Dedicated Wifi Router (DWR) User's Guide

Version: 1.1

Date: October 17, 2008

3JTech Co., Ltd. 2F, No. 342, Fu-Shing N. Rd. Taipei, Taiwan Tel: +886-2-2500 6916 e-mail: <u>info@3jtech.com.tw</u>



Revision History

Version	Date	Changes
1.0	09/18/2008	First Release of DWR User's Guide
1.1	10/17/2008	Add the FCC Caution

Table of Contents

Revision History	2
TABLE OF CONTENTS	2
CHAPTER 1. PRODUCT OVERVIEW	4
1.1 INTRODUCTION	4
1.2 Features	5
1.3 Package Contents	5
CHAPTER 2. PHYSICAL DESCRIPTION	6
2.1 PANELS	6
2.1.1 Front and Rear Panels	6
2.1.2 Bottom Panel	7
2.2 Illustration	7
2.2.1 Front and Rear Panel Information	8
WAN Port	8
LAN1~LAN 4 Port Network Connectors	8
wifi ANT SMA Connector	8
Power Supply Connector	8
LEDs	8
2.2.2 Bottom Panel Information	8
Reset Button	8
2.2.3 LED Description on the Front Panel	8
CHAPTER 3. INSTALLATION	10
3.1 HARDWARE INSTALLATION	10
3.2 Software Installation	10
3.2.1 Software Configuration	10
3.2.2 Prepare your PC for DWR Configuration	11
3.2.3 Connect to DWR	13
3.2.4 Management and Configuration on DWR	13
3.2.4.1 Status	13
3.2.4.2 Setup Wizard	10
Time Zene Setting	10 17
I Mu Interface Setup	۱۱ 17 ــــــــــــــــــــــــــــــــــــ
WAN Interface Setup	۱ <i>۱</i> 1717
3 2 4 3 Operation Mode	۱ <i>۲</i> ۱۸ 18
3 2 4 4 Wireless - Basic Settings	۱۵ ۱۹ – – – – – – – – – – – – – – –
3.2.4.5 Wireless - Advanced Settings	2 <u>0</u>
3.2.4.6 Wireless - Access Control	22

Copyright of 3JTech Co., Ltd. (also doing business as A3J Engineering Inc.)



3.2.4.7 WDS Settings	23
3.2.4.8 Site Survey	24
3.2.4.9 LAN Interface Setup	25
3.2.4.10 WAN Interface Setup	27
Static IP	27
DHCP Client	29
PPPoE	30
PPTP	33
3.2.4.11 Firewall - Port Filtering	35
3.2.4.12 Firewall - IP Filtering	36
3.2.4.13 Firewall - MAC Filtering	37
3.2.4.14 Firewall - Port Forwarding	38
3.2.4.15 Firewall – URL Filtering –	39
3.2.4.16 Firewall - DMZ	40
3.2.4.17 Management - Statistics	41
3.2.4.18 Management - DDNS	42
3.2.4.19 Management - Time Zone Setting	43
3.2.4.20 Management - Denial-of-Service	44
3.2.4.21 Management - Log	45
3.2.4.22 Management - Upgrade Firmware	46
3.2.4.23 Management - Save/ Reload Settings	46
3.2.4.24 Management - Password Setup	47
3.2.4.25 Logout	48
APPENDIX A - FCC CAUTION	49



1. Product Overview

1.1 Introduction

DWR (Dedicated WIFI Router), a special WiFi broadband router, not only it can be used as a regular router but also make 3JTech WIFI cameras Plug-and-Play. With our proprietary wifiDHCP technology, the WIFI cameras will get the SSID and WEP key automatically from the DWR via Ethernet connection. The SSID and WEP key are randomly assigned upon the hardware reset of DWR.





1.2 Features

- As VPN client or pass-through.
- Offer 3JTech's Wifi camera to be Plug-and-Play wifi cameras.

1.3 Package Contents

- 1 x DWR Router
- 1 x CD with Quick Installation Guide and User's Manual
- 1 x RJ45 Ethernet Cable
- 1 x Power Adapter



2. Physical Description

The following information contains the physical description of DWR. This includes the functions and the locations of each connector and indicator. This information provides useful reference when installing the product. Please familiarize yourself with DWR.

2.1 Panels

2.1.1 Front and Rear Panels

For more related description, please refer to the Section 2.2 and Section 2.2.1.





2.1.2 Bottom Panel

For more detailed description, please refer to the Section 2.2 and Section 2.2.2.



2.2 Illustration

No. in Figures	Name on DWR	Description	Remark
1	WAN Port	For the access of Internet	Refer to section 2.2.1 for front and real panels information.
2	LAN1~LAN 4 Port Network Connectors	To connect to the device and Ethernet port via RJ45 cable	Refer to section 2.2.1 for front and real panels information.
3	wifi ANT SMA Connector	To connect with the wifi antenna	Refer to section 2.2.1 for front and real panels information.
4	Power Supply Connector	To connect with DWR and the power adapter	Refer to section 2.2.1 for front and real panels information.
5	LEDs	To display the status of DWR	Refer to section 2.2.3 for LED description on the front panel.
6	Reset Button	To reset DWR to its factory defaults	Refer to section 2.2.2 for bottom panel information.



2.2.1 Front and Rear Panel Information

WAN Port

Offer the access of Internet.

LAN1~LAN 4 Port Network Connectors

DWR is designed for 10/100Mbps Ethernet networks. DWR connects to the network via category 5 cable.

wifi ANT SMA Connector

Support WEP and WPA modes for wireless access.

Power Supply Connector

Plug the power adapter. The specifications of DWR's power adapter are as follows:

- Input: 100 ~ 240V AC, 50/60Hz
- Output: 12V DC / 1.5A

LEDs

Include the LEDs of POWER, WLAN (Wireless LAN), WAN Link and LAN Link.

2.2.2 Bottom Panel Information

Reset Button

Support the hardware reset function.

2.2.3 LED Description on the Front Panel





LED	Color	Status
POWER	Green	Lit when +12V DC power is on and working.
MI ANI/Mirologg ANI)	Groop	Lit when device is normal.
WLAN(WITCHESS LAN)	Gleen	Flash when any traffic is present.
		Lit when connection with remote device is good.
WAN Link	Green	Flash when any traffic is present.
		Off when cable connection is not good.
		Lit when connection with remote device is good.
LAN Link	Green	Flash when any traffic is present.
		Off when cable connection is not good.



3. Installation

3.1 Hardware Installation

- **Step 1:** Place DWR to the best optimum transmission location. The best transmission location for your DWR is usually at the geographic center of your wireless network, with line of sign to all of your mobile stations.
- Step 2: Connect DWR to your wired network. Connect the Ethernet WAN interface of DWR by category 5 Ethernet cable to your switch/ hub/ xDSL modem or cable modem. A straight-through Ethernet cable with appropriate cable length is needed.
- **Step 3:** Supply DC power to DWR. Use only the AC/DC power adapter supplied with DWR; it may occur damage by using a different type of power adapter.

3.2 Software Installation

There is no software drivers, patches or utilities installation needed, but only the configuration settings. Please refer to this chapter which will instruct you how to configure and manage DWR through the web user interface it supports. With this facility, you can easily access and monitor through any one LAN port of DWR.

It will take about 55 seconds to complete the boot up sequence after powering on DWR.

3.2.1 Software Configuration

In DWR, it supports a simple user management function to configure the system. The DWR is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: **192.168.8.1** Default IP subnet mask: **255.255.255.0** WEB login User Name: **cameras** WEB login Password: **cameras**



3.2.2 Prepare your PC for DWR Configuration

■ For OS of Microsoft Windows 95/ 98/ Me:

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.

Windows Me users may not see the Network control panel. If so, *select* View all Control **Panel options** on the left side of the window.

- 2. Move mouse and double-click the right button on Network icon. The Network window will appear.
- 3. Check the installed list of Network Components. If TCP/IP is not installed, click the **Add** button to install it; otherwise go to step 6.
- 4. Select Protocol in the Network Component Type dialog box and click **Add** button.
- 5. Select TCP/IP in Microsoft of Select Network Protocol dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to Network dialog box after the TCP/IP installation.
- 6. Select TCP/IP and click the **Properties** button on the Network dialog box.
- 7. Select Specify an IP address and type in values as following example.
 - ✓ IP Address: **192.168.8.1**, any IP address within 192.168.8.1 to 192.168.8.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: 255.255.255.0
- 8. Click **OK** and reboot your PC after completing the IP parameter settings.



■ For OS of Microsoft Windows 2000, XP:

- 1. Click the Start button and select Settings, then click Control Panel. The Control Panel window will appear.
- Move mouse and double-click the right button on Network and Dial-up Connections icon. Move mouse and double-click the Local Area Connection icon. The Local Area Connection window will appear. Click **Properties** button in the Local Area Connection window.
- 3. Check the installed list of Network Components. If TCP/IP is not installed, click the **Add** button to install it; otherwise go to step 6.
- 4. Select Protocol in the Network Component Type dialog box and click **Add** button.
- 5. Select TCP/IP in Microsoft of Select Network Protocol dialog box then click **OK** button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to Network dialog box after the TCP/IP installation.
- 6. Select TCP/IP and click the **Properties** button on the Network dialog box.
- 7. Select Specify an IP address and type in values as following example.
 - ✓ IP Address: 192.168.8.1, any IP address within 192.168.8.1 to 192.168.8.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: 255.255.255.0
- 8. Click **OK** to complete the IP parameter settings.

■ For OS of Microsoft Windows NT:

- 1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
- 2. Move mouse and double-click the right button on Network icon. The Network window will appear. Click Protocol tab from the Network window.
- 3. Check the installed list of Network Protocol window. If TCP/IP is not installed, click the **Add** button to install it; otherwise go to step 6.
- 4. Select Protocol in the Network Component Type dialog box and click Add button.
- 5. Select TCP/IP in Microsoft of Select Network Protocol dialog box then click **OK** button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to Network dialog box after the TCP/IP installation.
- 6. Select TCP/IP and click the **Properties** button on the Network dialog box.
- 7. Select Specify an IP address and type in values as following example.
 - ✓ IP Address: **192.168.8.1**, any IP address within 192.168.8.1 to 192.168.8.253 is good to connect the Wireless LAN Access Point.
 - IP Subnet Mask: 255.255.255.0
- 8. Click **OK** to complete the IP parameter settings.



3.2.3 Connect to DWR

After DWR has been connected to your PC via the network cable, please initiate a web browser, i.e. Microsoft Internet Explore and enter <u>http://192.168.8.1</u> on the URL to login DWR. Then, input the default user name as well as the password, and click the **OK** button. The setup page for DWR will be displayed once the login process is successful.

As the figure below shows, for example, left section is the whole list of sub functions while each of main functions, including Setup Wizard, Operation Mode, Wireless, TCP/IP Settings, Firewall, Management and Logout is selected.

V	VLAN Acc	ess Point
Site contents:	Operation M	Node
Operation Mode 	You can setup different	modes to LAN and WLAN interface for NAT and bridging function.
Basic Settings Advanced Setting Advanced Setting Stopping WDS settings Site Survey TOP/IP Settings	© Gateway:	In this mode, the device is supposed to connect to internet via ADSL/Cable Modern. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
LAN Interface	O Bridge:	In this mode, all ethemet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
	○ Wireless ISP:	In this mode, all ethemet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethemet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
	Apply Change	Reset
Log Dygrade Firmware Save/Reload Sett Password		

Fig. 3-1

3.2.4 Management and Configuration on DWR

3.2.4.1 Status

This page shows the current status and some basic settings of the device, includes system, wireless, Ethernet LAN and WAN configuration information.



Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	Oday:1h:5m:17s
Firmware Version	V1.5
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
CI 22	mWVVqH3JOhoFRtP8
Channel Number	11
Encryption	WEP 64 bits
DI228	00:e0:4c:00:00:10
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.8.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.8.1
DHCP Server	Enabled
MAC Address	00:e0:4c:00:00:10
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	61.56.193.38
Subnet Mask	255.255.255.128
Default Gateway	61.56.193.120

Fig. 3-2

ltem	Description
System	·
Uptime	It shows the duration since DWR is powered on.
Firmware version	It shows the firmware version of DWR.
Wireless Configuration	bn
Mode	It shows wireless operation mode.
Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of this DWR.
	The SSID is the unique name of DWR and shared
	among its service area, so all devices attempts to join
	the same wireless network can identify it.
Channel Number	It shows the wireless channel connected currently.



Encryption	It shows the status of encryption function.
BSSID	It shows the BSSID address of DWR. BSSID is a
	six-byte address.
Associated Clients	It shows the number of connected clients (or stations,
	PCs).
TCP/IP Configuration	1
Attain IP Protocol	It shows type of connection.
IP Address	It shows the IP address of LAN interfaces of DWR.
Subnet Mask	It shows the IP subnet mask of LAN interfaces of DWR.
Default Gateway	It shows the default gateway setting for LAN interfaces
	outgoing data packets.
DHCP Server	It shows the DHCP server is enabled or not.
MAC Address	It shows the MAC address of LAN interfaces of DWR.
WAN Configuration	
Attain IP Protocol	It shows how DWR gets the IP address. The IP address
	can be set manually to a fixed one or set dynamically by
	DHCP server or attain IP by PPPoE / PPTP connection.
IP Address	It shows the IP address of WAN interface of DWR.
Subnet Mask	It shows the IP subnet mask of WAN interface of DWR.
Default Gateway	It shows the default gateway setting for WAN interface
	outgoing data packets.
MAC Address	It shows the MAC address of WAN interface of DWR.



3.2.4.2 Setup Wizard

This page guides you to configure DWR for the first time. Please press **Next** to continue.



Fig. 3-3

Operation Mode

This page followed by Setup Wizard page to define the operation mode.

1. Oper	ration Mode
You can setup	different modes to LAN and WLAN interface for NAT and bridging function.
⊙ Gatewa	y: In this mode, the device is supposed to connect to internet via ADSL/Cable Modern. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
O Bridge:	In this mode, all ethemet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
⊂ Wireles	In this mode, all ethemet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethemet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
	Cancel < <back next="">></back>

Fig. 3-4



Time Zone Setting

Enable NTP cli	ent update		
Time Zone Select :	(GMT+08:00)Taipei	 	V
NTP server :	192.5.41.41 - North America 👻		

This page is used to enable and configure NTP client.

Fig. 3-5

LAN Interface Setup

This page is used to configure local area network IP address and subnet mask.

3. LAN Inte	rface Setup	
This page is used to con your Access Point. Here	gure the parameters for local area network which connects to the LAN port of you may change the setting for IP addresss, subnet mask, DHCP, etc	
IP Address:	192.168.8.1	
Subnet Mask:	255.255.255.0	
	Cancel < <back nexts<="" td=""><td>>></td></back>	>>

Fig. 3-6

WAN Interface Setup

This page is used to configure WAN access type.

4. WAN Inte	rface Setup	
This page is used to config your Access Point. Here yo click the item value of WAI	ure the parameters for Interne 11 may change the access me 11 Access type.	t network which connects to the WAN port of hod to static IP, DHCP, PPPoE or PPTP by
WAN Access Type:	DHCP Client Static IP DHCP Client PPPoE PPTP	
		Cancel < <back finished<="" th=""></back>

Fig. 3-7

Copyright of 3JTech Co., Ltd. (also doing business as A3J Engineering Inc.)



3.2.4.3 Operation Mode

This page is used to configure which mode that DWR will act.

WLAN Access Point				
Site contents: Setup Wizard Wireless TCP/IP Settings Firewall Management Logout	Operation N You can setup different	Operation Mode You can setup different modes to LAN and WLAN interface for NAT and bridging function.		
	© Gateway:	In this mode, the device is supposed to connect to internet via ADSL/Cable Modern. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.		
	O Bridge:	In this mode, all ethemet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.		
	C Wireless ISP:	In this mode, all ethemet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethemet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.		
	Apply Change	Reset		

Fig. 3-8

ltem	Description
Gateway	Traditional gateway configuration. It always
	connects Internet via ADSL/Cable Modem. LAN
	interface, WAN interface, Wireless interface, NAT
	and Firewall modules are applied to this mode.
Bridge	Each interface (LAN, WAN and Wireless) regards as
	bridge. NAT, Firewall and all router's functions are
	not supported.
Wireless ISP	Switch Wireless interface to WAN port and all
	Ethernet ports in bridge mode. Wireless interface
	can do all router's functions.
Apply Changes	Click the Apply Changes button to complete the
	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.



3.2.4.4 Wireless - Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your DWR. Here you may change wireless encryption settings as well as wireless network parameters.

	WLAN Acces	ss Point
 Site contents: Setup Wizard Operation Mode Wireless Basic Settmos 	Wireless Bas	ic Settings
	This page is used to config Access Point. Here you ma —	ure the parameters for wireless LAN clients which may connect to your y change wireless encryption settings as well as wireless network parameters.
Advanced Settings	Disable Wireless	LAN Interface
WDS settings Site Survey TCP/IP Settings Firewall Management Logout	Band:	2.4 GHz (B+G) 💌
	Mode:	AP
	Network Type:	Infrastructure 👻
	SSID:	1RvPBW8XxrqlIf8F
	WEP Key:	7578d73fb7
	Channel Number:	11
	Associated Clients:	Show Active Clients
	Enable Mac Close	ne (Single Ethernet Client)
	Apply Changes I	Reset

Fig. 3-9

Item	Description
Disable Wireless LAN	Click on to disable the wireless LAN data
Interface	transmission.
Band	Click to select 2.4GHz(B) / 2.4GHz(G) /
	2.4GHz(B+G).
Mode	Click to select the WLAN AP / Client / WDS /
	AP+WDS wireless mode.
Network Type	Support Inferstructure mode in wireless network
	connection. In this mode, the device can connect to
	DWR.
SSID	It is the wireless network name. The SSID can be 32
	bytes long.
WEP Key	64Bit encryption algorithm.
Channel Number	Select the wireless communication channel from the
	pull-down menu.



Associated Clients	Click the Show Active Clients button to open Active		
	Wireless Client Table that shows the MAC address,		
	transmit-packet, receive-packet and		
	transmission-rate for each associated wireless		
	client.		
Enable Mac Clone	Take Laptop NIC MAC address as wireless client		
(Single Ethernet	MAC address. [Client Mode only]		
Client)			
Apply Changes	Click the Apply Changes button to complete the		
	new configuration setting.		
Reset	Click the <i>Reset</i> button to abort change and recover		
	the previous configuration setting.		

3.2.4.5 Wireless - Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your DWR.

WLAN Access Point				
 Site contents: Setup Wizard Operation Mode Wireless Basic Settings Advanced Settings 	Wireless Adva These settings are only for m wireless LAN. These settings on your Access Point.	anced Settings ore technically advanced users who have a sufficient knowledge about should not be changed unless you know what effect the changes will have		
Access Control WDS settings	Authentication Type:	C Open System C Shared Key 💿 Auto		
Site Survey	Fragment Threshold:	2346 (256-2346)		
Firewall	RTS Threshold:	2347 (0-2347)		
Management	Beacon Interval:	100 (20-1024 ms)		
	Data Rate:	Auto		
	Preamble Type:	⊙ Long Preamble ○ Short Preamble		
	Broadcast SSID:	⊙ Enabled C Disabled		
	IAPP:	⊙ Enabled C Disabled		
	802.11g Protection:	⊙ Enabled C Disabled		
	WMM:	C Enabled ⓒ Disabled		
	RF Output Power:	⊡ 100% C 50% C 25% C 10% C 5%		
	Turbo Mode:	⊙ Auto ⊂ Always ⊂ Off		
		Note: "Always" may have compatibility issue. "Auto" will only work with DWR Series product.		
	Apply Changes H	Reset		

Fig. 3-10



ltem	Description		
Authentication Type	Click to select the authentication type in Open		
	System, Shared Key or Auto selection.		
Fragment Threshold	Set the data packet fragmentation threshold, value		
	can be written between 256 and 2346 bytes.		
RTS Threshold	Set the RTS Threshold, value can be written		
	between 0 and 2347 bytes.		
Beacon Interval	Set the Beacon Interval, value can be written		
	between 20 and 1024 ms.		
Data Rate	Select the transmission data rate from the pull-down		
	menu. Data rate can be auto-select, 11M, 5.5M, 2M		
	or 1Mbps.		
Preamble Type	Click to select the <i>Long Preamble</i> or <i>Short</i>		
	Preamble support on the wireless data packet		
	transmission.		
Broadcast SSID	Click to enable or disable the SSID broadcast		
	function.		
IAPP	Click to enable or disable the IAPP function.		
802.11g Protection	Protect 802.11b user.		
WMM	Click Enabled/Disabled to init WMM feature.		
RF Output Power	To adjust transmission power level.		
Turbo Mode	Click to Enable/Disable turbo mode. (Only apply to		
	the application of DWR to DWR).		
Apply Changes	Click the Apply Changes button to complete the		
	new configuration setting.		
Reset	Click the <i>Reset</i> button to abort change and recover		
	the previous configuration setting.		



3.2.4.6 Wireless - Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.

	WLAN Access Poi	nt	
Site contents: Setup Wizard Operation Mode Wireless Advanced Settings Advanced Settings WDS settings Site Survey TCP/IP Settings Firewall Management Logout	Wireless Access Co If you choose 'Allowed Listed', only those control list will be able to connect to your clients on the list will not be able to connec Wireless Access Control Mode: MAC Address: Apply Changes Reset Current Access Control List:	entrol e clients whose wireless MAC a Access Point. When Deny Liste ct the Access Point. Allow Listed Comment:	ldresses are in the access al'is selected, these wireless
	MAC Address	Comment	Select
	00:02:72:81:86:01	ST-1	
	00:00:55:66:66:50	ST-2	
	Delete Selected Delete All	Reset	

Fig. 3-11

Item	Description
Wireless Access	Click the Disable , Allow Listed or Deny Listed of
Control Mode	drop down menu choose wireless access control
	mode.
	This is a security control function; only those clients
	registered in the access control list can link to this
	DWR.
MAC Address	Fill in the MAC address of client to register this DWR
	access capability.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the Apply Changes button to register the
	client to new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.



Current Access	It shows the registered clients that are allowed to
Control List	link to this DWR.
Delete Selected	Click to delete the selected clients that will be
	access right removed from this DWR.
Delete All	Click to delete all the registered clients from the
	access allowed list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

3.2.4.7 WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other AP that you want to communicate with in the table and then enable the WDS.

VNOTE: WDS / AP + WDS mode must be selected in Wireless Basic Settings if you would like to enable the function of WDS settings.

	WLAN Access Poi	nt		
 Site contents: Setup Wizard Operation Mode Wireless Basic Settings Advanced Settings Access Control WDS settimes Site Survey TCP/IP Settings Firewall Management Logout 	WDS Settings Wireless Distribution System uses wirele dces. To do this, you must set these APs you want to communicate with in the table ✓ Enable WDS Add WDS AP: MAC Address Apply Changes Reset Current WDS AP List:	ss media to communicate with o in the same channel and set MA e and then enable the WDS. Comm Set Security Show Stat	other APs, like the Eth C address of other Al nent	nemet Ps which
	MAC Address	Comment	Select	
	00:02:72:81:86:0a	AP-1		
	00:02:72:81:86:0b	ΔP-7		
	Delete Selected Delete All	Reset		

Fig. 3-12



ltem	Description	
Enable WDS	Click the checkbox to enable wireless distribution	
	system function.	
MAC Address	Fill in the MAC address of AP to register the wireles	
	distribution system access capability.	
Comment	Fill in the comment tag for the registered AP.	
Apply Changes	Click the Apply Changes button to register the AP	
	to new configuration setting.	
Reset	Click the Reset button to abort change and recover	
	the previous configuration setting.	
Set Security	Click button to configure wireless security like	
	WEP(64bits), WEP(128bits), WPA(TKIP),	
	WPA2(AES) or None	
Show Statistics	It shows the TX, RX packets, rate statistics	
Delete Selected	Click to delete the selected clients that will be	
	removed from the wireless distribution system.	
Delete All	Click to delete all the registered APs from the	
	wireless distribution system allowed list.	
Reset	Click the Reset button to abort change and recover	
	the previous configuration setting.	

3.2.4.8 Site Survey

This page is used to view or configure other APs near yours.

	WLAN Access I	Point				
 Site contents: Setup Wizard Operation Mode Wireless Basic Settings 	Wireless Site Su This page provides tool to scan the choose to connect it manually whe	WVCY wireless network. If a n client mode is enable	ny Access Pc d.	int or IBS	S is found, y	ou could
Advanced Settings	GISS	BSSID	Channel	Туре	Encrypt	Signal
Site Sulley	IN1MBLkHxzeq4ghq	00:09:b5:81:87:04	11 (B+G)	AP	WEP	100
TCP/IP Setungs	Adrian	00:09:b5:ab:od:ee	11 (B+G)	AP	WEP	55
Firewall Management Logout	Refiesh Connect					

Fig. 3-13



Item	Description
SSID	It shows the SSID of AP.
BSSID	It shows BSSID of AP.
Channel	It show the current channel of AP occupied.
Туре	It show which type AP acts.
Encrypt	It shows the encryption status.
Signal	It shows the power level of current AP.
Refresh	Click the <i>Refresh</i> button to re-scan site survey on
	the screen.
Connect	Click the Connect button to establish connection.

3.2.4.9 LAN Interface Setup

This page is used to configure the parameters for local area network that connects to the LAN ports of your DWR. Here you may change the setting for IP address, subnet mask, DHCP, etc.

	WLAN Access	Point
Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings	LAN Interface This page is used to configure your Access Point. Here you r	: Setup the parameters for local area network which connects to the LAN port of nay change the setting for IP addresss, subnet mask, DHCP, etc
WAN Interface	IP Address:	192.168.8.1
Management	Subnet Mask:	255.255.255.0
Logout	Default Gateway:	0.0.0.0
	DHCP:	Server 💌
	DHCP Client Range:	192.168.8.100 - 192.168.8.200 Show Client
	Domain Name:	
	802.1d Spanning Tree:	Disabled 💌
	Clone MAC Address:	0000000000
	Apply Changes Res	et

Fig. 3-14

Item	Description	
IP Address	Fill in the IP address of LAN interfaces of this WLA	
	Access Point.	
Subnet Mask	Fill in the subnet mask of LAN interfaces of this	
	WLAN Access Point.	



Default Gateway	Fill in the default gateway for LAN interfaces out
	going data packets.
DHCP	Click to select <i>Disabled</i> , <i>Client</i> or <i>Server</i> in
	different operation mode of wireless Access Point.
DHCP Client Range	Fill in the start IP address and end IP address to
	allocate a range of IP addresses; client with DHCP
	function set will be assigned an IP address from the
	range.
Show Client	Click to open the Active DHCP Client Table window
	that shows the active clients with their assigned IP
	address, MAC address and time expired
	information. [Server mode only]
Domain Name	Assign Domain Name and dispatch to DHCP clients.
	It is optional field.
_	
802.1d Spanning	Select to enable or disable the IEEE 802.1d
802.1d Spanning Tree	Select to enable or disable the IEEE 802.1d Spanning Tree function from the pull-down menu.
802.1d Spanning Tree Clone MAC Address	Select to enable or disable the IEEE 802.1d Spanning Tree function from the pull-down menu. Fill in the MAC address that is the MAC address to
802.1d Spanning Tree Clone MAC Address	Select to enable or disable the IEEE 802.1d Spanning Tree function from the pull-down menu. Fill in the MAC address that is the MAC address to be cloned.
802.1d Spanning Tree Clone MAC Address Apply Changes	Select to enable or disable the IEEE 802.1d Spanning Tree function from the pull-down menu. Fill in the MAC address that is the MAC address to be cloned. Click the <i>Apply Changes</i> button to complete the
802.1d Spanning Tree Clone MAC Address Apply Changes	Select to enable or disable the IEEE 802.1d Spanning Tree function from the pull-down menu. Fill in the MAC address that is the MAC address to be cloned. Click the <i>Apply Changes</i> button to complete the new configuration setting.
802.1d Spanning Tree Clone MAC Address Apply Changes Reset	Select to enable or disable the IEEE 802.1d Spanning Tree function from the pull-down menu. Fill in the MAC address that is the MAC address to be cloned. Click the <i>Apply Changes</i> button to complete the new configuration setting. Click the <i>Reset</i> button to abort change and recover



3.2.4.10 WAN Interface Setup

This page is used to configure the parameters for wide area network that connects to the WAN port of your DWR. Here you may change the access method to *Static IP*, *DHCP*, *PPPoE* or *PPTP* by clicking the item value of **WAN Access Type**.

Static IP

	WLAN Acces	s Point
Site contents:	WAN Interfac	ce Setup
Operation Mode Wireless TCP/IP Settings I AN Interface	This page is used to configu Point. Here you may change WAN Access type.	te the parameters for Internet network which connects to the WAN port of your Access the access method to static IP, DHCP, PPPoE or PPTP by click the item value of
WAN Interface	WAN Access Type:	Static IP
Management	IP Address:	172.1.1.1
	Subnet Mask:	255.255.255.0
	Default Gateway:	172.1.1.254
	MTU Size:	1500 (1400-1500 bytes)
	DNS 1:	
	DNS 2:	
	DNS 3:	
	Clone MAC Address:	0000000000
	Enable uPNP	
	Enable Ping Access	s on WAN
	🗖 Enable Web Serve	r Access on WAN
	Enable IPsec pass	through on VPN connection
	Enable PPTP pass	through on VPN connection
	Enable L2TP pass	through on VPN connection

Fig. 3-15

Item	Description	
Static IP	Click to select Static IP support on WAN interface.	
	There are IP address, subnet mask and default	
	gateway settings need to be done.	
IP Address	If you select the Static IP support on WAN interface,	
	fill in the IP address for it.	
Subnet Mask	If you select the Static IP support on WAN interface,	
	fill in the subnet mask for it.	
Default Gateway	If you select the Static IP support on WAN interface,	
	fill in the default gateway for WAN interface out	
	going data packets.	



MTU Size	Fill in the mtu size of MTU Size. The default value is
	1400.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to
	be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable Ping Access	Click the checkbox to enable Ping Access on WAN
on WAN	function.
Enable Web Server	Click the checkbox to enable web configuration from
Access on WAN	WAN side.
Enable IPsec pass	Click the checkbox to enable IPSec packet pass
through on VPN	through.
connection	
Enable PPTP pass	Click the checkbox to enable PPTP packet pass
through on VPN	through.
connection	
Enable L2TP pass	Click the checkbox to enable L2TP packet pass
through on VPN	through.
connection	
Apply Changes	Click the Apply Changes button to complete the
	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.



DHCP Client

	WLAN Access Point		
 Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings LAN Interface 	WAN Interface Setup		
	This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.		
WAN Interface	WAN Access Type: DHCP Client		
Logout	Host Name:		
	MTU Size: [1492 (1400-1492 bytes)		
	C Attain DNS Automatically		
	[⊙] Set DNS Manually		
	DNS 1:		
	DNS 2:		
	DNS 3:		
	Clone MAC Address: 00000000000		
	Enable uPNP		
	Enable Ping Access on WAN		
	Enable Web Server Access on WAN		
	Enable IPsec pass through on VPN connection		
	Enable PPTP pass through on VPN connection		
	Enable L2TP pass through on VPN connection		

Fig. 3-16

Item	Description	
DHCP Client	Click to select DHCP support on WAN interface for	
	IP address assigned automatically from a DHCP	
	server.	
Host Name	Fill in the host name of Host Name. The default	
	value is empty.	
MTU Size	Fill in the mtu size of MTU Size. The default value is	
	1400.	
Attain DNS	Click to select getting DNS address for DHCP	
Automatically	support. Please select Set DNS Manually if the	
	DHCP support is selected.	
Set DNS Manually	Click to select getting DNS address for DHCP	
	support.	
DNS 1	Fill in the IP address of Domain Name Server 1.	
DNS 2	Fill in the IP address of Domain Name Server 2.	
DNS 3	Fill in the IP address of Domain Name Server 3.	



Clone MAC Address	Fill in the MAC address that is the MAC address to
	be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable Ping Access	Click the checkbox to enable Ping Access on WAN
on WAN	function.
Enable Web Server	Click the checkbox to enable web configuration from
Access on WAN	WAN side.
Enable IPsec pass	Click the checkbox to enable IPSec packet pass
through on VPN	through.
connection	
Enable PPTP pass	Click the checkbox to enable PPTP packet pass
through on VPN	through.
connection	
Enable L2TP pass	Click the checkbox to enable L2TP packet pass
through on VPN	through.
connection	
Apply Changes	Click the <i>Apply Changes</i> button to complete the
	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

PPPoE

	WLAN Acces	s Point		
Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings	WAN Interfac	WAN Interface Setup		
	This page is used to configur Point. Here you may change WAN Access type.	e the parameters for Internet network which connects to the WAN port of your Access the access method to static IP, DHCP, PPPoE or PPTP by click the item value of		
WAN Interface	WAN Access Type:	PPPoE		
Logout	User Name:			
	Password:			
	Service Name:			
	Connection Type:	Continuous Connect Disconnect		
	Idle Time:	5 (1-1000 minutes)		
	MTU Size:	1452 (1360-1492 bytes)		
	• Attain DNS Automa	ntically		
	C Set DNS Manually			
	DNS 1:			
	DNS 2:			
	DNS 3:			
	Clone MAC Address:	0000000000		
	Enable uPNP			
	Enable Ping Acces	s on WAN		



Copyright of 3JTech Co., Ltd. (also doing business as A3J Engineering Inc.) 30



Item	Description
PPPoE	Click to select PPPoE support on WAN interface.
	There are user name, password, connection type
	and idle time settings need to be done.
User Name	If you select the PPPoE support on WAN interface,
	fill in the user name and password to login the
	PPPoE server.
Password	If you select the PPPoE support on WAN interface,
	fill in the user name and password to login the
	PPPoE server.
Service Name	Fill in the service name of Service Name. The
	default value is empty.
Connection Type	Select the connection type from pull-down menu.
	There are <i>Continuous</i> , <i>Connect on Demand</i> and
	<i>Manual</i> three types to select.
	■ Continuous connection type means to setup the
	connection through PPPoE protocol whenever this
	DWR is powered on.
	■ Connect on Demand connection type means to
	setup the connection through PPPoE protocol
	whenever you send the data packets out through the
	WAN interface; there are a watchdog implemented
	to close the PPPoE connection while there are no
	data sent out longer than the idle time set.
	Manual connection type means to setup the
	connection through the PPPoE protocol by clicking
	the <i>Connect</i> button manually, and clicking the
	Disconnect button manually.
Idle Time	If you select the PPPoE and Connect on Demand
	connection type, fill in the idle time for
	auto-disconnect function. Value can be between 1
	and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is
	1400.
Attain DNS	Click to select getting DNS address for PPPoE
Automatically	support. Please select Set DNS Manually if the
	PPPoE support is selected.



Set DNS Manually	Click to select getting DNS address for <i>Static IP</i>
	support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to
	be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable Ping Access	Click the checkbox to enable Ping Access on WAN
on WAN	function.
Enable Web Server	Click the checkbox to enable web configuration from
Access on WAN	WAN side.
Enable IPsec pass	Click the checkbox to enable IPSec packet pass
through on VPN	through.
connection	
Enable PPTP pass	Click the checkbox to enable PPTP packet pass
through on VPN	through.
connection	
Enable L2TP pass	Click the checkbox to enable L2TP packet pass
through on VPN	through.
connection	
Apply Changes	Click the <i>Apply Changes</i> button to complete the
	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.



PPTP

	WLAN Acces	es Point		
Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings	WAN Interface Setup			
	This page is used to configu Point. Here you may change WAN Access type.	re the parameters for Internet network which connects to the WAN port of your Access the access method to static IP, DHCP, PPPoE or PPTP by click the item value of		
WAN Interface	WAN Access Type:	PPTP 💌		
Logout	IP Address:	172.1.1.2		
	Subnet Mask:	255.255.255.0		
	Server IP Address:	172.1.1.1		
	User Name:			
	Password:			
	MTU Size:	1460 (1400-1460 bytes)		
	🗆 Request MPPE En	cryption		
	© Attain DNS Autom	atically		
	C Set DNS Manually			
	DNS 1:			
	DNS 2:			
	DNS 3:			
	Clone MAC Address:	0000000000		

Fig. 3-18

Item	Description	
РРТР	Allow user to make a tunnel with remote site directly	
	to secure the data transmission among the	
	connection. User can use embedded PPTP client	
	supported by this router to make a VPN connection.	
IP Address	If you select the PPTP support on WAN interface, fill	
	in the IP address for it.	
Subnet Mask	If you select the PPTP support on WAN interface, fill	
	in the subnet mask for it.	
Server IP Address	Enter the IP address of the PPTP Server.	
User Name	If you select the PPTP support on WAN interface, fill	
	in the user name and password to login the PPTP	
	server.	
Password	If you select the PPTP support on WAN interface, fill	
	in the user name and password to login the PPTP	
	server.	
MTU Size	Fill in the mtu size of MTU Size. The default value is	
	1400.	



Request MPPE	Click the checkbox to enable request MPPE
Encryption	encryption.
Attain DNS	Click to select getting DNS address for PPTP
Automatically	support. Please select Set DNS Manually if the
	PPTP support is selected.
Set DNS Manually	Click to select getting DNS address for PPTP
	support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to
	be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable Ping Access	Click the checkbox to enable Ping Access on WAN
on WAN	function.
Enable Web Server	Click the checkbox to enable web configuration from
Access on WAN	WAN side.
Enable IPsec pass	Click the checkbox to enable IPSec packet pass
through on VPN	through.
connection	
Enable PPTP pass	Click the checkbox to enable PPTP packet pass
through on VPN	through.
connection	
Enable L2TP pass	Click the checkbox to enable L2TP packet pass
through on VPN	through.
connection	
Apply Changes	Click the <i>Apply Changes</i> button to complete the
	new configuration setting.
Reset	Click the Reset button to abort change and recover
	the previous configuration setting.



3.2.4.11 Firewall - Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

	WLAN Access	Point		
 Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings 	Port Filtering Entries in this table are used to through the Gateway. Use of s	restrict certain types of dat uch filters can be helpful ir	a packets from your local netv securing or restricting your k	vork to Internet scal network.
LAN Interface WAN Interface Firewall IP Filt Ming IP Filtering MAC Filtering MAC Filtering	Enable Port Filtering Port Range: Apply Changes Res	Protocol: Both	Comment:	
URL Filtering DMZ Management Logout	Current Filter Table: Port Range 20-21	Protocol TCP+UDP	Comment FIP	Select
	Delete Selected Del	ete All Reset		

Fig. 3-19

Item	Description
Enable Port Filtering	Click to enable the port filtering security function.
Port Range	To restrict data transmission from the local network
	on certain ports, fill in the range of start-port and
	end-port, and the protocol, also put your comments
	on it.
Protocol	The <i>Protocol</i> can be TCP, UDP or Both.
Comment	Comment let you know about the reason to restrict
	data from the ports.
Apply Changes	Click the Apply Changes button to register the ports
	to port filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be
	removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the
	port-filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.



3.2.4.12 Firewall - IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

	WLAN Access	Point		
	IP Filtering			
Operation Mode Wireless TCP/IP Settings	Entries in this table are used to through the Gateway. Use of s	restrict certain types of dat uch filters can be helpful is	ta packets from your local n securing or restricting yo	network to Internet ur local network.
	Enable IP Filtering			
MAC Filtering	Loal IP Address:	Protocol: Bot	h 💌 Comment:	
Port Forwarding URL Filtering DMZ	Apply Changes Res	et		
Management	Current Filter Table:			
	Local IP Address	Protocol	Comment	Select
	192.168.8.201	TCP+UDP	ST-1	
	192.168.8.202	TCP	ST-2	
	Delete Selected Del	ete All Reset		

Fig. 3-20

Item	Description
Enable IP Filtering	Click to enable the IP filtering security function.
Local IP Address	To restrict data transmission from local network on
	certain IP addresses, fill in the IP address and the
	protocol, also put your comments on it.
Protocol	The <i>Protocol</i> can be TCP, UDP or Both.
Comment	Comment let you know about the reason to restrict
	data from the IP address.
Apply Changes	Click the Apply Changes button to register the IP
	address to IP filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.
Delete Selected	Click to delete the selected IP address that will be
	removed from the IP-filtering list.
Delete All	Click to delete all the registered entries from the
	IP-filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.



3.2.4.13 Firewall - MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

	WLAN Access Point		
Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings Frewall Port Filtering Port Filtering Port Forwarding URL Filtering DMZ Management	MAC Filtering Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network. Image:		
	MAC Address	Comment	Select
	00:02:72:00:81:90	ST-1	
	00:02:72:00:81:91	ST-2	
	Delete Selected Delete All Reset		

Fig. 3-21

Item	Description
Enable MAC Filtering	Click to enable the MAC filtering security function.
MAC Address	To restrict data transmission from local network on
	certain MAC addresses, fill in the MAC address and
	your comments on it.
Comment	Comment let you know about the reason to restrict
	data from the MAC address.
Apply Changes	Click the Apply Changes button to register the MAC
	address to MAC filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.
Delete Selected	Click to delete the selected MAC address that will be
	removed from the MAC-filtering list.
Delete All	Click to delete all the registered entries from the
	MAC-filtering list.
Reset	Click the Reset button to abort change and recover
	the previous configuration setting.



3.2.4.14 Firewall - Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

	WLAN Access I	Point		
Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings Firewall Port Filtering MAC Filtering URL Filtering URL Filtering MAR anagement	Port Forwarding Entries in this table allow you to an NAT firewall. These settings are of server on the private local network Image: Comparison of the private local network Image	tomatically redirect common ne nly necessary if you wish to hos behind your Gateway's NAT fi Protocol: Both Port Rar	twork services to a sp t some sort of server l rewall.	ecific machine behind the ike a web server or mail Comment:
— 3	Current Port Forwarding Tab	le:		
	Local IP Address Pro	otocol Port Range	Comment	Select
	192.168.8.201 TCF	+UDP 20-21	FTP	
	Delete Selected Delete .	All Reset		

Fig. 3-22

Item	Description
Enable Port	Click to enable the Port Forwarding security
Forwarding	function.
IP Address	To forward data packets coming from WAN to a
	specific IP address that hosted in local network
	behind the NAT firewall, fill in the IP address,
	protocol, port range and your comments.
Protocol	The <i>Protocol</i> can be TCP, UDP or Both.
Port Range	The Port Range for data transmission.
Comment	Comment let you know about the reason to allow
	data packets forward to the IP address and port
	number.
Apply Changes	Click the Apply Changes button to register the IP
	address and port number to Port forwarding list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.



Delete Selected	Click to delete the selected IP address and port	
	number that will be removed from the	
	port-forwarding list.	
Delete All	Click to delete all the registered entries from the	
	port-forwarding list.	
Reset	Click the Reset button to abort change and recover	
	the previous configuration setting.	

3.2.4.15 Firewall – URL Filtering

URL Filtering is used to restrict users to access specific websites in internet.

	WLAN Access Point	
 Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings 	URL Filtering	
	URL filter is used to deny LAN users from accessing the internet. Block keywords listed below.	those URLs which contain
Firewall	Enable URL Filtering	
IP Filtering MAC Filtering Ort Forwarding URL Filturing DMZ	URL Address:	
	Apply Changes Reset	
Management 	Current Filter Table:	
_ 3	URL Address	Select
	www.url-filter-list.com	
	Delete Selected Delete All Reset	

Fig. 3-23

Item	Description
Enable URL Filtering	Click to enable the URL Filtering function.
URL Address	Add one URL address.
Apply Changes	Click the Apply Changes button to save settings.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.
Delete Selected	Click to delete the selected URL address that will be
	removed from the URL Filtering list.
Delete All	Click to delete all the registered entries from the
	URL Filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.



3.2.4.16 Firewall - 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.

	WLAN Access Point
Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings Firewall Port Filtering MAC Filtering URL Filtering URL Filtering Management Logout	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. F Enable DMZ DMZ Host IP Address: [192.168.8.201] Apply Changes Reset

Fig. 3-24

Item	Description	
Enable DMZ	Click to enable the DMZ function.	
DMZ Host IP Address	To support DMZ in your firewall design, fill in the IP	
	address of DMZ host that can be access from the	
	WAN interface.	
Apply Changes	Click the <i>Apply Changes</i> button to register the IP	
	address of DMZ host.	
Reset	Click the Reset button to abort change and recover	
	the previous configuration setting.	



3.2.4.17 Management - Statistics

This page shows the packet counters for transmission and reception regarding to wireless, Ethernet LAN and Ethernet WAN networks.

onto: Statictice			
Vizard			
on Mode This page shows the parts of the par	cket counters for transmissic	on and reception regarding	g to wireless and Etherne
	Sent Packets	1161	
	Received Packets	239532	
	Sent Packets	5783	
	D : (D) .	5813	
ne Setting Ethernet LAN	Received Packets		
e Setting Ethernet LAN	Sept Packets	5225	



Item	Description
Wireless LAN	It shows the statistic count of sent packets on the
Sent Packets	wireless LAN interface.
Wireless LAN	It shows the statistic count of received packets on
Received Packets	the wireless LAN interface.
Ethernet LAN	It shows the statistic count of sent packets on the
Sent Packets	Ethernet LAN interface.
Ethernet LAN	It shows the statistic count of received packets on
Received Packets	the Ethernet LAN interface.
Ethernet WAN	It shows the statistic count of sent packets on the
Sent Packets	Ethernet WAN interface.
Ethernet WAN	It shows the statistic count of received packets on
Received Packets	the Ethernet WAN interface.
Refresh	Click the refresh the statistic counters on the screen.



3.2.4.18 Management - DDNS

This page is used to configure Dynamic DNS service to have DNS with dynamic IP address.

	WLAN Access Point
	Dynamic DNS Setting
Operation Mode Wireless TCP/IP Settings	Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address. ———————————————————————————————————
Management Management	Enable DDNS
Statistics	Service Provider : DynDNS
Time Zone Setting	Domain Name : host.dyndns.org
Denial-of-Service	User Name/Email:
	Password/Key:
Password Logout	Note: For TZO, you can have a 30 days free trial <u>here</u> or manage your TZO account in <u>control panel</u> For DynDNS, you can create your DynDNS account <u>here</u>
	Apply Change Reset

Fig. 3-26

Item	Description
Enable DDNS	Click the checkbox to enable DDNS service.
Service Provider	Click the drop down menu to pickup the right
	provider.
Domain Name	To configure the Domain Name.
User Name/Email	Configure User Name, Email.
Password/Key	Configure Password, Key.
Apply Change	Click the <i>Apply Changes</i> button to save the enable
	DDNS service.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.



3.2.4.19 Management - Time Zone Setting

This page is used to configure NTP client to get current time.

	WLAN Access Point
 Site contents: Setup Wizard Operation Mode Wireless 	Time Zone Setting You can maintain the system time by synchronizing with a public time server over the Internet.
────────────────────────────────────	Current Time : Yr 2000 Mon 1 Day 1 Hr 2 Mn 28 Sec 7 Time Zone Select : (GMT+08:00)Taipei </td
DDNS	Enable NTP client update
Denial-of-Service	NTP server : 192.5.41.41 - North America
Upgrade Firmware	C (Manual IP Setting)
Save/Reload Setting	Apply Change Reset Refresh

Fig. 3-27

Item	Description
Current Time	It shows the current time.
Time Zone Select	Click the time zone in your country.
Enable NTP client	Click the checkbox to enable NTP client update.
update	
NTP Server	Click select default or input NTP server IP address.
Apply Change	Click the Apply Changes button to save and enable
	NTP client service.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.
Refresh	Click the refresh the current time shown on the
	screen.



3.2.4.20 Management – Denial-of-Service

This page is used to enable and setup protection to prevent attack by hacker's program. It provides more security for users.



Fig. 3-28

Item	Description
Enable DoS	Click the checkbox to enable DoS prevention
Prevention	function.
Whole System Flood	Enable and set up prevention in details.
/ Per-Source IP	
Flood	
Select ALL	Click the checkbox to enable all prevention items.
Clear ALL	Click the checkbox to disable all prevention items.
Apply Changes	Click the <i>Apply Changes</i> button to save above
	settings.



3.2.4.21 Management - Log

This page is used to configure the remote log server and show the current log.

Site contents:	System Log		
Operation Mode Wireless	This page can be used to set remote	log server and show the system log.	
TCP/IP Settings Firewall	Enable Log		
Management		wireless DoS	
	🗆 Enable Remote Log	Log Server IP Address:	
Time Zone Setting Denial-of-Service	Apply Changes		
Upgrade Firmware	Oday 00:41:16 device wla	nO left promiscuous mode	
📲 Save/Reload Setting	Oday 00:41:16 br0: port	1(ethO) entering disabled state	
Password	Uday UU:41:16 device eth	U left promiscuous mode O entered premiscueus mode	
Logout	Oday 00:41:16 device eth	s 8305	
	Oday 00:41:16 device wla	nO entered promiscuous mode	
	Oday 00:41:16 br0: port	2(wlan0) entering listening state	
	Oday 00:41:16 br0: port	1(ethO) entering listening state	
	Oday 00:41:16 br0: port	2(wlan0) entering learning state	
	Uday UU:41:16 brU: port	2(wlanU) entering forwarding state	
	Uday UU:41:16 brU: topol	ogy change detected, propagating	
	0day 00:41:16 br0: port	1(eth0) entering forwarding state	
	Oday 00:41:16 br0: topol	ogy change detected, propagating	
			-

Fig. 3-29

Item	Description
Enable Log	Click the checkbox to enable log.
System all	Show all log of DWR.
Wireless	Only show wireless log.
DoS	Only show Denial-of-Service log.
Enable Remote Log	Click the checkbox to enable remote log service.
Log Server IP	Input the remote log IP address.
Address	
Apply Changes	Click the <i>Apply Changes</i> button to save above
	settings.
Refresh	Click the refresh the log shown on the screen.
Clear	Clear log display screen.



3.2.4.22 Management - Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

	WLAN Access Point
Site contents: Setup Wizard Operation Mode TCP/IP Settings Firewall Status Status DDNS DDNS Donial-of-Service Log Password Password Logout	Upgrade Firmware This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system. Select File: Browse Upload Reset

Fig. 3-30

Item	Description
Select File	Click the Browse button to select the new version
	of web firmware image file.
Upload	Click the Upload button to update the selected web
	firmware image to DWR.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

3.2.4.23 Management - Save/ Reload Settings

This page allows you save current settings to a file or reload the settings from the file that was saved previously. Besides, you could reset the current configuration to factory default.

	WLAN Access Point
Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings Firewall Status Status DDNS Time Zone Setting Denial-of-Service Log Uggrade Firmware Password Logout	Save/Reload Settings This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default. Save Settings to File: Save Load Settings from File: Browse Reset Settings to Default: Reset

Fig. 3-31

Copyright of 3JTech Co., Ltd. (also doing business as A3J Engineering Inc.)



Item	Description
Save Settings to File	Click the Save button to download the configuration
	parameters to your personal computer.
Load Settings from	Click the Browse button to select the
File	configuration files then click the Upload button to
	update the selected configuration to DWR.
Reset Settings to	Click the <i>Reset</i> button to reset the configuration
Default	parameter to factory defaults.

3.2.4.24 Management - Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

	WLAN Access Point
 Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings Firewall 	Password Setup This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.
Management Status Statistics DNS Time Zone Setting Denial-of-Service	Confirmed Password:
Log Dygrade Firmware Save/Reload Setting Control Passy hrg Logout	Apply Changes Reset

Fig. 3-32

Item	Description
User Name	Fill in the user name for web management login
	control.
New Password	Fill in the password for web management login
	control.
Confirmed Password	Because the password input is invisible, so please
	fill in the password again for confirmation purpose.
Apply Changes	Clear the User Name and Password fields to
	empty, means to apply no web management login
	control. Click the Apply Changes button to
	complete the new configuration setting.
Reset	Click the Reset button to abort change and recover
	the previous configuration setting.



3.2.4.25 Logout

This page is used to logout web management page. This item will be activated next time you login after you define user account and password.

	WLAN Access Point
Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings Firewall Status Statistics DDNS Time Zone Setting Denial-of-Service Upgrade Firmware Save/Reload Setting Password	Logout This page is used to logout. Do you want to logout ? Apply Change

Fig. 3-33

	WLAN Access Point
 Site contents: Setup Wizard Operation Mode Wireless TCP/IP Settings Firewall Management Status Statistics DDNS Time Zone Setting Denial-of-Service Lon 	Change setting successfully!
Upgrade Firmware Save/Reload Setting Password Logout	



Item	Description
Apply Change	Click the <i>Apply Change</i> button, Then click <i>OK</i>
	button to logout.



Appendix A – FCC Caution

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

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.

FCC Radiation Exposure Statement

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.