgrade Firmware - 딸 Save/Reload Setting	Reset Settings to Default:	Reset		
Password Reboot				

To save & restore configuration data of device, just assign the target filename with full path at your local host, then you can backup configuration data to local host or restore configuration data to the device.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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

FCC Radiation Exposure Statement:

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