Wireless LAN Device Series

WLAN Outdoor AP

NSK-2418-ZW5 User Manual

Version. 1.4.3.f (2007.09.13)

TABLE OF CONTENTS

NOTICE	3
PREFACE	5
CH 1. NSK-2418-ZW5 INSTALLATION	6
NSK-2418-ZW5-IA	6
Packing List	6
Hardware Installation	7
NSK-2418-ZW5-OD錯誤!	尚未定義書籤。
Packing List 錯誤!	<i>尚未定義書籤。</i>
Hardware Installation錯誤!	尙未定義書籤。
CH 2. FIRST TIME CONFIGURATION	9
BEFORE START TO CONFIGURE	9
KNOWING THE NETWORK APPLICATION	9
BASIC SETTINGS	
ADVANCED SETTINGS	
CONFIGURING WIRELESS SECURITY	
CONFIGURING AS WLAN CLIENT ADAPTER	
QUICK START TO CONFIGURE	
MAC CLONE FOR SINGLE ETHERNET CLIENT	40
CONFIGURING UNIVERSAL REPEATER	41
CH 3. CONFIGURING WDS	43
WDS NETWORK TOPOLOGY	43
WDS APPLICATION	45
CH 4. ADVANCED CONFIGURATIONS	47
CONFIGURING LAN TO WAN FIREWALL	47
Port Filtering	47
IP FILTERING	
MAC FILTERING	49
NAT (NETWORK ADDRESS TRANSLATION)	50
CONFIGURING PORT FORWARDING (VIRTUAL SERVER)	51
Multiple Servers behind NAT Example:	51
CONFIGURING DMZ	52
CONFIGURING WAN INTERFACE	53
STATIC IP	53
DHCP CLIENT (DYNAMIC IP)	54
РРРОЕ	55
РРТР	56
	1

CONFIGURING CLONE MAC ADDRESS
CONFIGURING DHCP Server60
BANDWIDTH CONTROL
QOS (QUALITY OF SERVICE)
STATIC ROUTE SETUP
DYNAMIC ROUTE SETUP
VPN Pass-through
USING CLI MENU
THE SYSTEM MANAGEMENT
SNMP AGENT
MISCELLANEOUS SETTINGS
PING WATCHDOG73
AIMING TOOL
CONNECTING PROFILE
FIRMWARE UPGRADE76
CONFIGURATION DATA BACKUP & RESTORE
AUTO DISCOVERY TOOL

Notice

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

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

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: 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 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 needed.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

Shielded interface cables must be used in order to comply with emission limits.



CAUTION :

- The antenna(s) used for this transmitter must be fixed-mounted on outdoor permanent structures with a separation distance of at least 2 meters from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. Users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.
- 2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

4

3. This equipment is only allowed to be professionally installed.

Preface

This guide is for the networking professional who installs and manages the SkyVertex Co., Ltd NSK-2418-ZW5 product hereafter referred to as the "device". To use this guide, you should have experience working with the TCP/IP configuration and be familiar with the concepts and terminology of wireless local area networks.

Ch 1. NSK-2418-ZW5 Installation

NSK-2418-ZW5

Packing List

Before you start to install the device, make sure the package contains the following items :

- ? Wireless AP unit * 1
- ? Mounting Kit * 1
- ? Power Over Ethernet Kit * 1
- ? Waterproof Connector * 1
- ? Ethernet Cable * 1



Hardware Installation

Once you check off everything from the package, you can start to install the IA. You can mount to a pipe. The steps are showed in the following :

1. You must mount the IA into the bracket first.



- 2. After checking the IA is mounted well, you can connect the RJ-45 network cable to Ethernet port of IA. The steps are showing as below:
- 3. Plug the other end of the RJ-45 network cable to "P+ DATA OUT" port of PoE device. The PoE device is guaranteed only in indoor environment.



<u>Caution</u>: DON'T plug the power cord into PoE device before you finish install the antenna and Ground wire to ensure the safety.

Make sure the maximum length of the RJ-45 cable is shorter than 100M (about 109 yards) for normal operation under IEEE 802.3 standards.

When you plug the regular RJ-45 cable into the PoE device, you should use the regular RJ-45 cable to plug into the "DATA IN" of "Power Over Ethernet Kit" to connect to hub/switch or use the crosslink RJ-45 cable (Not included in the Packing List) to connect with user's PC.

The RJ-45 network cable must be connected to the "P+DATA OUT" port.

<u>Caution</u>: Be careful! Don't plug the two cables inversely. It will damage the devices! And you have to use our PoE (included in the packing list) to guarantee that power supply is normal.

We recommend you refer to the following illustration as a guideline for hardware installation.



Ch 2. First Time Configuration Before Start to Configure

There are two ways to configure the device, one is through web-browser, and the other is through Secure Shell CLI interface. To access the configuration interfaces, make sure you are using a computer connected to the same network as the device. The default IP address of the device is 192.168.2.254, and the subnet-mask is 255.255.255.0.

The device has three operation modes (Router/Bridge/WISP). In bridge mode, also known as AP Client, you can access the device by both WLAN (Wireless Local Area Network) and wired LAN. And in router/WISP modes, the device can be accessed by both WLAN and WAN. The default IP addresses for the device are 192.168.2.254(for LAN), 172.1.1.1(for WAN), so you need to make sure the IP address of your PC is in the same subnet as the device, such as 192.168.2.X (for LAN), 172.1.1.X (for WAN).

Please note that the DHCP server inside the device is default to up and running. Do not have multiple DHCP servers in your network environment, otherwise it will cause abnormal situation.

We also provide an auto-discovery tool which is for finding out the IP of the device. In case, you've forgot the IP of the device or the IP of the device has been changed, you can use the tool to find out the IP of the device even your PC is not in the same subnet as the device is.

Knowing the Network Application

The device can act as the following roles, and it supports WDS (Wireless Distribution System) function.

- Access Point
- WDS (Wireless Repeater)
- Bridge/Router
- WISP
- AP Client

The device provides 3 different operation modes and the wireless radio of device can act as AP/Client/WDS. The operation mode is about the

communication mechanism between the wired Ethernet NIC and wireless NIC, the following is the types of operation mode.

Router

The wired Ethernet (WAN) port is used to connect with ADSL/Cable modem and the wireless NIC is used for your private WLAN. The NAT is existed between the 2 NIC and all the wireless clients share the same public IP address through the WAN port to ISP. The default IP configuration for WAN port is static IP. You can access the web server of device through the default WAN IP address 172.1.1.1 and modify the setting base on your ISP requirement.

Bridge

The wired Ethernet and wireless NIC are bridged together. Once the mode is selected, all the WAN related functions will be disabled.

WISP (Wireless ISP)

This mode can let you access the AP of your wireless ISP and share the same public IP address from your ISP to the PCs connecting with the wired Ethernet port of the device. To use this mode, first you must set the wireless radio to be client mode and connect to the AP of your ISP then you can configure the WAN IP configuration to meet your ISP requirement.

The wireless radio of the device acts as the following roles.

AP (Access Point)

The wireless radio of device serves as communications "hub" for wireless clients and provides a connection to a wired LAN.

AP Client

This mode provides the capability to connect with the other AP using infrastructure/Ad-hoc networking types. With bridge operation mode, you can directly connect the wired Ethernet port to your PC and the device becomes a wireless adapter. And with WISP operation mode, you can connect the wired Ethernet port to a hub/switch and all the PCs connecting with hub/switch can share the same public IP address from your ISP.

WDS (Wireless Distribution System)

This mode serves as a wireless repeater; the device forwards the packets to another AP with WDS function. When this mode is selected, all the wireless clients can't survey and connect to the device. The device only allows the WDS connection.

WDS+AP

This mode combines WDS plus AP modes, it not only allows WDS connections but also the wireless clients can survey and connect to the device.

The following table shows the supporting combination of operation and wireless radio modes.

	Bridge	Router	WISP
AP	V	V	х
WDS	V	V	Х
Client	V	Х	V
AP+WDS	V	V	Х

Hereafter are some topologies of network application for your reference.



Examples of Configuration



This example demonstrates how to set up a network with different device configurations. There are 2 DHCP servers (DEV1/DEV4) in the network to control the IP configuration of 2 domains (192.168.2.x/192.168.3.x). Once the setting is done, all the PCs can visit Internet through DEV1.

We assume all the devices keep the factory default setting. To make sure that user can continuing press the rest button for more than 5 seconds to restore the factory default setting.

The following descriptions show the steps to configure DEV1 to DEV5.

Configure DEV1:

- 1. Connect the ADSL modem to Ethernet port of device using Ethernet cable.
- 2. Access the web server (http://192.168.2.254) of device from the wireless station.
- 3. Use Wizard page to setup device.

Site contents	Setup Wizard
Contraction Mode Wireless	The outup wittand will guide you to configure access point for first time. Please follow the setup wittand step by step.
Firwal	Welcame to Settep Wizard.
Rebox	The Wizard will guide you the through following steps. Begin by clicking on Next.
	1. Setup Operation Mode 2. Choose your Trive Zone 3. Setup LAN Interface 4. Setup WAN Interface 5. Windows LAN Setting 6. Windows Security Setting
	Nano

4. Press "Next>>" button then set the "Operation Mode" to "Router" mode.



to
N

8. Press "Next>>" button then select the "AP+WDS" for "mode" and

Site contents:	5. Wireless	Basic Settings
Operation Mode Wineless TCPAP	This page is used to connect to your Acor the Client Mode.	configure the parameters for wireless CAN clients which may rss Point. If you want to use Wireless ISP reade, please cho
Management.	Bandt	24 GHz (B+G) 💌
	Node:	AP+WDS
	Network Type:	bistorer v
	SSID:	DEVI
	Channel Number:	11 -

9. Press "Next>>" button then select "None" for "Encryption" then press "Finished" button.

	Site contents Wisset Coperation Mode Wisses TCPAP	6. Wireless Security Setup This page down you amp for window accurry. Thus on WEP or WPA by using Encryption Keyn could prevent any searchedmil accurs to your variance network
	Freed Management E Rebot	flacepties: Non
10.	Wait for refresh	ing web page.
	Site contents Wisard Constant Mode Wireless TCP/IP Firmel Management Firmed	Change setting successfully! Please wait a while for refreshing webpage. If IP address was modified, you have to re-connect the WebServer with the new address.
11.	Use "WDS Sett	ings" page to configure WDS.
	Site contents B Woard Operation Mode Contents Basic Settings Basic Settings Basic Settings Basic Settings Baccess Control Baccess Control WDS settings	WDS Settings Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet dates. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and ther enable the WDS. Enable WDS
	Ste Suvey Gonnecting Perfile TCP/IP Fravai Management Falsost	Add WOS AP: MAC Address Commont
		MAC Address Construct Select

12. Enable WDS function and add the BSSID of DEV2 to "Current WDS AP List".



13. Since we access the device by wireless connection, it may temporarily disconnect when applying the WDS setting. After re-connecting to the device, use the "Status" page to check the settings.

Site contents	System		
Contraction of the second	Uptime	Dday:Dh/20m 6a	
Conversion Marche	Free Memory	10776 kB	
Walkers	Firmware Version	1.3.0.9a 20060712	
TONE	Webpage Version	1.3.0.9a 20060712	
Firewal	Wireless Configuratio	n	
Marsagement.	Mode	AP+WDS - Routal	
Status	Band	2.4 GHz (B+6)	
5 QuS	SSID	DEVI	
Bandwidth Centrol	Channel Hember	11	
SNMP	Encryption	Disabled(AP), Disabled(MDS)	
A DEPENDENCE	BSSID	00:00:00:04:27:28	
Tone Jone	Associated Clients	D	
Loo	Power(0F0M/G)	24 ibm	
Miscolaneeus	Power(CCKB)	27 dbn	
Upgrada Firmwara	TCP/IP Configuration	and the second	
Save Reload Exting	Attain IP Protocol	Fixed IP	
Password	IP Address	192.168.2.254	
Veboot	Subort Mask	255.255.255.0	
	Default Gateway	192.168.2.254	
	DHCP Server	Enabled	
	MAC Address	00:00:00:04 27:28	
	WAN Configuration	The second s	
	Attain IP Protocol	PPPsE Connected	
	IP Address	218.168.146.93	
	Subnit Mask	255.255.255.0	
	Default Gateway	218.168.146.254	
	MAC Address	00.00.00.04.27.29	

Configure DEV2:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you not able to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.



5. Press "Next>>" button then set the IP address of LAN interface.

Site contents Site contents Site Wand Site Operation Mode Witeless TORMP Freevall	3. LAN Int This page its used to to the device. Here y DHCP Server will be Server is your netwo	erface Setup configure the perameter ou may change the set op and running, please of when the deecs is in	e for Iscal area notwork which connects ng for IP Address, Subnat, Masik The take sum there is no another DHCP Bridge/Client Modes.
Hanagemont.	IP Address:	192.168.1.202	
	Subnet Mask:	256,258,258,0	
			Case odlad Neto

6. Press "Next>>" button then select the "AP+WDS" for "mode" and change the SSID to "DEV2".

Site contents	5. Wireless	Basic Settings
Waard Operation Mode Wireless TCP/P	This page is used to connect to your Acce the Clent Mode.	configure the parameters for windows LAN clients which may so Paint, If you want to use Windows ISP mode, please choose
Management 5 Retext	Band:	14 Oht (0+G) 💌
	Mede:	AP+WDC -
	Network Type:	Metters -
	55ID:	DEVI
	Channel Number:	11 12
	Enable Nac Cl	ene (Single Ethemet Client) Cauril ocBack Narto

7. Press "Next>>" button then select "None" for "Encryption" then press "Finished" button.

Site contents Site contents Vicent Contact Contact Witelass	6. Wireless Security Setup The page dates now setup for Vietos accests. Then on WEP or WPA by using Exception Keys could perform any manifoldarial score to your Vietos articula.	
TCPAP Freed Management Rebot	Eacryptice. None	
	Cause codied Fairled	
Wait for refresh	ning web page.	
Eltra contractor	We also the construction of the second s	

Site contents	Change setting successfully!
Constant Mode	Please wait a while for refreshing webpage.
Firwal	If 1P address was modified, you have to re-connect the WebServer with the new address.
Rebox	

8.

9. Access the web server by new IP address "192.168.2.202" then use "LAN Interface" page to disable DHCP Server.

	Ster contents Waad Cosratian Mode Windexs	LAN Interface This page is used to careful the device. Here you may atc.	• Setup gave the parameters for local area network which connects to change the setting for IP Address, Subnet Mask, DHCP,
	ANA Interface WAAN Interface Touto Management Hatagement Tubout	IP Address: Subnet Mask: Default Gateway: DHCP: DHCP Client Range: BI2.1d Spanning Tree: Clone MAC Address: NTU Size: Apply Cauges Ree	190.000.3.000 256.256.256.0 000.0 Davkied 10.100.000 1.000 1.000
10.	Wait for refreshi	ng web page.	
	Sibe contents.	Change setting succes Please wait a while fo If IP address was mod with the new address.	infully! a refreshing webpage. lified, you have to re-connect the WebServer
11.	Use "WDS Setti	nas" page to c	onfigure WDS.
	Ste contents Withed Desistion Mode Withers Statistics Advanced Setters Advanced Setters Advanced Setters Secury Access Control WIDS setters Ste Survey Connecting Partie TCPVP Fravel Reboxt	WDS Settings Weiess Distributes Syste Net the Ethernet dates. To set MAC address of other thes enable the WDS Causet WDS AP: WAC Ad Cappe Change Ren Causet WDS AP List	In uses wholess media to communicate with other APs, do this, you must set these APs in the same channel and APs which you want to communicate with in the table and In the same
		(Deelerst) (De	TAL Rost



Configure DEV3:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you not able to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.

2. Use "LAN Interface" page to set the IP address of LAN interface and disable DHCP server.

Openation Mode Wineless TCPTP	This page is used to confi the device. Here yes may stc.	gave the parameters for local area network which connects to change the setting for IP Address, Subnet Mask, DHCP,
LAN Interface	IP Address:	192.168.2.209
Four	Submot Mask:	255 255 255.0
Management	Default Gateway:	0000
Reboot	DHCP:	Duokieł -
	DHCP Client Range:	PRIMINE - PRIMINE - Services
	802.1d Spanning Tree:	Custini -
	Class MAC Address	00000000
	MTU Size:	1900

3. Wait for refreshing web page.

Site contents:	Change setting successfully!
Wisiess	Flease wait a while for refreshing webpage.
B LAN Interface B WAVI Warface B Traute	If IP address was modified, you have to re-connect the WehServer with the new address.
Fiteral	
G listert	

"Basic Settings"	page t	o change S	SSID and	CHANNE	L.		
Site contents	Wirele	ess Basic S	ettings				
Withard Operation Mode Withard Description Advanced Settings Advanced Settings Security	This page to connect to well as wre as AP and connected	I used to configure the your Access Point. Hi less network parameti clent simultaneouty br AP	e parameters for verele ere you may change r ere. Enable universal ut remember the char	esa LAN chierts who vestess encryption s repeater mode can t wel must be as sam	ch mag Iaitings as et radio act le as the		
Access Cantrol	Disat	le Wireless LAN Int	erface				
Sto Suvey	Band	24 GH2 (D+G) 🐱					
TCP/P	Node:	NP ¥					
Management	Network Type:	bisment -					
Bunner	SSID:	DEV3					
	Channel Number:	5 Y		Show Activ	Clinit		
	Enel	de Mac Clone (Singl	le Ethernet Client)				
	Enal	de Universal Repeat	ter Mode				
	Extended SSID:	[
	(once select	et and applied, within det 5	010 and channel number	will be upstaled)			
	2	SSID	BSSID	Channel Typ	s Escrypt	R557	Quality
	(Anirek)						
	-						
	Apple Ch	Ago Rost					

5.

site contents	System	THE REPORT OF
Wittent	Uptime	Dday 2h 33m 1Bs
peratern Mode	Free Memory	11362 kB
less.	Firmware Version	1.3.0 9s 20060712
₽.	Webpage Version	1.3.0.9s 20060712
ni l	Wireless Configuratio	n -
(percent)	Nede	AP - Bridge
8006	Band	2.4 GHz (8+G)
08 Contract Constant	SSID	ZPUs-G192
MART CHIEFON	Charmel Number	11
NUMER.	Encryption	Disabled
INS	BSSID	00:00:00:04:26:29
тө Хахө	Associated Clients	0
9	Power(0FDM/G)	24 dbm
ocelateres	Power(CCICIE)	27 fbm
grade Firmware	TCP/IP Configuration	li
Heritation Setting	Attain IP Protocal	Freed IP
COWERS .	IP Address	192 108 2 203
84 C	Subnet Mask	255.255.255.0
	Default Gateway	0000
	DHCP Server	Disabled
	MAC Address	00.00.00.04.28.29

Configure DEV4:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you unable to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.

2. Use Wizard page to setup device.



3. Press "Next>>" button then set the "Operation Mode" to "Wireless ISP"

Ciperation Mode	Yes can setup title function	ent modes to LAN and WLAN interface for NAT and bridging
Eroval Management Rebot	O Rauter:	In this mode, the device is supposed to connect to internet via ADSL/Cable Modern. The NAT is enabled and PCs connected with WLAN state the same IP to CP through WAN part. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or Static IP. 172.1.1.1 is the default State: IP address for WAN pert.
	O Bridge:	In this mode, the ethernet pert and wireless interface are bridged together and NAT function is disabled. All the WAN selated function and fravail are not supported.
	() Workss SP:	In this mode, the weekses steent will connect to ISP access point. The NAT is enabled and PCs connecting with the othernal point share the same IP to ISP through versions LAN. You must net the withings to clean mode and connect to the ISP AP. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP cleart or State: IP.
		Ond office Netwo
Press "Next>>	" button ther	n disable "Time Zone" function.
Sate contents	2. Time Z	one Setting
- Witard	You can maintain f	the system time by spectramition with a multir time space more
Greation Mode Wireloss	the internet.	and the second statement and the second second second
Guessian Mode Wireloss TCP/IP Frewal	the internet.	fiest update
Operation Mode Wireless TCP/IP Frewall Management Reboxt	the internet.	fient update
Coenstion Mode Wireloos TCP/IP Frewal Management Reboxt	The Internet.	first updats 1) (1017-01001ecto Terr III in Cherto, Tarasa (1010000) (101 11) (1017-01001ecto Terr III in Cherto, Tarasa (1010000) (101000) (10100000) (1010000) (1010000) (10100000) (10100000) (10100000) (10100000) (10100000) (10100000) (10100000) (10100000) (10100000) (101000000) (101000000) (101000000) (1010000000000
Gaenstion Mode Wireloss TCP/IP Frevail Miningement Frebold	The Internet Enable HTP o Time Zone Selec HTP server :	fiest update 1 (CAT - Mathematic Sear) - C. & Conston Space - Conston - Space (CLT-ALA: - Mark Agentical - Space - Conston
Gaession Mode Wireloss TOP/IP Frewall Management Reboxt	The Internet.	fiont update 1 (2017-3-1919-5): Swe (22.8: Constr. Space 2019-50): gl

5. Press "Next>>" button then set the IP address of LAN interface.

ention Mode roless PNP roval	This page is used to to the device. Here y DHCP Server will be Server in your netwo	configure the parameters numary change the sette up and ranking, please a sk when the device is in E	far local area network which connects g for IP Address, Subnet Mask. The skie sure there is no another DHCP volge/Clivit Modes
agement st	IP Address:	192.168.3.1	
	Subnet Mask:	245,255,255.0	

6. Press "Next>>" button then select the "DHCP Client" for "WAN Access



7. Press "Next>>" button then select the "Client" for "mode" and change the SSID to "DEV4".

Site contents	5. Wireless	Basic Settings
Wizerd Operation Mode Wireless TCP/IP	This page is used to connect to your Acce the Cleant Mode.	configure the parameters for weekees LAN clients which may no Paint. If yos want to use Witelees SP mode, please choose
Management	Band: Mede:	14 GhtdH+G ⊯ Cline ⊯
	Network Type:	BEEDRORE W
	SSID:	DEVA
	Channel Number:	
	Enable Mac Cl	ene (Single Ethemet Client)
		Oani cclict Nirto

8. Press "Next>>" button then select "None" for "Encryption" then press "Finished" button.

Site contents:	6. Wireless Security Setup
Conversion Mode Windees	This page allows you seeps the wardets aroundy. Turn on WEP or WPA by using Encorption Keys could preven only unarchooling access to your whether network.
Freed Management Bebart	Escryption: Nor
	Caul other Failed

9. Wait for refreshing web page.



10. Change the IP address of your PC to 192.168.3.x then access the web server by the new IP address "192.168.3.1" and use "Status" page check the setting.

Site contents: System	
Uptime	0day:2h:96 m 36a
Free Momery	10696 kB
Firanware Version	1.3.8.9a 20060712
Webpage Version	1.3.0.9a 20060712
Firewall Witeless Configurati	80
Marsonerd Note	Infrastructure Client - Router
Elater Band	2.4 GHz (B+G)
OuS SSID	DEV4
Eatdwells Control Channel Number	5
Encryption	Disabled
BSSID	00:00 00:00 00:00
State	Scenning
RSSI	0
Miccelateres AP Inte	
Upgrada Firmware TCP/IP Configuration	Add States
SaverReload Setting Anale IP Protocol	Fixed IP
Password IP Address	192.168.3.1
Subnet Mask	255.255.295.0
Default Gateway	192, 168, 3, 1
DHCP Server	Enabled
MAC Address	00:00:00:05:12:13
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server.
IP Address	0000
Subnet Mask	0000
Befault Gateway	0000
MAC Address	00:00:00:05:12:14

11. If the "State" of "Wireless Configuration" is not "Connected" or you want to refresh the "RSSI ", please use "Site Survey" page to re-connect a AP

ard The	his page provides to used, you could cho	col to scan the wineless lose to connect it many	: tetwork: If a saily when cli	ny Acce ent mod	es Point or it ris enabled	185 in			
lasis Settings Idvanced Settings	STID	REERO	Chund	Type	facept	REEL	Quility	Select	20
cosus Cortral	DEVI	00.000004 27:28	11 (8+3)	AP.	80	67149dim)	96	0	0
VDS setings		00.0£14.00.80.11	1(8+0)	AP.		61 (43 dan)	新	0	0
Innecting Profile	Gaved)	000556304669	11.00	AP	90	40177(dan)	90	0	0
NP.	INTECH-IF	000596401143	18+9	AP	355	36(-6il dan)	92	0	0
eront 2	INTECH-JF	0005.9e 80 ki lai	11 (B+C)	AP.	je	29(-72.dan)	85	0	0
	TLN Midelah	0000.00msbint	7 (B+G)	AP	30	(15 dan)	68	0	0
	Aros.	0005.9e10 10107	6.8+9	AP	-10	(J) (-10 diard)	34	10	0

Configure DEV5:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you unable to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command "arp –d" then you can access the web server of device using the default IP address.

2. Use Wizard page to setup device.



3. Press "Next>>" button then set the "Operation Mode" to "Wireless ISP"



5. Press "Next>>" button then set the IP address of LAN interface.

This gage is used to to the device. Here y DHCP Server will be Server in your netwo	configure the parameter ou may change the setti up and remning, please is of when the device is in t	far local area network which connect g for IP Address, Subnet Mask. The also sure there is no another DHCP idge/Client Modes	02
IP Address:	192.168.2.205		
Subnet Hask:	215,215,255.0		
	This page is used to to the device. Here y DHCP Server will be Server in your netwo IP Address: Subset Hask:	This page is used to configure the parameters to the device. Here you may change the setting DHCP Server will be up and ranning, please on Server in your network when the device is in Br P Address: Subset Mask: 215.255.0	This page is used to certifyine the parameters for local area network which connects to the device. Here you may change the earling for IP Address, Subnet Mack. The DHCP Server will be up and ramming, please make such there is no another DHCP Server in your network when the device is in Bridge/Client Mades P Address: 199.168.2.05 Subnet Mask: 285.255.0

6. Press "Next>>" button then select the "Client" for "mode" and change the SSID to "DEV5".

Site contents	5. Wireless Basic Settings		
Witzerd Operation Mode Wireless TCPIP Frewall Nanagement Reboot	This page is used to configure the parameters for windows LAN clients which may connect to your Access Point. If you want to use Wasters SP mode, please choose the Client Mode.		
	Band: 3.4 GHz (H+G) w Mede: Clina w Network Type: Microschur w Sall-		
	Channel Number:		
	Enable Not Clene (Single Ethemet Clent) Oncel cdick Nerto		

7. Press "Next>>" button then select "None" for "Encryption" then press "Finished" button.

Site contents: Site contents: Site Consultant Made Windess TCPAP Site Contents Site Conten	6. Wireless Security Setup The page directory to setup for vietness accounts. Then on WEP or WPA by using Encorption Keys and performing manifoldated accounts your vietness artificial Encorposition: None
Wait for refres	hing web page.
Site contents Wizard Gamilian Mode Wireless TCP/P Finwal	Change setting successfully! Please wait a while for sefreehing webpage. If 1P address was modified, you have to re-connect the WebServer with the new address.

8.

9. Access the web server by the new IP address "192.168.2.205" and use



RSSI

E Reboot

AP lafe

IP Address

Submit Mask

DHCP Server

MAC Address

Default Gateway

TCP-IP Configuration Attain IP Protocol

D

Faud P

0.000

Deabled

192, 168, 2, 205

255 255 255 0

00 00 00 04 22 21

to refresh the "RSSI ", please use "Site Survey" page to re-connect a AP.

Constant Made	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.								
Advanced Settings Security	251D	RED	Chinad	Type	Entrypt	RSSI	Quility	Select	
Arturery Arturery Arturery Arturery VOS antonas VOS antonas Constanting Profile Constanting Profile Traveal Management Fishant	DEV1	00.000004.2552	11 (8+0)	NP.	nc-	61 (-13 dim)	- 85	0	R
		110600313000	1 (8+G)	NP:	30	601-54 dim)	H.	0	K
	ZINTECH-OF	00059e8051e3	1 (B+O)	42	55	41 (-65 dim)	90	0	1
	Ziveti	00.05.9±80.46.69	11:00	NP.	30	40(-70-fim)	99	0	
	22010323-35	0005.9e KO M M	11(0+0)	AP.	303	29(-72.dus)	28	0	
	RTL8186-defind)	10-Mim 00.0000	7(B+C)	42	an ca	25(-74 dim)	89	0	
	date.	00.05.9e.8l 89.67	6 (B+Cl	12	30	13 (-82 dim)	67	0	1

Basic Settings

Site contents: Wire	eless Basic Se	ettings				
Wated Constant Made Constant Made Constant Descriptings B Advanced Settings Constant Constant B Security	ge is used to configure the to your Azzess Point. Her windess network parameter and client simultaneously bur and AP.	parameters for wonin a you may change v rs. Enable universal (remember the chao	es LAN clients indices encryp repeater mode nel must be as	i which may from settings as can let redo act i same as the		
Access Control B WDS antings	sable Wireless LAN Inter	face				
Band:	24 GHb (B+G) 🐱					
TCPAP Mode:	AP =					
Freed Network Type:	ik <u>identitier</u> -					
SSID:	healt					
Chans Numb	al 11 💌		Show	Actwident		
	nable Mac Clone (Single	Ethernet Client				
	nable Universal Repeate	r Node				
Extens SSID:	led					
force as	iected and applied, extended 31	D and chancel number	vill be updated)	_		-
	SSID	BSSID	Charnel	Type Encrypt	RSSI	Quality
1000						
	Mar - A Street					
Appl	Changes Root					

Disable Wireless LAN Interface

Disable the wireless interface of device

Band:

The device supports 2.4GHz(B), 2.4GHz(G) and 2.4GHz(B+G) mixed modes.

Mode:

The radio of device supports different modes as following:

1. AP

The radio of device acts as an Access Point to serves all wireless clients to join a wireless local network.

2. Client

Support Infrastructure and Ad-hoc network types to act as a wireless adapter.

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.

Infrastructure:

This type requires the presence of 802.11b/g Access Point. All communication is done via the Access Point.



Ad Hoc:

This type provides a peer-to-peer communication between wireless 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 including Firewall and WAN settings.

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

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

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
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.

Note :

Any unreasonable value change to default setting will reduce the throughput of the device.

Interestings and any second se	for more techni is LAN. These inges will have	cally advanced unans who have a sufficient settings shauld sat be changed unless you on your Access Point.				
Authentication Type:	O Open Sy	stern O Shared Key ® Auta				
Ecess Control Fragment Threshold:	2346	(256-2346)				
RTS Thrusheld:	2347	(0-2347)				
Beacos Interval	300	(20-1024 me)				
ACK Timing:	94	(0-265 * 4 us)				
Client Expired Time:	300	(101-40000000 sec)				
MTU Size:	1500	100-1000				
Data Rate:	Anu 🛥					
Preamble Type:	Preamble Type: OLang Preamble OSbart Preamble					
Broadcast SSID:	@Enklet	ODisabled				
IAPP:	@ Enabled	ODisabled				
802.11g Protection:	C Enabled	ODisabled				
Block WLAN Relay:	Othisblet	Obtabled				
Turbo Hode:	O Enabled	Disubled (auto)				
Aggregation Mode:	Enabled	Disabled				
Tx Burst Mode:	Endlet	- Disabled				
Transmit Power(OFD)	n) 24 dbm 💌					
Transmit Power(CCK)	27 dhan 🐱					

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.

Beacon Interval

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

ACK Timing

Acknowledgement Timing, is the amount of time that device wait client's response. This concept is related to EIFS (Extended Inter-Frame Space). The EIFS interval shall begin while the device is idle after detection of the erroneous frame. The EIFS is defined to provide enough time for another device to acknowledge what was, to this device, an incorrectly received frame before this device commences transmission. The default ACK timing is 91*4us. You may need to change this value due to the environment or distance.

Client Expired Time

The client expired time determines time interval the client need to re-associate with the device while client is idle. The default client expired time is 300 sec.

MTU Size

Maximum Transmission Unit, the default MTU size is 1500. The MTU setting controls the maximum Ethernet packet size your PC will send. Why a limit? Because although larger packets can be constructed and sent, your ISP and Internet backbone routers and equipment will fragment any larger than their limit, then these parts are re-assembled by the target equipment before reading. This fragmentation and re-assembly is not optimal. You may need to change the MTU for optimal performance of your wireless LAN traffic.

Data Rate

The standard IEEE 802.11b/11g supports 1, 2, 5.5, 11 / 6, 9, 12, 18, 24, 36, 48 and 54 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.

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.

IAPP (Inter-Access Point Protocol)

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 is as the following figure.

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

<u>Note</u> : For implementing the roaming function, the setting MUST comply the following 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 eleven transmission output power levels from 17 to 27dBm for CCK (802.11b) mode and eight transmission output power levels from 17 to 24dBm 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.

Cperation Mode	The page allows you setup the venesis security. Tain on VEP of Week by using Encryption Keys could prevent any unauthorized access to your wheleas network					
Basic Settings Advanced Settings Security B. Security	Authentication Type: O Open System: O Shand Kay ® Auto					
Access octers WDS settings Site Starwy Site Starwy TCPAP TCPAP Forwell Management	Use 802.1x Authentication WEP Sabits WEP 1285ts Enable MAC Authentication WPA Authentication Mode: Enterprise (RADUS) Passonal (Pre-Shared Kay) Pre-Shared Key Fermat: Pre-Shared Key					
	Enable Pre- Authentication Authentication RADIUS Pat P address Password Server:					
	Note: When encryption WEP is selected, you must set WEP key value Apply Charges Faces					

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

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.
| of as the encryption a | ey, and select ASCI or Hex as the format of input value. |
|------------------------|--|
| Key Length: | 64.1ar 🐱 |
| Key Format: | Hes. (10 characters) |
| Default Tx Key: | Easy 1 🐱 |
| Encryption Key 1: | ****** |
| Encryption Key 2: | ****** |
| Encryption Key 3: | ******** |
| Encryption Key 4: | ******** |

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 OWEP 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.

Site contents Witwel Generation Mode Without Book Settings Advected Settings Advected Settings Societ	Wireless Basic Settings This page is used to configure the parameters for wheless LAN clients which may connect to your Access Point. Here you may change wheless encryption settings ao well as wheless network parameters. Enable universal regeator mode can let ratio act as AP and client sensitizereoxy but remember the channel must be as same as the connected AP.
MC Access Central MDS settings Ste Savey Connecting Parkle	Disable Wireless LAN Interface Band: 24 GHz (5+3)
Farwall	Node: Clas
Pa Rebox	4 SSID: Tege-AP-CCD
	Channel Bor Acte Chen Rumber: Bor Acte Chen Enable Mac Clone (Single Ethernet Client) Exable Universal Repeater Mode Extended SSID:
	5510 USSID Channel Type Lecryot R551 Quality
	5 Apply Chington (Rever)





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.

B Wized Constant Mode Viscons Basic Settings	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.									
Advanced Settings	SID	RIED	Channel	Type	Escrypt	RSSI	Quality	Select		
Access Control	WLANG_TERT	000000000000000	11 (B+C)	NP.	nc-	61 (33 dim)	85	3	0	
WDS settings		00.06.54.00.90.18	1 (8+G)	NP:	30	601-54 dim)	H.	0	0	
Conserver Profile	ZINTECH-3F	00069e8081e3	1 (B+O)	48	55	41 (-65 dim)	90	0	0	
ТСРИР	Zivreil	00.05.9± 80.45.69	日田	NP.	30	40(-70-fim)	99	0	0	
Fisheral Management	28/09/29-28	0005.9e1006164	11(0+0)	AP	301	29(-72.dus)	28	0	0	
5 fishaat	RTL8186-defindt	10-Mi = 00.0000	7(B+C)	AP	and Car	25(-74 dim)	89	0	0	
	dates.	00.05.9e 81 69.67	6 (B+Cl	12	30	13 (-82 dim)	67	0	0	

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.

Site contents.	System	A MORE AND THE R	12
5 Waard	Uptime	0day 01 16m 32s	
Coeration Made	Free Nemary	11912 88	
Winness	Firmware Version	1.3.0.99 20060712	
TCP/F	Webpage Version	1.3.0.9x 20060712	
Filovali	Wireless Configuratio		
Also appreciate	Mede	Infrastructure Client - Bridge	- 01
E Status	Band	2.4 GHz (E+G)	
Ce8	550	WLAN_G_TELT	
Basdwidth Control	Channel Number		
	Encryption	Disabled	
TOTALS	BSSID	00:00:01:02:03:04	
B True Zone	State	Casserted	
B	RSS	36.572 dtm. Quality 79)	
E Macelanous	AP into		
Upgrado Firmware	TCP/IP Configuration		2
E Eave/Related Setting	Attain IP Protocol	Fixed IP	- 2
Passend	IP Address	192 168 2 205	
E fichaut	Saluret Hask	0.000 200 200 D	
- 92	Default Gateway	0000	
	DHCP Server	flicabled	
	MAC Address	00.00.00.01.72-71	

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.

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.

SRP contents. SRP contents. Constant Mode Static Satings Satis Satings Security Access Control B Access Control B Access Control	Wirele This page is connect to well as vice as AP and connected	ess Basic Se s used to configure the p your Access Point Hand less network parameter client simultaneoutly but AP.	ttings aranators for weaks you may change wi a. Enable universal in remember the chann	os LAN client releaa encryp speater mode rel most be a	s which n tion satt can let n t same a	nay ngs 4s ado act s the		
WOS entrops Site Survey Sovecting Profile TOPAP Fainnal Matagement BRebeet	Band: Mode: Network Type: SSID: Channel Number:	34 GHs (9+0) - Clins - lafsetschat -			Acres 1			
4	Enal Estended SSID: Erres select	tie Nac Clene (Single de Universal Repeater et ent applietuerendel 11 5510	Ethermet Client) Node E end chienel number + BSSID	f is point Channel	Туре	Encrypt	#55I	Coally

Configuring Universal Repeater

This device can be configured as a Repeater. In this mode, the device can extend available wireless range of other AP let user can link the network that they want, Also the device working as AP and Repeater same time.

Following two ways describe how to make Universal Repeater effective.

 Enable Universal Repeater Mode and then select a SSID in the Table that you want. Final click Apply Changes button to take effective. (Click Refresh button to make table renew)

Generation Mode Generation Mode Generation Mode Generation G	Disable Wireless LAN Interface Band: 24 GHz (9+0) Node: AP Notecoli Type: SSID: 2Plot-0192 Channel II Enable Mac Clone (Single Ethemet Client) Enable Universal Repeater Mode Extended				Show Act	er Cleas	ן		
	SSID:								
	SSID:	d and applied, a dands	E STAT and charmed mumber	and barget	ited)	Manager 1	BARKI.	· water	-
	SSID:	ssio	USSID UDDe 14 00 ID 15	Channel	Type AD	Encrypt	RSSI 37 km drai	Deality	Select
	SSID: WLANCO	nd and applied, other do SSID TECT a fault	00.00 00 14 00 10 18 00.00 14 00 10 18	Channel 1 (E+5) 1 (E+6)	Type AP	Encrypt ro	RSSI 32.670 dbmj 16.660 dbmj	Duality III 76	Sele

Note: Under **AP** • **WDS** and **AP+WDS** mode, The Universal Repeater can take effective.

2. Enter specific SSID in the Extended SSID field and then click Apply Changes button to take effective.

Site contents	Wireless Basic Settings		
Wizart Crenation Mode Desit Settings Advected Settings Bosic	This page is used to cardigure the parameters for wireless, connect to your Access Paint. Here you may change wirel wold as wireless network parameters. Enable universal rope as AP and client simultaneously but remember the channel connected AP.	LAN clients which may less encryption settings as outer mode can let radio act must be as same os the	
Access Control S WOS settings	Disable Winsless LAN Interface		
5 Site Starwy 5 Connecting Profile	Band: 14 (Hu (B+C))		
TCP/IP Fitewali	Made: AP		
Management B Rebot	Type:		
	Channel II	Slow Actor Gant	
	Enable Mac Clene (Single Ethernet Client)	2	
3	Enable Universal Repeater Mode Extended WLAN, G, TET		
	(analy related and approximated \$10 and charged (under with	te goldet) Phonesel finans factores fillet	e.
	3300 13300 1	Channel Lype Intrype Rasi Gually	1
	Refmh		
	Apply Clauges Bener		

Ch 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.



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:







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.



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 4. 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.



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.

Witzard Operation Mode Windows TCPVP Frence Port Filtering MAC Printing MAC Printing Frittering Frittering	Entries in this table are local network to Internet securing your local network debuilt palicy in Route p Enable Part Filter Part Range:	used to restrict[allow] or through the Gateway I ors. Denied or Allowed aga ing (deeled line) Pretocal: Both	estain tyges of date poo No of such Store cast Int depends on your P	kots fram your ia holgful in forwarding	
			Alexandra a	in contraction of the local distance of the	
	Piet Ringt	Protocol	COLLECT	ACCUSE 1	
	Pint Rings 20-21	TCP-41DP	FTP		
	Pret Range 20-21 20	TOP-100 TOP	FTP		

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.

Operation Mode Wireless TCP/P Firework	Entries in this table are o local network to internet securing your local netwo default policy in Route po	se helpfal in 9 helpfal in 9 forwarding			
P Filling	🖅 Enable Port Filter	ing (allowed list)			
MAC Filtering	Part Range:	Protocal: Both	Commont:		
Fort Farwarding	Activities of the second of the				
Feet Farwarding					
Fort Forwarding 5 DMZ 5 VPN Management	Apply Changes Re	ली)			
First Farwarding E DMZ VPN Management Rebot	Apply Changes Re				
Fort Forwarding E DMZ E VPN Management Reboot	Apply Changes Re	9 1			
Fort Forwarding E DMZ E VPN Management Reboot	Apply Changes Re Current Filter Table: Post Range	or Protocol	Createrial	Start	
Fort Farwarding E DMZ E VPN Maragement Reboot	Apply Changes Re Correct Fifter Table: Part Range 20-21	Princel TCI+LEP	Convent PD	Stint	
Fort Farwarding E DMZ YPN Maragement Reboot	Apply Chings Re Correct Filter Table: Print Rauge 20-21 20	Protocol T/3+USP T/3F	Convent PD Take	Steel	

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.

Sibe contents: Wizard Coeration Mode Wrieters TCPAP Part Fileerers B. Part Fileerers	IP Filtering Entries in this table are a local network to Internet to securing your local retwo default policy in Route per Exable IP Filtering	and to restrict(allow) hrough the Gateway rk. Denied at Allowed ge.	certain types of data p Use of such filters ca list depends on your	nacivats itom pilat n be kelpta in IP forwarding	
MAC Filtering	Local IP Address:	Protocel:	Both 💌 Comment	£	
A OVE B VFN Management. B Rebot	Apply Chings Table:	٥			
	Local P Address	Protocol	Countri	Select	
	192168211	4.1	Climi 11		
	190168.2.23	RPHOF	Clies 23		
	192164.3.35	UDP	Class 36		
	190164123	R39400P UDP	Class 23 Class 35		

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: Wissel Coordion Made Windess TCPAP Torong	IP Filtering Entries in this table are used to restrict(allow) certain types of data packets from your local network to internet through the Gatoway. Use of such filters can be helpful in sociaring your local network. Danied or Allowed list depends on your IP forwarding default policy in Raste page.					
E P Fibring	Local IP Address: Protocol: 500. Comment:					
Pat Forwarding						
G DMZ G VPN Management Refect	Apply Charges Res					
	Local IP Adves	Pastocol	Connext	Select		
	190168311	709	Clerv 11			
	1921/08/2/23	702+000	Climt 23			
	HEE 664.001	UDP	Cliny 35			
	Delete Scienced Dele	# All From				

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.

Wizard Operation Mode Viewess TCD4P Travel Put Fibering S Pithering	Entres in this table are used to n local network to internet through security your tocal network. Den default policy in Reute page	estinct()allow) certain types of data the Gatoway. Use of such there o and ar Allowed list depends on you aind lint	packetis from your or be kelpful in r IP forwarding	
MAC Flares Pat Forwarding DMZ VPN Management Febeet	MAC Address: Apply Clarges [Root] Current Filter Tables	Connent		
	MAC Address	Consent	Sidect	
	00000312:01:02	Gint1		
	00:00:00:06:06:10	Cint3	0 1 0	

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.

Operation Mode Westers TOPIP Course Topip Freese Freese	Entries in this table are used to restrict[allow] certain types of data packets from your local network to leternot through the Gateway. Use of such fibers can be helpful in secaring your local network. Denied or Allowed kit depends on your IP forwarding default paticy in Route page.				
MAC Fiterry	MAC Address:	Comment			
For Panalony F	Apply Chouges [Rent]	Apply Classes Rent			
Management Reboot	Current Filtur Table:				
Management Reboot	Carrent Filter Table: NAC Address	Countral	Select		
Management Reboxt	Carrent Filter Table: MAC Alteres 000003120102	Countral Client I	Select		
Management Reboot	Carrent Filter Table: MAC Alteres 0000031243 02 00000060630	Countral Client Client			

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



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
Coperation Mode Windess TEPAP	Entries in this table allow you're automatically redirect common network services to a specific reachine behind the NAT feawall. Those 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 feavall.
Dart Filtering	Enable Pert Forwarding
MAC Fileson Post Forwarding Cover Source Source Management Rebust	IP Address: Protocol: Dol. Port Range: Comment:
	Lord P Allens Person Per Part Country Stat
	And a provide a state of the st
	Dian Distan Dian AL Real

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

About 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	

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.

Site contents	DMZ	
B Woard Denstion Mode Winkers TCP/IP	A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ heat conterns devices accessible to Internet Italic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.	
Fort Fittering Fort Fittering MAC Fittering Fort Fatering Fort Fatering DM2 DM2 VFN Management Breboot	CMZ Host IP Address:	

DMZ Host IP Address:

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

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



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"

Ste contents	WAN Interfa	ce Setup	
Constant Made Wissiens	port of your Access Pol Client, PPPsE or PPTP	rt. Here you may change the access method to Static IP, DHCP by click the item value of WAN Access type.	
LAN Interface	WAN Access Туре:	Stric P 🖉	
Fiteval	IP Address:	1723.1.4	9
Management (S. Dahard	Subnet Hask:	155.355.255.0	
C HANNEL	Default Gateway:	172.1.1.254	
	DHS 1:		
	DHS 2:		
	DHS 3:		
	Clana MAC Address:	0000000000	
	🔲 Enable sPnP		
	🖻 Enable Web Ser	ver Access on WAN	
	🗌 Enable Paec pae	s through on VPN connection	
	🗌 Enable PPTP par	in through on VPN connection	
	Enable L2TP pas	a through on VPN connection	
	Apply Clauges (R		

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 Wizard Coperation Mode Witeless	WAN Interface Setup This page is used to candigue the parameters for Internet network which connects to the WAN pot of sour Access Paint. Here you may change the access method to Static IP, DHCP Client, PPPsE or PPTP by click the term value of WAN Access type.			
LAN Interface	WAN Access Type:	State F 💗		
Finado	IP Address:	1723.1.1		1
Management IN Report	Subnet Mask:	153,153,153,0		
Contract.	Default Gateway:	172.1.1.254		
	DNS t:	1		
	DNS 2:	1		
	DHS 3:	-		
	Clene MAC Address:	00000000000		
	🔲 Enable sPnP			
	🖻 Enable Web Ser	ver Access on WA	n	
	🗌 Enable IPsec par	s through an VPN	connection	
	🗌 Enable PPTP par	a through on VPN	connection	
	Enable L2TP pas	a through on VPN	connection	
	Apply Changes (R	80		

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.
Default Gateway:	The IP address of Default Gateway provided by your ISP or MIS. Default Gateway is the intermediate network device that has knowledge of the network IDs of the other networks in the Wide Area Network, so it 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 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)

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 Worked Wrekes Tohr	WAN Interface Setup This page is used to configure the parameters for internet network which cannects to the WAN pet of your Access Point. Here you may change the access method to Static IP, DHCP Client, PPPuE or PPTP by click the item value of WAN Access type				
WAN Interface	WAN Access Type: DBCP Class -				
Foute Frewall Management Bologet	Attain DNS Automatically Set DNS Manually				
The second	DNS 1:				
	DWS 2:				
	DWS 3:				
	Clene MAC Address: 00000000				
	🗖 Enable uPaP				
	🕑 Enable Web Server Access on WAN				
	Enable IPaec pass through on VPN connection				
	Enable PPTP pass through an VPN connection				
	Enable LZTP pass through on VPN connection				
	Apply Clouges Rese				

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:	PPPoB	*
Cperator: Made Waskes	User Name: Password:	-	
LAN Meetice	Connection Type:	Costanoes	Count Remain
Fished	MTU Size:	1412	(1-1088 mmstas) (1400-1492 bytes)
Statuptert	C Attain DNS Autom Set DNS Manually	atically	
	DNS 1: DNS 2:	_	
	DHS 3: Classe MAC Address:		
	Enable sPnP		
	Enable Web Ser	ver Access on Is through an	WAN VPN connection
	🔲 Enable PPTP par	as through on	VPN connection
	Apply Changes (B)	a through on	VPN connection

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.

IP Address	172112	1			
Sabaat Bask	166.166.266.0				
Same II Address	121111				
Server of Address.	area a				
User Name:					
Pasawordt					
MTU Size:	1412	(1400-1492 bytes)			
MPPE:	() Enabled	Obsabled			
O Attain DHS Autom	atically				
Set DNS Manually					
DNS 1:					
DNS 2:					
DHS 3:	1				
Clene MAC Address:	30000000000				
🔲 Enable sPriP					
🖻 Enable Web Ser	Exable Web Server Access on WAN				
🗌 Enable Prec pa	Enable Prec pass through an VPN connection				
📋 Enable PPTP pa	as through on	VPN connection			
Enable L2TP par	a through on '	VPN connection			

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 Static IP WAN access type

WARACCON WARACCON Type	e Dee P				
IP Address:	1221.1.1				
Subnet Mask:	25.25.250				
Default Gateway:	172113294				
DWS 1:					
0WS 2:					
DWS 3:					
Clene MAC Addre	mai 001122334455				
🔲 Enable uPoP					
🖻 Enable Web	🖻 Enable Web Server Access on WAM				
E Fachia Base	Enable IPsec pass through on VPN connection				

2. Clone MAC address for DHCP Client WAN access type WAN Interface Setup

With Michael Description Muchael With Needed With Needed With Needed With Needed With Needed Prove Prove
B Construction WANN Interface WANN Access Type: D Freeval Freeval C Amain DNS Automatically Muragement Set DNS Mensally DNS 1: DNS 2: DNS 3: DNS 3: Cheme MAC Address: DX12234455
Anala DMS Automatically Set DNS Mensafly Set DNS Mensafly DNS 1: DNS 2: DNS 3: Cleme MAC Address: 0012203455 Enables uPnP
Set DNS Mensafly DNS 1: DNS 2: DNS 3: Cleme MAC Address: 0012203455 Exables uPnP
DNS 1: DNS 2: DNS 3: Cleane MAC Address: 000122334455
DNS 2: DNS 3: Cleve MAC Address: 0012203455 Enable uPnP
DNS 3: Cleane MAC Address: 001122334455
Clene HAE Address: 00112233455
Enable uPoP
🗠 Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through an VPH connection
Enable L2TP pass through on VPN connection
Apply Changes Rent

3. Clone MAC address for PPPoE WAN access type

Site contents	WAN Access Type:	PPPvE	4		
Coperation Mode	User Name:	87043600464	nit att		
Wednes	Password:			Ī	
LAN Interface	Connection Type:	Contairios	4	Count	
Ande	Idle Time:	3	(1-1000	minutes)	
Freed	MTU Size:	1412	(1400-1	492 bytes)	
🖺 Rebout	© Artain DHS Autor © Set DHS Manually DHS 1: DHS 2: DHS 3:	/			
	Clone MAC Address:	0012233845	5		
	Enable sPnP				
	Enable Web Ser	ver Access or	WAN		
	🗌 Enable IPsec pa	as through an	VPN cen	nection	
	Enable PPTP pa	as through on	VPN con	nection	
	Apply Changes 1 (3	ss through on	VPN con	ection	

4. <u>Clone MAC address for PPTP WAN access type</u>

Site contents:	WAN Access Type:	FPTP 🛩
Coperation Mode	IP Address:	172113
TOP/F	Subset Mask:	255 255 255.0
LAN Interface	Server IP Address:	172.144
Roze	User Name:	
Frend	Pasoword:	
E Rebast	MTU Size:	1412 (1400-1492 bytes)
- International -	MPPE	@Enulted ODisabled
	Artain DHS Autom Set DHS Manually DHS 1: DHS 2: DHS 3:	arically r
	Close MAC Address:	001122334453
	Enable uPnP Enable Web Sen Enable Prec par Enable PPTP par Enable L2TP par	ver Access on WAN as through an VPN connection as through on VPN connection as through on VPN connection

5.	Physical LAN interface MAC address clone
----	--

Operation Mode	This page is used to confl the desire labor and point	figure the parameters for local area network which connects to a choice the parameters for E. Addesse, School Misch, CHCS.
Webss	eli.	f confige the sound of a sound sound matter, process
Ba LAN Interface		
WAN Interface	IP Address:	102.168.2.254
Freedo	Submet Mask:	255.255.255.0
Management	Default Gateway:	0000
Rebox	DHCP:	Same 🚽
	DHCP Client Range:	[1921642100 - [1921612200] [200# Clear]
	002.1d Spanning Tree:	c Dustini 🛥
	Clone MAC Address:	0001122534455
	MTU Size:	1900

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.

e contents:	LAN Interface	e Setup
Wizard Operation Mode Windese TCRNI	This page is used to canfi the device. Here you may atc.	figure the parameters for local area setwork which caseacts to change the setting for IP Address, Subnet Mask, DHCP;
LAN Interface WAN Interface	IP Address:	192.568.3.354
Roze Treval	Subnet Mask:	155 155 155.0
Masagement.	Default Gateway:	0000
*5361	DHCP:	Serves 💌
	DHCP Client Range:	192.168.2.100 - 192.168.2.200 Diow Cliew
	802.1d Spanning Tree:	Destand 🛥
	Clone MAC Address:	000000000
	MTU Size:	1500

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.

fens fD			
3	🕑 Bandwidth Control		
Earlie I	Upstream Data Rate:	20000	(15-24000 kiters)
	Upstream Latency:	50	(20-1024 ms)
Bandwidth Control 2	Upstream Burst Packet:	25600	(1600-40000 Bytes)
Italistics	Downstream Data Rate:	24000	(15-24000 ktps)
Junes Erre Zane	Bownstream Latency:	30	(20-1024 ms)
	Downstream Bunt Packet:	25600	(1600-40000 Bytes)

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%.

Site contents:	QoS setting	
Wizett Cperation Made Winkess TCPAP Finenal Consent	Entries in this table are used to restrict certain quality of service for your network. Use of such setting can be helpful in treffic control or queuing discipline of your network. The traffice control arrang WLAN stations is fatile,it works between LAN(WLAN)/WAN or LAN/WLAN. The debuilt queue is Med and once the bandwidth borrowed is enabled , the higher bandwidth priority will get the remaining bandwidth first.	
Sofue Gos Gos Bandweb Control Bistance Sofue Sofue	OeS Enabled OeS Enabled Max Throughput : 2000 (dops) Bandwidth Ratio (HML): 30 (100 (30) Apph Cleage	

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%)
 - ☑ QoS Enabled☑ 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
	by 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 Match	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.

Sre Aile	Dat Adr	Ste MAC	Dist MAC	Sto Post	Dat Post	Pau	Pri	Filtur	TOS	Set
192, 168.2.11/24	140,113.27.181/24	00:05:9e:00.aa.ee	(*)	21-21	21-21	TCP	LOW	0	Normal	
anywhere	anywhere	+	(+)	00-00	•	TERVUDP	MED	a	Normal	
192.168.2.13/24	anywhere		- 141	50000-50050	-	TOPUDP	LOW	2	Normal	
anywhere	192,168,2,12/24			Survey Survey		TCP/UDP	MED	1	Normal	
192 168 2 16/24	anywhere	00:05:9e:00:aa:cc	141	+	-	TCP/UDP	HIGH	0	Normal	

An example for usage



For 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.

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**.

Stc Adr	Dat Adu	SIC MAC	Dax MAC	Sic Part	Dat Part	Pre	Par.	Filter	TOS	Sel
92.168.2.11/24	anywhere		+	5060-5061		TOPUDP	HCH	0	Normal	
92.168.2.12/24	anywhere	1.7.		21-21		TCP	LOW	0	Normal	
92.168.2.13/24	anywhere		14	80-80	14	TOP	MED	0	Normal	

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.

Enable Static Route				
IP Address:	192.168.3.0			
Subnet Mask:	255.255.255.0			
Default Gateway:	192.168.2.1			
Apply Changes	Reset Show Route Table			

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	how 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 Rou	ite
IP Address:	
Subnet Mask:	
Default Gateway:	
Apply Changes R	eset Show Route Table

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

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
255.255.255.255	0.0.0.0	255.255.255.255	UH	0	0	0	br0
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	br 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	wland
0.0.0.0	172.1.1.254	0.0.0.0	UG	0	0	0	wlanC

VPN Pass-through

Routing Table

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	
G Wizard G Operation Mode Withless	This page is used to set the account to access the web server of Access Paint. Empty user name and paceword will disable the protection.	
Firewall	User Name:	
B Status Pi GelS Bandwidth Control	New Password: Confirmed Password:	
語 Stave 語 Statistics 語 DONS 語 Time Zone	Apply Clauges Exer	
Bi Log Bi Maseilaneous Bi Upgrade Firmware Bi SawiRelsad Settings		
S Rebert		

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

📲 192.168.2.3 - PoTTY 📃 💷	83
System Settings************************************	10
A. Root Password G. Exit	
Please choice one selection:	
Flease key-in the Password quertyuiop Changing password for root Password changed	
Press any key to continue	+

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.

 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.

Wizard Deveation Mode Wireless Ensect	This page is used to configure the information was noting the SNAP	SIMP settings artwork protocol	You can get some of the system	
Matagement	3 System Community String: System Name:	prhic heak		
SIMP 2 Sidence	System Location: System Centact: Turn Receiver III Address:	IF hask	4	
Mi Time Zate Mi Lag Miscelaneoza Mi Uggide Firmeare	Address1 Community String: Trap Receiver IP Address2:	lost		
SaveRelated Setting Password B Rebeat	Address2 Community String: Trap Receiver IP Address2:	-		
	Address3 Community String: 5 Apply Charges From			

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/Rash 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	/bir/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	

1.3.6.1.4.1.99.7 - 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	0 AP-WEP
.1.3.6.1.4.1.99.8.101.1	WEP(AP), Disabled(WDS)

Miscellaneous Settings

Site contents:	Miscellaneous	Settings				
Coperation Mode	This page is used to configure	This page is used to configure the miscellaneous settings				
TCPAP	HTTP Port.	80	(1-65636)			
	RSSI Interval:	100	(30-86400 seconds)			
E Cell	🔲 Ping WatchDog Enable	d				
E Sandvetth Control	Target Host IP Address:	192.168.2.254				
E Shelistice	Ping Interval:	100	(15-B6400 seconds)			
CONS Tree Tree	Ping Threshold:	5	(1-100 times)			
8	Ping Rebosting Delay:	-60	(10-600 seconds)			
B Miscellaneous D Upprate Firmware Save/Feleral Setting	Apply Charges Front)				
G Rebert						

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.

🖹 Canı	not	find se	erver - Mi	crosof	t Inte	ernet Explo	rer	
File E	dit	View	Favorites	Tools	Hel	P		
🕞 Ba	ick -	• 6	- 🗙	2		🔎 Search	📌 Favorites	0
Address	htt	p://192.	168.2.254:6	5500				

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.

This page provides tool to scan the wireless network. If any Access Point or IBSS is bund, you could choose to connect it manually when client mode is enabled.								
SSID	BSSID	Chianti	Туре	Eacrypt	RSSI	Quality	Select	Aim
ZPhes-G120	00.05.9e.11.53.fb	11 (B+G)	AP	yes	86 (-31 dbm)	87	0	0
tuce.	00.05.9e/11.39.67	6 (B+G)	AP	BO	81 (-41 dhm)	92	0	0
hot	00:03:14:00:63:4e	10 (B+G)	AP	yes	56 (-56 dbm)	19	0	0
ZPD-1	00.05.9e.81-9a.ed	1 (B+G)	AP	RÔ	52 (-51 dbm)	12	0	0
ZINTECH-QA	00.00.00.04:78:74	1 (B+G)	AP	965	16 (-80 dbm)	73	0	0
ZPhs-2200-G	00.01±7:12:34:56	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	e Survey					
This page provides tool to found, you could choose	o scan the wireless net to connect it manually	work. If any A when client n	ccess Poin tode is ena	t or IBSS is bled.		
CII22	BSSID	Channel	Type	Hacrypt	RSSI	Quality
hot	00:02:14:00:62:4e	10 (B+G)	AP	yes	58 (-55 dim)	89
Refesh Stop Aining	58%					

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.

Connecting Profile

Site contents B Wizard Dersition Mode Dersition Mode Dersition B Base Sattings S Advanced Sattings S Security S Advanced Control	Connecting Pro Enable the connecting paties is and BSSD in a fixed period, it with them one by one and regi- that check the preferred APc v strength is good enough, other the prefiles share the same se	ofile Settings in client mode, the system will preferred APs are found, the r reflexes of the signal quality an will impact the throughput a lot wise don't set the interval too conty setting.	I check the performed SSID adia well try to connect d strength. Please note 1 Unless the signal short. And cuttertly ,all	
Konsection Control	Enable connecting prof SSID: Apply Clanges Report	lle BSSID:		
	Checking Interval:	10 61	443 minutes)	
	Current preferred AP list:		1999-1997) 	
	SSID	#SSID	Select	
	Text AP 1	00 00 00 00 00 00 00		
	Delere Selected Delere A	I (Rear)		

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.

Current preferred AP list:		
SSID	BSSID	Select
Test AP 1	00:00:00:00:00:00	
Device AP 1	00:00:00:00:00:00	
Delete Selected Delete All	Reset	

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.

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-2000webpages_adv.bin** and **zwa-2000linux_adv_led1.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
B Wizard B Coorstion Mode Wintess TCPAP	This page allows you save current settings to a life or reload the settings from the life which was saved previously. Besides, you could result the current configuration to factory default.
Freed Management Souther GeS Souther GeS Souther Souther	Save Settings to File: Dom. Load Settings from File: Opton Reset Settings to Default: Fourt

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.

WirelessConf 🛛 🔀
Login failed! Please try again.
OK

4	Wi	slass LAN Series Con	figrration Tool (¥1.00.11					
	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	D	-
	2	WLAN-TEST-1	192.168.2.50	255.255.255.0	AP-Bridge	6	00:00:00:44:00:02	D	-
	<								
	Pass	word:	Log	in New	Password:		Change Passwo	rd 1	
	D	iscover Setu	Det Det	ail 0/1	Active Cli	ents	Connect to Web S	erver C	iose
		000			Provide data		Contraction Process		
		2 3	(4) (5) 6				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.

]>	
New Passw	ord *****	Change Password	
WDS	Active Clients	Connect to Web Server	Close

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</u> on AP-Client 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 End	abled								
IP Address:	192		168		2		1	1	
Netmask:	255		255		255		0		
Default Gateway:	0		0		0		0		
User Name:	test								
Password:	****	_		_				1	
Apply Changes						<u>C</u> lo	ose		

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.

10	MAC Address	TxPackets	Tx Errors	Po: Packets	Tx Rate (Mops)
1	00:05:9e:80:aa.11	41	37	0	1 contractor and the
	00:05:9e:00:se:22	41	39	0	1
	00.e0:4c:81.86:21	20	3	633	11

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:



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