# **Connecting Profile**

Site contents:	Connecting Profile Settings -wlan2
<ul> <li>Wizard</li> <li>Operation Mode</li> <li>Wireless</li> <li>Wian1</li> <li>Wan2</li> <li>Basic Settings</li> <li>Advanced Setting</li> <li>Security</li> <li>Access Control</li> <li>WDS settings</li> <li>Site Survey</li> <li>Connecting Profile</li> </ul>	Enable the connecting profile in clinet mode, the system will check the preferred SSID and BSSID in a fixed period, if preferred APs are found, the radio will try to connect with them one by one and regardless of the signal quality and strength. Please note that check the preferred APs will impact the throughput a lot ! Unless the signal strength is good enough, otherwise don't set the interval too short. And currently ,all the profiles share the same security setting.
	Enable connecting profile  SSID:  Apply Changes Reset
Management	Checking Interval: 10 (5-1440 minutes)
	Current preferred AP list:
	SSID BSSID Select
	Test AP 1 00:00:00:00
	Delete Selected Delete All Reset

To enable this function, this device must be in the client mode. User clicks to enable this function and input the SSID of preferred AP and then click "Apply Changes". The BSSID field is an option in case of two preferred APs having the same SSID. In this case, this device will check both SSID and BSSID and connect to the matching AP. We can leave it empty in the normal case.

After enabling the connecting profile, the system will check the preferred SSID in a fixed period. If preferred APs are found, the radio will try to connect with them one by one from top to down of the list and regardless of the signal quality and strength. The users can put their most favorite AP on the top so it will be connected first. Please note that check the preferred APs will impact the throughput a lot! Unless the signal strength is good enough, otherwise don't set the interval too short. The default value is 10 minutes. And currently, all the profiles share the same security setting.



To delete one SSID in the list, users click the square to select it and click "Delete Selected" and then click "OK" in the pop-up window to confirm it. The user can delete the whole list once for all! Just click "Delete All" and then click "OK" in the pop-up window to confirm it.

To simply disable this function, the user just clicks to disable "Enable connecting profile". The preferred AP list will be preserved for the next use.

# **MAC Clone for Single Ethernet Client**

Enable/Disable Mac Clone (Single Ethernet Client) in Wireless-Basic Settings page determines whether the Ethernet Client use it's own MAC address or AP-Client's MAC address to transmit data. Enable MAC Clone, the single Ethernet client can use its own MAC address. Disable MAC Clone, the single Ethernet client must to use AP-Client's MAC address.

While you use this device act as AP-Client and only one host connect to this device via Ethernet, you need to check this option in this page, otherwise the other device can't recognize your host behind AP-Client. If you use hub/switch connect multi-device to this AP-Client, you should uncheck this option.

enerit, jea eneara	
Site contents:	Wireless Basic Settings -wlan2
딸 Wizard 알 Operation Mode = 국 Wireless 에너희 Wian1 국 Wian2 딸 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. Enable universal repeater mode can let radio act as AP and client simultaneouly but remember the channel must be as same as the connected AP.
- 🗳 Advanced Setting - 🗳 Security	Disable Wireless LAN Interface
- E Access Control	Band: 5 GH2 (A)
Site Survey	Mode: Client 🔽
Connecting Profil	Network Infrastructure V
Firewall Gament	SSID: Targe-AP-SSID
Reboot	Channel 64 Show Active Clients
	Enable Mac Clone (Single Ethernet Client)
	Apply Changes Reset

### **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 3.* 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.

Site contents:		Wireless Basic Settings -wlan1	
Wizard Geration Mode Wireless Wireless Wineless Advanced Settings Charles Advanced 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. Enable universal repeater mode can let radio act as AP and client simultaneouly but remember the channel must be as same as the connected AP.	
Security		□ Disable Wireless I AN Interface	
WDS settings		Band: 2.4 GHz (B+G) V	
Site Survey     Connecting Profil     Wan2     TCP/IP     Firewall		Mode: Client 🗸	
		Network Type:	
		SSID: Target-AP-SSD	
Reboot		Channel 11 Show Active Clients	
		Enable Mac Clone (Single Ethernet Client)	
		Enable Universal Repeater Mode	
		Extended SSID:	
		(once selected and applied,extended SSID and channel number will be updated)	
		SSID BSSID Channel Type Encrypt RSSI Qu	ality
		Refresh	
	3		
		Apply Changes Reset	

Step 4. Check the status of connection in "Status" web page

Site contents:	System	
Wizard	Uptime	Oday:1h:50m:26s
Concretion Mode	Free Memory	7604 kB
	Firmware Version	1.4.1 20061101
	Webpage Version	1.4.1 20061101
📄 Firewall	Wireless 1 Configurati	ion
- 🔁 Management	Mode	Infrastructure Client - Bridge
🕒 Status	Band	2.4 GHz (B+G)
- 🗳 QoS	SSID	Target-AP-SSID
📲 Bandwidth Control	Channel Number	5
	Encryption	Disabled
	BSSID	00:00:00:00:00
	State	Scanning
	RSSI	0
Miscellaneous	Wireless 2 Configurati	ion
📲 Upgrade Firmware	Mode	AP - Bridge
🕒 皆 Save/Reload Setting	Band	5 GHz (A)
Password	SSID	Test
皆 Reboot	Channel Number	64
	Encryption	Disabled
	BSSID	00:00:88:99:88:02
	Associated Clients	0
	Power(OFDM/G)	50mW
	TCP/IP Configuration	
	Attain IP Protocol	Fixed IP
	IP Address	192.168.2.88
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP Server	Disabled
	MAC Address	00:00:88:99:88:00

The alternative way to configure as following:

*Step 4.* In "Wireless Site Survey" page, select one of the SSIDs you want to connect and then press "Connect" button to establish the link.

touna,	you could choo	se to connect it man	ually when cl	ient mode	e is enabled.				
Settings	CII22	BSSID	Channel	Туре	Encrypt	RSSI	Quality	Select	A
ity WLAN	_G_TEST999	00:0d:14:00:80:18	11 (B+G)	AP	nO	75 (-45 dbm)	89 1	$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	(
ZPlus-(	3192-mega	00:05:9e:81:bd:2b	3 (B+G)	AP	yes	69 (-48 dbm)	92	0	0
		00:03:7f:be:f1:9b	9 (B+G)	AP	yes	67 (-49 dbm)	89	0	C
rofil zw2200	)-G-254	00:00:85:aa:aa:ab	11 (B+G)	AP	yes	56 (-56 dbm)	89	0	C
802.11;	g-SSID	00:e0:4c:81:86:d1	11 (B+G)	AP	no	56 (-56 dbm)	90	0	C
ZINTE	CH-2F	00:05:9e:80:b1:e3	1 (B+G)	AP	yes	40 (- <i>66</i> dbm)	92	0	C
ZINTE	CH-3F	00:05:9e:80:b1:bd	11 (B+G)	AP	yes	40 (- <i>66</i> dbm)	87	0	C
ZPlus-2	1200-G-99	00:00:77:66:55:11	6 (B+G)	AP	no	33 (-70 dbm)	90	0	C

*Step 5.* If the linking is established successfully. It will show the message "Connect successfully". Then press "OK".



*Step 6.* Then you can check the linking information in "Status" page.

	-	
Site contents:	System	
🕒 Wizard	Uptime	Oday:Oh:8m:28s
Operation Mode	Free Memory	7876 kB
😐 🧰 Wireless	Firmware Version	1.4.1 20061101
	Webpage Version	1.4.1 20061101
🛁 Firewall	Wireless 1 Configurat	ion
🔁 Management	Mode	Infrastructure Client - Bridge
	Band	2.4 GHz (B+G)
une QoS	SSID	WLAN_G_TEST
	Channel Number	11
	Encryption	Disabled
	BSSID	00:00:01:02:03:04
🗳 Time Zone	State	Connected
E Log	RSSI	36 (-72 dbm, Quality 79)
📲 Miscellaneous	Wireless 2 Configurat	ion
💾 Upgrade Firmware	Mode	AP - Bridge
Save/Reload Setting	Band	5 GHz (A)
Password	SSID	Test
E Repool	Channel Number	64
	Encryption	Disabled
	BSSID	00:00:88:99:88:02
	Associated Clients	0
	Power(OFDM/G)	50mW
	TCP/IP Configuration	
	Attain IP Protocol	Fixed IP
	IP Address	192.168.2.88
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP Server	Disabled
	MAC Address	00:00:88:99:88:00

#### 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.

# Ch 5. 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.



#### Star topology:



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

#### **Ring topology:**

45 WDS #	LANT WDS #1 WDS #1 (P) WDS #2 (D) WDS #3 LAN4 LAN3 LAN4 LAN3	
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

#### <u>Mesh topology:</u>



The MAC Addresses of WDS1, WDS2, WDS3 and WDS4

# **WDS** Application

#### **Wireless Repeater**

WDS5

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.

Yes

- 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.

# Ch 6. Advanced Configurations Configuring LAN to WAN Firewall

Filtering function is used to block or permit 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 or allow 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. Denied or Allowed list depends on your IP forwarding default policy in Route page. The IP forwarding default policy is "ACCEPT".

If you want block some application from LAN to WAN, you can go to Route page to select "ACCEPT" for IP Forwarding Default Policy.



If you want permit some application from LAN to WAN, you can go to Route page to select "DROP" for IP Forwarding Default Policy.

site contents:	Routing Setup
Wizard Operation Mode Wireless TCP/IP LAN Interface WAN Interface Route Frewall Management	This page is used to setup dynamic routing protocol or edit static route entry. Disable the NAT will turn off IP masqerade and the functions of DMZ,Port Forwarding.

### **Port Filtering**

When you enable the Port Filtering function, you can specify a single port or port ranges in current filter table. If you select ACCEPT for the IP forwarding default policy, 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 form LAN to WAN.

	Fort Intering	,			
Wizard     Wizard     Wireless     TCP/IP     Firewall	Entries in this table are o local network to Internet securing your local netw default policy in Route p	used to restrict(allow) c through the Gateway. I ork. Denied or Allowed age.	ertain types of data pao Jse of such filters can l list depends on your IP	ckets from your be helpful in 9 forwarding	
달 Port Filtering 또 IP Filtering 또 MAC Filtering 또 DMZ 면 VPN 에 Management 또 Reboot	Enable Port Filter     Port Range:      Apply Changes Re     Current Filter Table:	ing (denied list) Protocol: Both	Comment:		
	Port Range	Protocol	Comment	Select	
	20-21	TCP+UDP	FTP		
	23	TCP	Telnet		
	80	TCP+UDP	Http		
	Delete Selected De	lete All Reset			

If you select DROP for the IP forwarding default policy, once the source port of outgoing packets match the port definition or within the port ranges in the table, the firewall will allow those packets form LAN to WAN.

Site contents:	Port Filtering	sed to restrict(allow) o hrough the Gateway. rk. Denied or Allowed ge. ng (allowed list) Protocol: Both et	ertain types of data pac Use of such filters can b list depends on your IP Comment:	kets from your re helpful in forwarding	
	Port Range	Protocol	Comment	Select	
	20-21	TCP+UDP	FTP		
	23	TCP	Telnet		
	80	TCP+UDP	Http		
	Delete Selected Del	ete All Reset			

### **IP Filtering**

When you enable the IP Filtering function, you can specify local IP Addresses in current filter table. If you select ACCEPT for the IP forwarding default policy, once the source IP address of outgoing packets match the IP address definition in the table, the firewall will block those packets form LAN to WAN.

Site contents: Wizard Operation Mode Wireless TCP/IP Filtering MAC Filtering MAC Filterin	IP Filtering Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.  ✓ Enable IP Filtering (denied list) Local IP Address: Protocol: Both ✓ Comment: Apply Changes Reset				
	Local IP Address	Protocol	Comment	Select	
	192.168.2.11	TCP	Client 11		
	192.168.2.23	TCP+UDP	Client 23		
	192.168.2.35	UDP	Client 35		
	Delete Selected Dele	ete All Reset			

If you select DROP for the IP forwarding default policy, once the source IP address of outgoing packets match the IP address definition in the table, the firewall will allow those packets form LAN to WAN.

Site contents: Vizard Operation Mode Vireless TCP/IP Frewall Port Filtering MAC Filtering	IP Filtering Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.  V Enable IP Filtering (allowed list) Local IP Address: Protocol: Both Comment:  Apply Changes Reset				
	Local IP Address	Protocol	Comment	Select	
	192.168.2.11	TCP	Client 11		
	192.168.2.23	TCP+UDP	Client 23		
	192.168.2.35	UDP	Client 35		
	Delete Selected Del	ete All Reset			

#### **MAC Filtering**

When you enable the MAC Filtering function, you can specify the MAC Addresses in current filter table. If you select ACCEPT for the IP forwarding default policy, once the source MAC Address of outgoing packets match the MAC Address definition in the table, the firewall will block those packets form LAN to WAN.

Site contents:	MAC Filtering					
Wizard Operation Mode Wireless TCP/IP Freevall Port Filtering Port Filtering Port Forwarding DMZ VPN Management Best	Entries in this table are used to restrict(all local network to Internet through the Gatew securing your local network. Denied or Allo default policy in Route page. Enable MAC Filtering (denied list) MAC Address: Con Apply Changes Reset	Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.           Image: Comparison of the security of the				
	Current Filter Table:					
	MAC Address	Comment	Select			
	00:00:03:12:01:02	Client 1				
	00:00:06:06:10	Client 5				
	00:00:00:10:10:22	Client 13				
	Delete Selected Delete All Reset					

If you select DROP for the IP forwarding default policy, once the source MAC Address of outgoing packets match the MAC Address definition in the table, the firewall will allow those packets form LAN to WAN.

Site contents: Vizard Operation Mode Vireless TCP/IP Frewall Port Filtering MAC Filtering MAC Filtering Port Forwarding Port Forwarding DMZ VPN Maggement Reboot	MAC Filtering Entries in this table are used to restrict(all local network to Internet through the Gatew securing your local network. Denied or Allo default policy in Route page. ✓ Enable MAC Filtering (allowed list) MAC Address: Con Apply Changes Reset Current Filter Table:	ow) certain types of data p vay. Use of such filters ca wed list depends on your ment:	packets from your n be helpful in IP forwarding	
	MAC Address	Comment	Select	
	00:00:03:12:01:02	Client 1		
	00:00:06:06:10	Client 5		
	00:00:00:10:10:22	Client 13		
	Delete Selected Delete All Reset			

# **NAT (Network Address Translation)**

NAT is the translation between public IP address and private IP address. While NAT is enabling, you can use port forwarding or DMZ to redirect your common network services. If you want to disable NAT, you can go to Management-Route page to disable it and the functions of DMZ, Port Forwarding will be disabled.

site contents:	Routing Setup	
	This page is used to setup dynamic routing protocol or edit static route entry. Disable the NAT will turn off IP masqerade and the functions of DMZ,Port Forwarding.	
LAN Interface WAN Interface Route Firewall	3 Disable NAT         IP Forwarding Default Policy         4 Apply Changes	
International		

# **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.

site contents:	Port Forwarding
Wizard     Operation Mode     Wireless     TCP/IP     TCP/IP     Trewall	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.
말 Port Filtering 말 IP Filtering 말 MAC Filtering 말 Port Forwarding 말 DMZ	☐ Enable Port Forwarding IP Address: Protocol: Both ♥ Port Range: Comment:
→ Management → Management → Reboot	Apply Changes Reset
	Current Port Forwarding Table:
	Local IP Address Protocol Port Range Comment Select
	Delete Selected Delete All Reset

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

A.L (	Services	Port Number	
About	ECHO	7	- the
	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	

the other

well-known ports, please search in http://www.iana.org/assignments/port-numbers.

### Multiple Servers behind NAT Example:

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



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 Re	zet		

# **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.

Sito contonto:	DMZ
	DIVIZ
B       Wizard         B       Operation Mode         Wireless       TCP/IP         Trewall       Port Filtering         B       Port Forwarding         B       POT Forwarding         B       DMZ         WN       Management	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. <b>Enable DMZ</b> <b>DMZ Host IP Address:</b> Apply Changes Reset
Reboot	
able DMZ:	Enable the "Enable DMZ", and then click "Apply Changes" button to

Enable DMZ:

**DMZ Host IP Address:** 

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



DNS Host

# **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".

Site contents:	WAN Interfa	ce Setup				
	This page is used to con port of your Access Poir Client, PPPoE or PPTP —	figure the parameters for Internet network which connects to the WAN t. Here you may change the access method to Static IP, DHCP by click the item value of WAN Access type.				
LAN Interface	WAN Access Type:	Static IP 🗸				
- Firewall	IP Address:	172.1.1.1				
Management	Subnet Mask:	255.255.255.0				
	Default Gateway:	172.1.1.254				
	DNS 1:					
	DNS 2:					
	DNS 3:					
	Clone MAC Address:	000000000				
	🗌 Enable uPnP					
	🗹 Enable Web Serv	er Access on WAN				
	🗌 Enable IPsec pas	s through on VPN connection				
	🗌 Enable PPTP pas	s through on VPN connection				
	Enable L2TP pass	Enable L2TP pass through on VPN connection				
	Apply Changes Re	set				

### 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.		
Site contents:	WAN Interfat	ce Setup figure the parameters for Internet network which connects to the WAN it. Here you may change the access method to Static IP, DHCP by click the item value of WAN Access type.
UAN Interface	WAN Access Type:	Static IP 🗸
🕒 Route	IP Address:	172.1.1.1
Management	Subnet Mask:	255.255.255.0
	Default Gateway:	172.1.1.254
	DNS 1:	
	DNS 2:	
	DNS 3:	
	Clone MAC Address:	0000000000
	🗌 Enable uPnP	
	🗹 Enable Web Serv	rer Access on WAN
	🔲 Enable IPsec pas	s through on VPN connection
	Enable PPTP pas	s through on VPN connection
	Enable L21P pass	s through on VPN connection
	Apply Changes Re	set
IP Address:	The Intern ISP or MI local netwo	et Protocol (IP) address of WAN interface provided by your S. The address will be your network identifier besides your ork.
Subnet Mask:	The numb the IP add	er used to identify the IP subnet network, indicating whether lress can be recognized on the LAN or if it must be reached
Default Gateway: DNS 1~3:	The IP add Default Ga of the netw can forwar one conne The IP add DNS (Dor	dress of Default Gateway provided by your ISP or MIS. Ateway is the intermediate network device that has knowledge work IDs of the other networks in the Wide Area Network, so it of the packets to other gateways until they are delivered to the cted to the specified destination. dresses of DNS provided by your ISP. nain Name Server) is used to map domain names to IP
Clone MAC Address: Enable uPnP <sup>.</sup>	Clone devi Internet un Clone devi ISP	DNS maintain central lists of domain name/P addresses and omain names in your Internet requests to other servers on the till the specified web site is found. The MAC address to the specify MAC address required by your nP, this function allows the device to be found and configured.
	automatica	ally by the system. (Ex. Window XP)

### **DHCP Client (Dynamic IP)**

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

Site contents: Wizard Geration Mode Wireless COP/IP LAN Interface Route Firewall Maagement Reboot	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 Client, PPPoE or PPTP by click the item value of WAN Access type.         WAN Access Type:       DHCP Client IM         • Attain DNS Automatically       •         • Set DNS Manually       DNS 1:         DNS 2:       DNS 3:         Chone MAC Address:       0000000000         • Enable uPnP       • Enable Web Server Access on WAN         • Chable IPsec pass through on VPN connection       • Chable L2TP pass through on VPN connection	
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)

### 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.

Site contents:	WAN Access Type: PPPoE
Wizard Operation Mode	User Name:
Wireless	Password:
LAN Interface	Connection Type: Continuous 🗸 Connect Disconnect
Route	Idle Time: 5 (1-1000 minutes)
Firewall	MTU Size: 1412 (1400-1492 bytes)
E Reboot	O Attain DNS Automatically
	⊙ Set DNS Manually
	DNS 1:
	DNS 2:
	DNS 3:
	Clone MAC Address: 00000000000
	Enable uPnP
	Enable Web Server Access on WAN
	Enable IPsec pass through on VPN connection
	Enable 12TP pass through on VPN connection
	Apply Changes Reset

User Name:	The account provided by your ISP		
Password:	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 needs to access the Internet.		
Idle Time:	The number of inactivity minutes to disconnect from ISP. This setting is only available when "Connect on Demand" connection type is selected.		
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)		

### PPTP

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

Site contents:	WAN Access Type: PPTP	
📲 Wizard		
Operation Mode     Wireless	IP Address: 172.1.1.2	
	Subnet Mask: 255.255.255.0	
LAN Interface	Server IP Address: 172.1.1.1	
Route	User Name:	
	Password:	
🕒 🕒 Reboot	MTU Size: 1412 (1400-1492 bytes)	
	MPPE: O Enabled O Disabled	
	O Attain DNS Automatically	
	⊙ Set DNS Manually	
	DNS 1:	
	DNS 2:	
	DNS 3:	
	Clone MAC Address: 000000000000	
	Enable uPnP	
	✓ 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	
	Apply Changes Reset	

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 add	ress for Statio	c IP WAN access type			
	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 Client, PPPoE or PPTP by click the item value of WAN Access type.				
· 말 Wiza - 말 Oper - ■ Wirel - 즉 TCP/ 말 ਯ 망	₩izard Coperation Mode Wireless					
	LAN Interface WAN Interface Route Firewall Management Reboot	WAN Access Type:	Static IP 🗸			
		IP Address:	172.1.1.1			
		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 Server Access on WAN				
		Enable IPsec pass through on VPN connection				
		Enable PPTP pass through on VPN connection				
		Enable LZTP pas	s through on VPN connection			
		Apply Changes Re	हरत इ.स.			

2. Clone MAC address for DHCP Client WAN access type

Site contents:	WAN Interface Setup			
<ul> <li>➡ Wizard</li> <li>➡ Operation Mode</li> <li>➡ Wireless</li> <li>➡ TCP/IP</li> </ul>	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 Client, PPPoE or PPTP by click the item value of WAN Access type.			
- 딸 LAN Interface - 딸 WAN Interface - 딸 Route	WAN Access Type: DHCP Client 💌			
- 🔁 Firewall	O Attain DNS Automatically			
Management	• Set DNS Manually			
	DNS 1:			
	DNS 2:			
	DNS 3:			
	Clone MAC Address: 001122334455			
	Enable uPnP			
	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			
	Apply Changes Reset			

3. Clone MAC address for PPPoE WAN access type

Site contents:	WAN Access Type:	PPPoE 🗸
Vizard Operation Mode	User Name:	87043609@hinet.net
	Password:	•••••
LAN Interface	Connection Type:	Continuous Connect Disconnect
WAN Interface	Idle Time:	5 (1-1000 minutes)
- Firewall	MTU Size:	1412 (1400-1492 bytes)
Management	○ Attain DNS Autom	atically
	⊙ Set DNS Manually	,
	DNS 1:	
	DNS 2:	
	DNS 3:	
	Clone MAC Address:	001122334455
	🗌 Enable uPnP	
	🗹 Enable Web Ser	ver Access on WAN
	🔲 Enable IPsec pa	ss through on VPN connection
	🔲 Enable PPTP pa	ss through on VPN connection
	🔲 Enable L2TP pas	ss through on VPN connection
	Apply Changes R	teset

4. Clone MAC address for PPTP WAN access type

Site contents:	WAN Access Type:	PPTP 💌		
<ul> <li> <sup>™</sup> Wizard         <sup>™</sup> Operation Mode         <sup>™</sup> Wireless         <sup>™</sup> TCP/IP         <sup>™</sup> TCP/IP         <sup>™</sup> <sup>™</sup> TCP/IP         <sup>™</sup> <sup>™</sup></li></ul>	IP Address:	172.1.1.2		
	Subnet Mask:	255.255.255.0		
LAN Interface	Server IP Address:	172.1.1.1		
Route	User Name:			
- 🚞 Firewall - 🧰 Management	Password:			
🖳 🗳 Reboot	MTU Size:	1412 (1400-1492 bytes)		
	MPPE:	⊙ Enabled O Disabled		
	○ Attain DNS Automa	atically		
	💽 Set DNS Manually			
	DNS 1:			
	DNS 2:			
	DNS 3:			
	Clone MAC Address:	001122334455		
	Enable uPnP			
	🗹 Enable Web Serv	er Access on WAN		
	Enable IPsec pass through on VPN connection			
	🔲 Enable PPTP pas	s through on VPN connection		
	Enable L2TP pass	s through on VPN connection		
	Apply Changes Re	set		

# 5. Physical LAN interface MAC address clone

🕒 Wizard 🗣 Operation Mode	This page is used to confi	igure the parameters for local area network which connects to
Wireless	the device. Here you may etc	change the setting for IP Address, Subnet Mask, DHCP,
TCP/IP		
WAN Interface	IP Address:	192.168.2.254
Route	Subnet Mask:	255.255.255.0
Management	Default Gateway:	0.0.0
E Reboot	DHCP:	Server 🖌
	DHCP Client Range:	192.168.2.100 - 192.168.2.200 Show Client
	802.1d Spanning Tree:	Disabled 🗸
	Clone MAC Address:	001122334455
	MTU Size:	1500

# **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.

Site contents:	LAN Interface Setup
<ul> <li>➡ Wizard</li> <li>➡ Operation Mode</li> <li>➡ Wireless</li> <li>➡ TCP/IP</li> </ul>	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 Address, Subnet Mask, DHCP, etc
UAN Interface	IP Address: 192.168.2.254
E Route	Subnet Mask: 255.255.255.0
🗎 Management	Default Gateway: 0.0.00
E Reboot	DHCP: Server 🔽
	DHCP Client Range: 192.168.2.100 - 192.168.2.200 Show Client
	802.1d Spanning Tree: Disabled 💌
	Clone MAC Address: 00000000000
	MTU Size: 1500
	Apply Changes Reset

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.

# **Bandwidth Control**

This functionality can control Bandwidth of Up/Downstream

1. Enable Bandwidth Control and then enter Data Rate 
< Latency and Burst Packet in the specific field.

٩	Site contents:		Bandwidth Contr	ol Setti	ngs	
- - -	Wizard Operation Mode Wireless		This page is used to configure the networking bandwidth. You can set the upstream and downstream data rate when the device is set to client mode.			
È	Firewall	3	Bandwidth Control			
	Management 1		Upstream Data Rate:	24000	(16-24000 kbps)	
	📴 QoS	_	Upstream Latency:	50	(20-1024 ms)	
	말 Bandwidth Control 달 SNMP	2	Upstream Burst Packet:	25600	(1600-40000 Bytes)	
	Statistics		Downstream Data Rate:	24000	(16-24000 kbps)	
	별 DDNS 탈 Time Zone		Downstream Latency:	50	(20-1024 ms)	
	🗳 Log		Downstream Burst Packet:	25600	(1600-40000 Bytes)	
	Upgrade Firmware Save/Reload Setting	4	Apply Changes Reset			

Note: Only device on Client mode or WISP mode this functionality can take effective. 2. Parameter Definition

Label	Description
Upstream Data Rate	Speed of transmit data that from Ethernet
	interface to Wireless interface.
Upstream Latency	Similar a waiting time the data queuing- time.
Upstream Burst Packet	Similar a buffer the data will into the buffer
	while the data is transmit or receive.
Downstream Data Rate	Speed of transmit data that from Wireless

interface to Ethernet interface.			
Downstream Latency	Similar a waiting time the data queuing- time.		
Downstream Burst	Similar a buffer the data will into the buffer		
Packet	while the data is transmit or receive.		

# **QoS (Quality of Service)**

Filter Priority and IP-ToS have not finished yet and also fine tuning.

QoS allows you to specify some rules, to ensure the quality of service in your network. Such as use Bandwidth Priority concept to allocate bandwidth. This function can be helpful in shaping and queuing traffic from LAN (WLAN) to WAN or LAN to WLAN, but not WLAN to WLAN.

Enable the QoS and then fill in Bandwidth Ratio (H/M/L) the device has three Bandwidth Priorities High, Medium and Low user can allocation Bandwidth to these and default is High:50%, Medium:30% and Low:20%.

	-	
í	Site contents:	QoS setting
	Wizard     Gperation Mode     Wireless     TCP/IP     TCP/IP     Firewall     Management	Entries in this table are used to restrict certain quality of service for your network. Use of such setting can be helpful in traffic control or queuing discipline of your network. The traffice control among WLAN stations is futile,it works between LAN(WLAN)/WAN or LAN/WLAN. The default queue is Med and once the bandwidth borrowed is enabled , the higher bandwidth priority will get the remaining bandwidth first.
	<mark>딸</mark> Status <b>딸</b> QoS 딸 Bandwidth Control	<ul> <li>✓ QoS Enabled</li> <li>✓ Bandwidth Borrowed</li> </ul>
	SNMP	Max Throughput : 20000 (kbps)
	발 DDNS 발 Time Zone 같 Log	Bandwidth Ratio (H/M/L):     50 : 20 (%)       Apply Changes
	Miscellaneous	

The following table describes the priorities that you can apply to bandwidth.

Priority Level	Description
High	Typically used for voice or video applications that is
	especially sensitive to the variations in delay.
Medium	Typically used for important traffic that can tolerate
	some delay.
Low	Typically used for non-critical traffic such as a large
	number of transfers but that should not affect other
	application.

Click the **QoS** link under **Management** to open the QoS Setting page. This page is divided into three parts: basic settings, QoS rule settings, and current QoS setting table.

1. Enable QoS and enter Max Throughput (default 20Mbps) 
Bandwidth Ratio (default H:50%, M:30%, L:20%)

<b>~</b>	QoS	Enabled	
	005	LIIGUIGU	

Bandwidth Borrowed		
Max Throughput :	20000	(kbps)
Bandwidth Ratio (H/M/L):	50 : 30 : 20	(%)

Apply Changes

The following table describes the labels in this part.

Label	Description							
QoS Enabled	Select this check box to enable quality of service.							
Bandwidth Borrowed	Select this check box to allow a rule to borrow							
	unused bandwidth. Bandwidth borrowing is decided							
	y priority of the rules. Higher priority will get the							
	remaining bandwidth first.							
Max Throughput	Enter the value of max throughput in kbps that you							
	want to allocate for one rule. The value should							
	between 1200 kbps and 24000 kbps.							
Bandwidth Ratio	You can specify the ratio of priority in these fields.							
(H/M/L)	The range from 1 to 99. The High priority's ratio							
	should higher than Medium priority's ratio and							
	Medium priority's ratio should higher than Low							
	priority's ratio.							
Apply Changes	Click this button to save and apply your settings.							

### 2. QoS Rule settings

Source IP Address :	
Source Netmask :	
Destination IP Address :	
Destination Netmask :	
Source MAC Address :	
Destination MAC Address :	
Source Port / range:	to
Destination Port / range:	to
Protocol:	×
Bandwidth Priority:	×
Filter Priority:	(Lower number,Higher Priority)
IP TOS Set:	~
Apply Changes Reset	

The following table describes the labels in this part.

Label	Description
IP Address	Enter source/destination IP Address in dotted
	decimal notation.

Netmask	Once the source/destination IP Address is entered,
	the subnet mask address must be filled in this field.
MAC Address	Enter source/destination MAC Address.
Port / range	You can enter specific port number or port range of
	the source/destination
Protocol	Select a protocol from the drop down list box.
	Choose TCP/UDP, TCP or UDP.
Bandwidth Priority	Select a bandwidth priority from the drop down list
	box. Choose Low, Medium or High.
Filter Priority	Select a filter priority number from the drop down
	list box. Lower number gets higher priority while
	two rules have the same bandwidth priority.
IP TOS Set	Select an IP type-of-service value from the drop
	down list box. Choose Normal Service, Minimize
	Cost, Maximize Reliability, Maximize Throughput,
	or Minimize Delay.
Apply Changes	Click this button to save and apply your settings.
Reset	Click this button to begin re-input the parameters.

### **Current QoS setting table**

In this part, you can see how many rules have been specified. And you can see the detail about the rules and manage the rules. This table can input 50 rules at most.

Current QoS Set (Mask 255.255.255.25	ting: 55 means single host)									
Src Adr	Dst Adr	Src MAC	Dst MAC	Src Port	Dst Port	Pro	Pri	Filter	TOS	Sel
192.168.2.11/24	140.113.27.181/24	00:05:9e:80:aa:ee	-	21-21	21-21	TCP	LOW	0	Normal	
anywhere	anywhere	-	-	80-80	-	TCP/UDP	MED	0	Normal	
192.168.2.13/24	anywhere	-	-	50000-50050	-	TCP/UDP	LOW	2	Normal	
anywhere	192.168.2.12/24	-	-	-	-	TCP/UDP	MED	1	Normal	
192.168.2.15/24	anywhere	00:05:9e:80:aa:cc	-	-	-	TCP/UDP	HIGH	0	Normal	
Delete Selected	Delete All	leset								

### An example for usage



example, there are three users in your network.

- User A wants to **browse the websites** to retrieve information.
- User B wants to use FTP connection to download a large file.
- User C wants to use **software phone** to connect with customer.

For

The voice is sensitive to the variations in delay; you can set **High** priority for **User C**. The FTP transmission may take a long time; you can set **Low** priority for **User B**.

Current QoS Setting: Mask 255.255.255 means single host)										
Src Adr	Dst Adr	Src MAC	Dst MAC	Src Port	Dst Port	Pro	Pri	Filter	TOS	Sel
192.168.2.11/24	anywhere	-	-	5060-5061	-	TCP/UDP	HIGH	0	Normal	
192.168.2.12/24	anywhere	-	-	21-21	-	TCP	LOW	0	Normal	
192.168.2.13/24	anywhere	-	-	80-80	-	TCP	MED	0	Normal	
Delete Selected	Delete All	Reset								

# **Static Route Setup**

User can set the routing information let the Router knows what routing is correct also it can not learn automatically through other means.



For example, if user wants to link the Network 3 and Network 4 separately from Network 1 that Routing Table configuration as below:

 Enable Static Route in Route Setup of TCP/IP page and then enter IP Address of Network 3 
 Subnet Mask and IP Address of Router (R1) in Default Gateway field final click Apply Change button.



2. Enter IP Address of Network 4 
Subnet Mask and IP Address of Router (R2) in Default Gateway field final click Apply Change button.

Enable Static Route	
IP Address:	192.168.4.0
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.2.2
Apply Changes Reset S	Show Route Table

3. In Static Route Table there have two routings for Network 3 and Network 4

Static Route Table:			
Destination IP Address	Netmask	Gateway	Select
192.168.3.0	255.255.255.0	192.168.2.1	
192.168.4.0	255.255.255.0	192.168.2.2	

### **Dynamic Route Setup**

The Dynamic Route utilizes RIP1/2 to transmit and receive the route information with other Routers.

1. Enable Dynamic Route and then select RIP 1 
RIP2 or Both to transmit/receive packets final click Apply Change button.

Enable Dynamic Route	
RIP transmit to WAN	RIP1 and RIP2 🛩
RIP receive from WAN	RIP1 and RIP2 🐱
RIP transmit to LAN	RIP1 and RIP2 🐱
RIP receive from LAN	RIP1 and RIP2 🐱
Apply Changes	

2. Click Show Route Table button to show Dynamic Route Table.

Enable Static Route	
IP Address:	
Subnet Mask:	
Default Gateway:	
Apply Changes Reset	Show Route Table

3. In Dynamic Routing Table there have two routings for Network 3 and Network 4

### Routing Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
255.255.255.255	0.0.0.0	255.255.255.255	UH	0	0	0	<b>br</b> 0
192.168.4.0	192.168.2.2	255.255.255.0	UG	2	0	0	br0
192.168.3.0	192.168.2.1	255.255.255.0	UG	2	0	0	<b>br</b> 0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
172.1.1.0	0.0.0.0	255.255.255.0	U	0	0	0	wlan(
0.0.0.0	172.1.1.254	0.0.0.0	UG	0	0	0	wland

# **VPN Pass-through**

This functionality let the device can Pass-through the VPN packets including PPTP/ L2TP/IPsec VPN Connection.



1. Check the VPN Pass-through in WAN Interface of TCP/IP Page that you want and then click Apply Changes button.



# **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



# The System Management

#### **Password Protection**

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

site contents:	Password Setup
Wizard  Operation Mode  Wireless  TOP/IP	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:
- Cos	New Password:
Bandwidth Control	Confirmed Password:
	Apply Changes Reset
- C Time Zone	
Log Miscellaneous	
Upgrade Firmware	
Save/Reload Setting	
E Reboot	

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. Management $\rightarrow$ F. Password

# **SNMP** Agent

This device is compatible with SNMP v1/v2c and provides 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.

1. Enable SNMP and then enter IP Address of SNMP Manager in Trap Receiver IP Address field and Community String in System Community String field. Final click Apply Changes button.

site contents:	SNMP Settings	
Wizard     Operation Mode     Wireless     TCP/IP	This page is used to configure the information via setting the SNMP i	SNMP settings. You can get some of the system network protocol.
- 📄 Firewall	3 🗹 SNMP Enabled	
Management Management	System Community String:	public
🗳 QoS	System Name:	hank
Bandwidth Control	System Location:	1F
Statistics	System Contact:	hank
- UDNS - UDNS - UDNS Time Zone	Trap Receiver IP Address1:	192.168.2.11
	Address1 Community String:	hank
Upgrade Firmware	Trap Receiver IP Address2:	
Save/Reload Setting	Address2 Community String:	
Reboot	Trap Receiver IP Address3:	
	Address3 Community String:	
	5 Apply Changes Reset	

### 2. Following Table describes the SNMP configuration parameter

Label	Description
System Community String	This is password sent with each trap to the
	SNMP Manager.
System Name	Type the Name which is name of device.
System Location	Type the Location which is location of
	device
System Contact	Type the Name which is person or group
	when the device has problem can find
	they.
Trap Receiver IP Address	Type the IP Address which is address of
	SNMP Manager.
Trap Receiver Community	This is password receive with trap from
String	the device (SNMP Agent).

### 3. SNMP Traps

Traps	Description
coldStart(0)	The trap from device after reboot the
	device
linkDown(2)	The trap is sent when any of the links are
	down. See the following table.
linkup(3)	The trap is sent when any of the links are
	UP. See the following table.
authenticationFailure(4)	The trap is sent when the device receiving
	gets or sets requirement with wrong
	community.

#### 4. Private MIBs

OID	Description
1.3.6.1.4.1.99.1	Mode, Operation Mode in device.
1.3.6.1.4.1.99.2	SSID, SSID of the device
1.3.6.1.4.1.99.3	Channel, Channel of the device in WLAN
1.3.6.1.4.1.99.4	Band, 802.11g / 802.11b only
1.3.6.1.4.1.99.5	RSSI, Receive Signal Strength Index
	(Support AP and Client RSSI)
1.3.6.1.4.1.99.6	Active_Clients, The number of associate
	clients
1.3.6.1.4.1.99.7	Active_Clients_List, Client's Information
	(MAC Address, Data Rate, RSSIetc)
1.3.6.1.4.1.99.8	Encryption, Encryption type of device in
	Wireless Network

#### 1.3.6.1.4.1.99.1 - Mode

.1.3.6.1.4.1.99.1.2.1	MODE
.1.3.6.1.4.1.99.1.3.1	/bin/flash snmpget MODE
.1.3.6.1.4.1.99.1.100.1	0
.1.3.6.1.4.1.99.1.101.1	AP - Bridge

#### 1.3.6.1.4.1.99.2 - SSID

.1.3.6.1.4.1.99.2.2.1	SSID
.1.3.6.1.4.1.99.2.3.1	/bin/flash snmpget SSID
.1.3.6.1.4.1.99.2.100.1	0
.1.3.6.1.4.1.99.2.101.1	hank

#### 1.3.6.1.4.1.99.3 - Channel

.1.3.6.1.4.1.99.3.1.1	1
.1.3.6.1.4.1.99.3.2.1	CHANNEL
.1.3.6.1.4.1.99.3.3.1	/bin/flash snmpget CHANNEL
.1.3.6.1.4.1.99.3.100.1	0
.1.3.6.1.4.1.99.3.101.1	11

#### 1.3.6.1.4.1.99.4 - Band

.1.3.6.1.4.1.99.4.2.1	BAND
.1.3.6.1.4.1.99.4.3.1	/bin/flash snmpget BAND
.1.3.6.1.4.1.99.4.100.1	0
.1.3.6.1.4.1.99.4.101.1	802.11bg

#### 1.3.6.1.4.1.99.5 - RSSI

.1.3.6.1.4.1.99.5.2.1	RSSI
.1.3.6.1.4.1.99.5.3.1	/bin/flash snmpget RSSI
.1.3.6.1.4.1.99.5.100.1	0
.1.3.6.1.4.1.99.5.101.1	100

#### 1.3.6.1.4.1.99.6 - Active\_Clients

.1.3.6.1.4.1.99.6.2.1	ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.3.1	/bin/flash snmpget ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.100.1	0
.1.3.6.1.4.1.99.6.101.1	1

#### 1.3.6.1.4.1.99.7 - Active\_Clients\_List

.1.3.6.1.4.1.99.7.2.1	ACTIVE_CLIENTS_LIST
.1.3.6.1.4.1.99.7.3.1	/bin/flash snmpget ACTIVE_CLIENTS_LIST
.1.3.6.1.4.1.99.7.100.1	0 MAC Data Rate RSSI
.1.3.6.1.4.1.99.7.101.1	00:13:02:03:51:5e 102,125(54 no,300(57(-55 dbm)

#### 1.3.6.1.4.1.99.8 - Encryption

.1.3.6.1.4.1.99.8.2.1	ENCRYPTION
.1.3.6.1.4.1.99.8.3.1	/bin/flash snmpget ENCRYPTION
.1.3.6.1.4.1.99.8.100.1	O AP-WEP
.1.3.6.1.4.1.99.8.101.1	WEP(AP), Disabled(WDS)

### **Miscellaneous Settings**

site contents:	Miscellaneous Se	ettings		
Vizard Coperation Mode	This page is used to configure the	e miscellaneous settir	igs.	
	HTTP Port:	80 (1-65	;535)	
Firewall	RSSI Interval:	100 (30-8	6400 seconds)	
- 말 Status - 말 QoS - 말 Bandwidth Control	Ping WatchDog Enabled Target Hest IP Address:	192.168.2.254	]	
🚰 SNMP 🚰 Statistics	Ping Interval:	100	(15-86400 seconds)	
	Ping Threshold:	5	(1-100 times)	
E Log	Ping Rebooting Delay:	60	(10-600 seconds)	
말 Miscellaneous 말 Upgrade Firmware 말 Save/Reload Setting 말 Password 말 Reboot	Apply Changes Reset			

#### **HTTP Port**

The default http port is 80. For security concern, you can change the device's http port, to protect this web server from intrusion and attack.

1. Entering the port number you want to change in HTTP PORT field, then click Apply Changes button.

HTTP Port:	65500	(1-65535)
RSSI Interval:	100	(30-86400 seconds)

2. After apply change, you should re-login the web server. Type http://192.168.2.254:65500/ in URL field.



#### **RSSI** Interval

HTTP Port:	80	(1-65535)
RSSI Interval:	100	(30-86400 seconds)

Input your RSSI Interval to specify the refresh time of RSSI information. The RSSI information can be found on the page of Wireless Basic Setting, Active Client Table, Wireless Site Survey and Status. Because it has to wait to receive the radio signal, the throughput of this device will be impacted if the interval is too short. The default interval is 100 seconds.

### **Ping WatchDog**

Ping WatchDog Enabled:

Click to enable this function. This device can check its own status by ping another host. When user enable this option, the device perform ping to a specific network host. Once the ping is timeout, it may be caused by its network function crashes, and the device will reboot to fix it.

Ping WatchDog Enabled		
Target Host IP Address:	192.168.2.254	]
Ping Interval:	100	(15-86400 seconds)
Ping Threshold:	5	(1-100 times)
Ping Rebooting Delay:	60	(10-600 seconds)
Apply Changes Reset		

Following Table describes the Ping WatchDog configuration parameter

Label	Description
Target Host IP	Specify the IP Address of the Network host to ping.
Address	
Ping Interval	Specify the waiting time for the next ping. If this time
	is too short, it will impact the through of this AP. The
	default value is 100.

Ping Threshold	Specify the Ping-fail times of criteria. If this device
	ping fails several times continuously, and the fail
	times meet this criterion, it will perform reboot. The
	default value is 5.
Ping Rebooting	The time before it starting rebooting. When it meets
Delay	the Ping Threshold, it will wait for this time and then
	reboot. The default value is 60.

# **Aiming Tool**

The "Aiming tool" can help the installer of the device to find the best direction targeting the specific Access Point or IBSS. It displays the RSSI of the specify SSID on the Wireless Site Survey page on the web and LED, so the installer can adjust the antenna of this device and visually check RSSI by LED.

ound, you could ch	tool to scan the wireless oose to connect it manu	ally when cl	ient mode	ss Point or It e is enabled.	BSS IS			
SSID	BSSID	Channel	Туре	Encrypt	RSSI	Quality	Select	Аіш
ZPlus-G120	00:05:9e:81:fd:fb	11 (B+G)	AP	yes	86 (-38 dbm)	87	0	0
throu.	00:05:9e:81:b9:67	6 (B+G)	AP	no	81 (-41 dbm)	92	0	0
hot	00:0d:14:00:6d:4e	10 (B+G)	AP	yes	56 (-56 dbm)	89	0	$\odot$
ZPD-1	00:05:9e:81:9a:ed	1 (B+G)	AP	nO	52 (-58 dbm)	82	0	0
ZINTECH-QA	00:00:00:04:78:74	1 (B+G)	AP	yes	16 (-80 dbm)	73	0	0
ZPlus-2200-G	00:01:c7:12:34:56	11 (B+G)	AP	yes	9 (-84 dbm)	32	0	0

When this device is in AP Client mode, the user can click the "Aim" option of one SSID on the list in the Wireless Site Survey page and then click the "Aiming" button.

Wireless Site Survey							
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.							
SSID	CII 228	Channel	Туре	Encrypt	RSSI	Quality	
hot	00:0d:14:00:6d:4e	10 (B+G)	AP	yes	58 (-55 dbm)	89	
Refresh Stop Aiming	ł,						

After clicking the "Aiming" button, RSSI will be displayed on the web page. It's also displayed by the LED. The flashing frequency of each LED shows the RSSI; the more

frequency the LED flashing, the more RSSI it detected. From 20% to100% on the following picture, the more LED on means the more RSSI detected. For example, if the 20% LED and 40% LED are both on and flash quickly, that means the RSSI of the specific SSID is approaching 40%.



To stop the Aiming tool, the user just click "Stop Aiming" button.

### **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 **zwa-2200webpages\_adv.bin** and **zwa-2200linux\_adv\_led2.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.



### **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

site contents:	Save/Reload Settings
Wizard Operation Mode Wireless TCP/IP	This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
<ul> <li>TCP/IP</li> <li>Firewall</li> <li>Status</li> <li>GoS</li> <li>Bandwidth Co</li> <li>Statistics</li> <li>DDNS</li> <li>Time Zone</li> <li>Log</li> <li>Miscellaneous</li> <li>Usorade Firms</li> <li>Save/Reload S</li> <li>Password</li> </ul>	Save Settings to File:       Save         Load Settings from File:       谢贾         Reset Settings to Default:       Reset

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.

# **Auto Discovery Tool**

User can use this tool to find out how many devices in your local area network. The name of tool is WirelessConf.exe it in the packing CD.

Login:

When the user opens this Auto Discovery tool, the login password must be inputted. The default password is "qwert". After inputting the password, click "Login" button to open the tool.

Password:	****	Login	N
-----------	------	-------	---

If the user doesn't input the password or input a wrong password, he can't login the tool and see the alert window.

Wi	relessConf							
L	ogin failed! Please t	ry again.						
	OK							
19	🕽 Wireless LAN Series C	ionfiguration Tool (	( ¥ 1.0.0.1 )					×
	No SSID	IP Address	Subnet Mask	Mode	Channel	MAC Address	Active Client	RSSI
	1 WLAN-TEST	192.168.2.88	255.255.255.0	AP - Bridge	11	00:00:00:06:06:51	0	-
	2 WLAN-TEST-1	192.168.2.50	255.255.255.0	AP - Bridge	6	00:00:00:AA:00:02	0	-
	Password:		ain New	Password		Change Passwo		
	Discover Se	etup IP De	tail W	DS Active Cl	ients	Connect to Web S	erver C	lose
125	(2) (	3) (4	4) (5	6		$\overline{7}$		8

#### 1. Change Password

The user can change the default login password. Just enter new password after login this tool and click "Change Password" button.



The pop-up window shows that the password has been successfully changed.

WirelessConf 🛛 🔀
Change password successful!!
OK

#### 2. Discover

After press this button, you could see there are how many devices in your network. And you would see the basic information about these devices, such as:

- SSID
- IP Address
- Subnet Mask
- Operation Mode
- Channel number
- MAC Address
- Active Client: this field shows how many clients associated with the device
- RSSI: this field shows <u>Received Signal Strength Indication while device is on AP-Client</u> mode

#### 3. Setup IP

After you press the *Setup IP* button, you would see *Setup IP Address* window. You could change device's IP Address, Netmask, and Default Gateway in this window. But if the device's web server needs User Name and Password to login, you should fill in these two fields and then apply changes.

Setup IP Address		×
- IP Address		1
DHCP Client En	nabled	
IP Address:	192 . 168 . 2 . 1	
Netmask:	255 . 255 . 255 . 0	
Default Gateway:	0.0.0.0	
User Name:	test	
Password:	****	
Apply Changes		

#### 4. Detail

If you want to see more detailed information, you could press the *Detail* button, and then you would see the **Detail Information** window.

Detail	
System Name:	hank
System Location:	1F
System Contact:	hank
Firmware Version:	
Mode:	AP - Bridge
Band:	802.11bg
TXPowerLevel:	OFDM 100mW / CCK 250mW
Upstream Data Rate:	24000 kbps
Upstream Latency:	50 ms
Upstream Burst Packet:	25600 Bytes
Downstream Data Rate:	24000 kbps
Downstream Latency:	50 ms
Downstream Burst Packet:	25600 Bytes
Encryption:	Disabled(AP),Disabled(WDS)
	Close

#### 5. WDS

If the device you selected is on WDS mode or AP+WDS mode, you could press **WDS** button, and then you would see the **WDS List** window.

W	DS L	ist				×
	No 1 2 3	MAC Address 00:05:9e:80:aa:11 00:05:9e:80:aa:22 00:e0:4c:81:86:21	Tx Packets 41 41 20	Tx Errors 37 39 3	Rx Packets 0 0 633	Tx Rate (Mbps) 1 1 11
						Close

#### 6. Active Clients

After press *Active Clients* button, you would see WLAN AP Active Clients window. In this window, you could see client's information, such as:

LAN	AP Active Clients					E
No	MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
1	00:05:9e:80:3a:d7	1	90	54	no	298
						Close

#### 7. Connect to Web Server

If you want connect to device's web server, you could press this button, or double-click on the device.

#### 8. Close

You could press this button to leave this tool.

#### 9. Reset the password to default password

If the user had changed the login password and forgot it, he can execute "ResetPassword.exe" to reset to the default password. When the password has been reset by this program, the following message window will be prompt on screen. Then the user can use the default password "qwert" to login the tool.

Reset Password
The password of auto-discovery tool is reset successfully!
OK

Item	Antenna Type	Antenna Gain	Type of Operation
No.			
1	2.4GHz Dipole Antenna (OA-2450-12)	12dBi	Point to Multipoint
2	2.4GHz Dipole Antenna (OA-2450-15)	15dBi	Point to Multipoint
3	2.4GHz Panel Antenna (PA-2450-16)	16dBi	Point to Multipoint
4	5GHz Panel Antenna (PA-5825-16)	16dBi	Point to Multipoint
5	5GHz Panel Antenna	18dBi	Point to Multipoint
6	5GHz Omni Antenna	12dBi	Point to Multipoint

Notes and Warnings to the User and Installer Caution :

%This Installation Guide is intended for use by the professional wireless LAN system installer.
%The device cannot be sold retail, to the general public or by mail order. It must be sold to dealers or have strict marketing control.

WARNING : It is the responsibility of the professional installer to ensure that the system is used exclusively for fixed, point-to-multipoint operations.

Warning : When using the ZW-2200IA / ZW-2200OD in the United States(or where FCC rules apply), it is the responsibility of the professional installer to ensure to control the output power not greater then the application(ZW-2200IA / ZW-2200OD : IEEE802.11a mode: 61mW; IEEE802.11b mode: 94.4mW; IEEE802.11g mode: 92.04mW)

Who Should Use this Guide

Installation of this device should be accomplished only by a qualified wireless LAN system installer who is  $\therefore$ 

⊘Knowledgeable of the use, installation and configuration procedures and associated network components.

Knowledgeable of each system component' s equipment User and Installation Guide.
 Knowledgeable of the installation and configuration procedures for the site' s network infrastructure system and wiring.

⊘Knowledgeable of the installation procedures, safety, and code requirements for the site's antenna, antenna mast, antenna cabling, and installation. We highly recommends that the antenna installation be preformed by a qualified antenna installation professional.

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

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 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 installation. , May cause harmful interference to radio communication. However, there is no guarantee that interference Will not occur in a particular installation. if this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna

- Increase the separation between the equipment and receiver

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected

- Consult the dealer or an experienced radio / TV technician for help

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

REMARK: This device must be installed by professional.