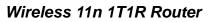
IEEE 802.11n Wireless Series

Wireless-11n-Router

Wireless 11n 2T2R Router







User Manual

Version 2.2 Date: August 19, 2010

FCC Certifications

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.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

CE Mark Warning

€€

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class B for ITE, the essential protection requirement of Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility and R&TTE Directive 1999/5/EC to meet the regulation of the radio equipment and telecommunications terminal equipment.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:

All trade names and trademarks are the properties of their respective companies. Copyright © 2010, All Rights Reserved.

經型式認證合格之低功率射頻電機,非經許可,公司、商號或使用者均不得擅自變更頻率、 加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信;經發現有干擾現象時,應立即停 用,並改善至無干擾時方得繼續使用。前項合法通信,指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Contents

Unpacki	ng In	form	ation ······	3
Chapter	1	Intro	oduction to the Wireless Router	7
1.1 Gene		Gen	eral Description	7
1.2 Key Features				
1.3	1.3 The Front Panel		3	
1.4 The Rear Panel				
1.5		Plac	zement (Optional) 10)
Chapter	2		allation and Basic Configuration11	
2.1		Con	necting This Router to Your Network11	1
2.2		Con	figuring the IP Address of Your Computer11	1
Chapter	3	Web	p-Based Management ······· 14	1
3.1		Star	ting the Web-Based Management Interface14	1
3.2			Graphic User Interface14	
3.3		Setu	ıp Wizard سنان الم	5
3.4	Ope	eratio	on Mode 19	9
3.5		Wire	eless20)
	3.5.1	1	Basic Settings 20)
	3.5.2	2	Advanced Settings 23	3
	3.5.3	3	Security24	1
	3.5.4	4	Access Control 27	7
	3.5.5	5	WDS Settings	3
	3.5.6	6	Mesh Settings 29	9
	3.5.7	7	Site Survey)
	3.5.8	8	WPS Settings	1
	3.5.9	9	Schedule 32	2
3.6		TCF	P/IP Settings ····································	2
	3.6.	1	LAN Interface Setup	2
	3.6.2	2	WAN Interface Setup	5
3.7		Fire	wall Settings 42	2
	3.7.′	1	Port Filter42	2
	3.7.2	2	IP Filter 44	1
	3.7.3	3	MAC Filter	5
	3.7.4	4	Port Forwarding 46	3
	3.7.	5	URL Filter 47	7
	3.7.6	6	DMZ 48	3
	3.7.7	7	VLAN 48	3

3.8	QoS	S	49
3.9	Mar	nagement ·····	50
	3.9.1	Status	50
	3.9.2	Statistics	50
	3.9.3	DDNS Settings	51
	3.9.4	Time Zone Setting	52
	3.9.5	Denial-of-Service	52
	3.9.6	Log	54
	3.9.7	Upgrade Firmware	55
	3.9.8	Save/Reload Setting	55
	3.9.9	Password	56
	3.9.10	Logout	56
Appendi	x A Produ	uct Specifications	57
Appendi	x B Gloss	sary	58

Unpacking Information

Thank you for purchasing the product. Before you start, please check all the contents of this package.

The product package should include the following:

- 1. One Wireless Router
- 2. One Power Adapter
- 3. Antenna
- 4. One resource CD, including:
 - ♦ User's Manual
 - ♦ QIG

Note:

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

Conventions

The Router mentioned in this guide stands for IEEE 802.11n Wireless Router without any explanation.

Chapter 1 Introduction to the Wireless Router

1.1 General Description

IEEE 802.11n Wireless Connectivity

The IEEE802.11n Wireless Router provides a better wireless signal for network than existing wireless 802.11g technology. It complies with IEEE 802.11n and IEEE802.11b/g wireless standards.

Greater Range and Coverage

The router allows multiple users to share one broadband connection, as well as secures your private network. With its built-in switch port and wireless AP, LAN users can share files, printers, or playing network games all at a blazing speed. This technology maximizes the speed and range of your wireless signal to significantly outperform 802.11g devices.

Advanced Network Security

As for security, it also supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or from the Internet. Moreover, supporting for WPA and WPA2 standards ensure that you will be able to use the best possible encryption, regardless of your client devices. In addition, this Wireless 11n Router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

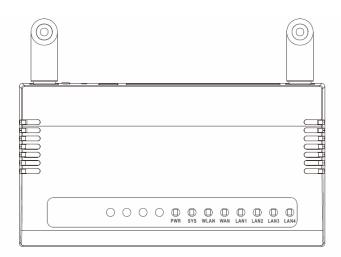
1.2 Key Features

- Supports 2.4 GHz frequency band
- Supports wireless data encryption with WPA, WPA2, Open/ shared key, and pair-wise key authentication services
- Supports QoS: WMM, WMM-SA Client mode, Ingress and Egress bandwidth control
- Supports authentication for wireless connectivity based on ESSID
- Provides MAC access control and hidden SSID function
- Support MDI/MDIX auto crossover function
- Supports NAT IP Sharing and DHCP server
- Supports WAN connection type: Static IP, PPPoE, PPTP, DHCP L2TP client
- Supports ACL, DOS, Virtual DMZ, DNS relay, UPnP, VPN-Pass through
- Supports DDNS (DynDNS, TZO)
- Supports firmware upgrade function via Web

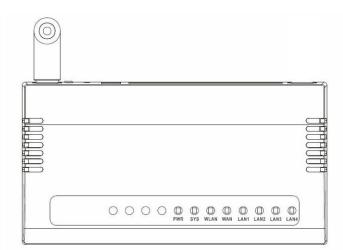
1.3 The Front Panel

The front panel of the Wireless Router:

Wireless 11n 2T2R Router:



Wireless 11n 1T1R Router:



Name	Status	Indication
PWR	Off	No power
FVK	On	Power is on
SYS	Blink Green	System Resetting
515	Dark	System stability
	Off	The wireless function is disabled
WLAN	Flashing	The wireless function is enabled
	Flashing fast	Sending or receiving data over wireless
	Off	There is no device linked to the corresponding port or the connection is dropping off.
WAN / LAN 1-4	On	There are devices linked to the corresponding ports but no data transmitted or received
	Flashing	Sending or receiving data over corresponding port

1.4 The Rear Panel

The rear panel of the Wireless Router is shown below.

Wireless 11n 2T2R Router:



Wireless 11n 1T1R Router



- LAN: Through these ports, you can connect the Router to your PCs and the other Ethernet network devices.
- WAN: This WAN port is where you will connect the cable/DSL Modem, or Ethernet.
- DC IN

Plug the circle end of the power adapter firmly into the rear panel of the Wireless Router, and put the other end into an electric service outlet then the system is ready.

Reset Button

Push the button for more than 5 seconds and then release it, the system will return to factory default setting. In the meantime, system rewrites flash to default value and Status LED flash for a while. Approximately 60 seconds later, the Status LED turn dark, now the whole system parameters have returned to factory default value. If the process has been interrupted by any reason(like power off), the system will fail. Before performing the process, ensure a safe operating environment please!

- Antenna: For the purpose of enhancing the wireless signal, and expanding the range of signal.
- WPS: Help users to connect this Router to Internet quickly. It uses PIN configuration method or PBC configuration method, in which users can easy setup WPS connection. Please refer

to <u>WPS settings</u> for more information.

Warning : Incomplete factory setting recovery procedure will cause the Wireless Router malfunction ! If you are unfortunately in this situation, do not try to repair it by yourself. Consult your local distributor for help!

1.5 Placement (Optional)

There are two ways to place the Router. The first way is to place the Router vertically on a surface. The second way is to attach it to the wall. If you select a wall-mount option, please follow the steps below:

- 1. Select a location with access for cables and a power outlet.
- 2. Unplug the unit. Place it upside down on a flat surface and mark the two holes for anchors.
- 3. Installing the wall mount anchor (not supplied) into the wall with tools such as drill or hammer.
- 4. Insert the screws (not supplied) in each hole of the stand parts.
- 5. Attach the unit to the anchors on the wall.

Chapter 2 Installation and Basic Configuration

This chapter provides a step-by-step guide to the installation and configuration of the Wireless Router. We suggest you go over the whole chapter and then do more advanced operation.

2.1 Connecting This Router to Your Network

Steps to build up the network:

- Connect the phone line from the wall socket to the line-in port on the ADSL modem, or the coaxial cable to the line-in port on the Cable modem.
- Connect the ADSL or Cable modem to the Ethernet WAN port on the back of the Wireless Router by using the UTP cable.
- Plug-in the power adapter to the modem and turn on the power. Install the Ethernet card into the computer by referring to the User Guide that came with the card.
- Connect the computer to the Wireless Router by using standard twisted-pair Ethernet cable from the computer's Ethernet card to a 10/100Mbps Ethernet port on the back of the Wireless Router.
- > Plug-in the power adapter to the Router and the other side to the wall outlet.

2.2 Configuring the IP Address of Your Computer

In order to communicate with this Wireless Router, you have to configure the IP addresses of your computer to make it compatible with the device.

Note: The router supports DHCP server and it is enabled as default. Users that configure your IP address as "**Obtain an IP address automatically**" may skip the following IP configuration instruction.

1. The default network setting of the device:

IP address: 192.168.100.1 Subnet Mask: 255.255.255.0 DHCP Server: enable

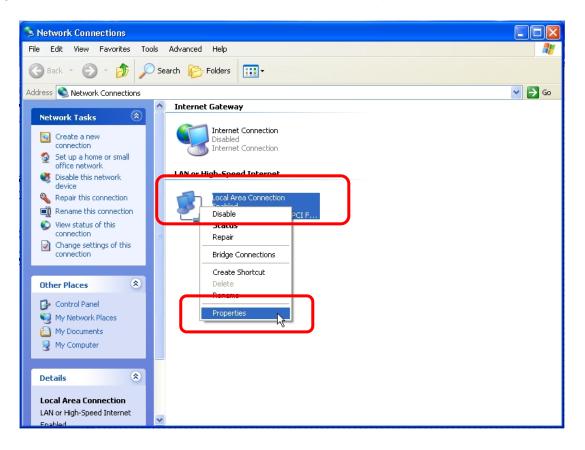
 In the following TCP/IP configuration guide, the IP address "192.168.100.2" is assumed to be your IP address if you want to specify IP addresses manually. Please **DO NOT** choose "192.168.100.1" as the IP address. For the IP address "192.168.100.1" has been set as the default IP for this device. 3. The following TCP/IP configuration guide uses windows XP as the presumed operation system.

Procedures to configure IP addresses for your computer

If you are in Classic Start menu view, click Start > Settings > Network Connections.
 If you are in Start menu view, click Start > Control Panel > Network Connections.



2. Right-click on Local Area Connection item and click on Properties.



3. Choose Internet Protocol (TCP/IP) and click Properties.

🕹 Local Area Connection Properties 🛛 🔹 🛛 🔀
General Authentication Advanced
Connect using:
Realtek RTL8139 Family PCI Fast Ethernet NIC
Configure
This connection uses the following items:
🗹 📮 QoS Packet Scheduler 🗾
AEGIS Protocol (IEEE 003 1x) v3.5.3.0 Internet Protocol (TCP/IP)
Install Uninstall Properties
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

4. You may choose "Obtain an IP address automatically" (recommend) to get IP address automatically or choose "Use the following IP address" to specify IP addresses manually. Please click the OK button after your configuration.

	automatically if your network supports ed to ask your network administrator for
🚫 Obtain an IP address autom	atically
Use the following IP addres	S:
IP address:	192.168.100.2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192.168.100.1
Obtain DNS server address	automatically
💿 Use the following DNS serv	er addresses:
Preferred DNS server:	202 . 96 . 128 . 86
Alternate DNS server:	202 . 96 . 128 . 166
	Advanced

Chapter 3 Web-Based Management

3.1 Starting the Web-Based Management Interface

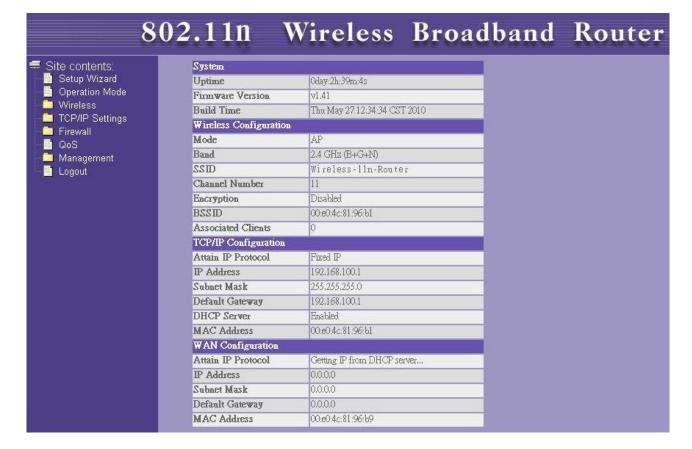
The device uses Web as the management interface. You can use a browser to access the management interface easily. Please follow the steps listed below.

- 1. Open the Internet Web browser.
- 2. Type **192.168.100.1** into the URL Web address location and press Enter.
- 3. The Login window appears.
- Enter admin in the User Name location (default value).
- Enter admin in the Password location (default value).
- Click OK button.

Connect to 192	.168.100.1	? 🗙
R	G	
username and pa Warning: This se	rver is requesting that your username in an insecure manner (basic authent	and
<u>U</u> ser name: ₽assword:	<u>R</u> emember my password	*
	ок с	ancel

3.2 The Graphic User Interface

After the password authorization, the information page shows up as the home page of the Graphic User interface. You may click on each folder on left column of each page to get access to each configuration page. Please note that you should click the Save Settings button to apply your configuration to this device. You can also restore the default settings by clicking the Reset Settings button.



3.3 Setup Wizard

If you are using the router for the first time, please follow the procedures of the setup wizard to do a step-by-step configuration.

Note: The following instruction does an overall introduction to the Setup Wizard. For detail information to each item, please refer to instruction of each page.

1. To start the Setup Wizard, click the "Next" button to proceed.



2. Select your demanding operation mode and click "Next".

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 , L2TP client or static IP.
• 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 , L2TP client or static IP.
Apply Change	Reset

3. Mark the check box to enable synchronizing time by NTP server. Select the religion you live and a NTP server by clicking the drop list then click "Next".

2. Time Zon	2. Time Zone Setting					
You can maintain the system time by synchronizing with a public time server over the Internet.						
 Enable NTP client update Automatically Adjust Daylight Saving 						
Time Zone Select :	(GMT+08:00)Taipei			~		
NTP server :	192.5.41.41 - North America 🔽					
		Cancel	< <back< th=""><th>Next>></th></back<>	Next>>		

4. Specify an IP address and subnet mask for connecting to the router in LAN.

3. LAN Inte	erface Setup		
	figure the parameters for local area network which connects to you may change the setting for IP addresss, subnet mask, DI		
IP Address:	192.168.100.1		
Subnet Mask:	255.255.255.0		
	Cancel	Back	Next>>

5. Select a WAN access type for the router to connect to Internet. Fill in the parameters that required in each blank, and then click the "Next" button. You may get those parameters from your ISP. WAN Access Type : Static IP, DHCP Client, PPPoE, PPTP, L2TP.

4. 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, PPTP or L2TP by click the item value of WAN Access type.					
WAN Access Type:	DHCP Client Static IP DHCP Client PPPoE PPTP L2TP				
			Cancel	< <back< th=""><th>Next>></th></back<>	Next>>

6. Select the wireless parameters that are used for associating with this router and click "Next".

5. Wireless Basic Settings				
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.				
Band:	2.4 GHz (B+G+N) 🐱			
Mode:	AP 💌			
Network Type:	Infrastructure 🐱			
SSID:	Wireless-11n-Router			
Channel Width:	40MHz 🗸			
ControlSideband:	Upper 🗸			
Channel Number:	11 💌			
Country:	USA(FOC)			
Enable Mac Clone (Single Ethernet Client)				
	Cancel < <back next="">></back>			

Items	Information
Band	2.4GHz(B),2.4GHz(G),2.4GHz(N),2.4GHz(B+G),2.4GHz(G+N), 2.4GHz(B+G+N)
Mode	AP, Client, WDS, AP+WDS, AP+MESH, MESH
Network Type	Infrastructure, Ad-hoc
Channel Width	40MHz, 20MHz
Control Sideband	Upper, Lower
Channel Number	Auto,5,6,7,8,9,10,11
Country	This contains USA(FCC), Canada(IC), Europe(ETSI), Spain, France, Japan(MKK)

 Click the drop list to select the encryption type for your wireless network. Fill in the parameters for the encryption type you select and click finish to complete configuration. Encryption type : None, WEP, WPA(TKIP), WPA2(AES), WPA2 Mixed

6. Wire	eless Se	cur	it	ty	1	Se	tu	p									
	vs you setup the my unauthorized									VPA	by u	sin	g En	ayptic	on F	Keys	
Encryption:	None None WEP WPA (TKIP) WPA2(AES) WPA2 Mixed								ſ	Car	nœl		~~	Back		Fin	ished

3.4 Operation Mode

To select an operation mode for this router, click on the mode that you want to perform and click the

Apply Change	button to execute.					
C	Operation Mode					
Ye	You can setup different modes to LAN and WLAN interface for NAT and bridging function.					
0	● 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 , L2TP client or static IP.				
(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 , L2TP client or static IP.				
C	Apply Change	Reset				

3.5 Wireless

3.5.1 Basic Settings

You can set up the configuration of your Wireless basic settings and monitor the Wireless Clients associate with your router.

Wireless Bas	Wireless Basic Settings					
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.						
Disable Wireless LAN Interface						
Band:	2.4 GHz (B+G+N) 💽					
Mode:	AP Multiple AP					
Network Type:	Infrastructure 😒					
SSID:	Wireless-11n-Router					
Channel Width:	40MHz					
Control Sideband:	Upper 😪					
Channel Number:	11 💌					
Country:	USA(FCC)					
Broadcast SSID:	Enabled 🔽					
WMM:	Enabled 😒					
Data Rate:	Auto 🗸					
Associated Clients: Show Active Clients						
Enable Mac Clone (Single Ethernet Client)						
Enable Universal Repeater Mode (Acting as AP and client simultaneouly)						
SSID of Extended Inte	eface:					
Apply Changes Reset						

Items	Information
Disable Wireless LAN Interface	Mark the checkbox to disable interface of Wireless LAN
Band	To select a band for this device to match 802.11b, 802.11g, 802.11n, 802.11b/g, 802.11g/n or 802.11b/g/n. optional parameters:

	2.4GHz(B),2.4GHz(G),2.4GHz(N),2.4GHz(B+G),2.4GHz(G+N), 2.4GHz(B+G+N)
Mode	Configure this device as AP, Client, WDS or AP+WDS. If you set this device as AP or AP+WDS mode, the Multiple AP button is available for you to set up four SSID for this wireless network. Click on this button to do more configurations.
Network Type	 When you configure this device in Client mode, this drop-down list allows users to change the network type into infrastructure mode or ad-hoc mode. Ad-Hoc mode: Connects two computers directly without the use of a router or AP. It is also know as a peer-to-peer network. Infrastructure Mode: The wireless network contains at least one wireless
	client and one wireless AP or router. This client connects to Internet or intranet by communicating with this wireless AP.
SSID	Service set identifier (SSID) for the name of the wireless network.
Channel Width	Select to use 20MHz or 40MHz as the wireless channel frequency.
Control Sideband	If you have selected the channel width of 40MHz for this router, you can control this router to use the frequency for a deflection of "Upper" or "Lower."
Channel Number	Select a channel for the wireless network of this device.
Country	This contains USA(FCC), Canada(IC), Europe(ETSI), Spain, France, Japan(MKK)
Broadcast SSID	If you enable "Broadcast SSID", every wireless station located within the coverage of this wireless router can discover this wireless router easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast SSID" can provide better security.
WMM	This will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network. WMM is not available in 11n mode.
Data Rate	The transmit limitation of data packets of this wireless router. The wireless router will use the highest possible selected transmission rate to transmit the data packets.
Associated Client	Click "Show Active Clients" button, then an "Active Wireless Client Table" pops up. You can see the status of all active wireless stations that are connecting to the access point.
Enable MAC clone	Mark the checkbox to clone the MAC address of the device. This function is only available when you set this router as Client mode. You can also manually set the MAC address in WAN setting.
Enable Universal Repeater Mode	Mark this checkbox to enable Universal Repeater Mode which acts this device as an AP and client simultaneously.
SSID of Extended Interface	While you enable the Universal Repeater Mode, you have to specify an SSID for the extended interface.

* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

1. Multiple APs

This is the window that pops up after clicking the Multiple AP button.

		rs and updates the wireless						
No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List
AP1		2.4 GHz (B+G+N) 💟	Wireless-11n-A	Auto 🐱	Enabled 🔽	Enabled 👻	LAN+WAN 🐱	Show
AP2		2.4 GHz (B+G+N) 🔽	Wireless-11n-A	Auto 🔽	Enabled	Enabled 🗸	LAN+WAN 👻	Show
٩РЗ		2.4 GHz (B+G+N) 🔽	Wireless-11n-A	Auto 😽	Enabled 🔽	Enabled 🔽	LAN+WAN 🐱	Show
4P4		2.4 GHz (B+G+N) 🗸	Wireless-11n-A	Auto 🗸	Enabled 🗸	Enabled 🗸	LAN+WAN 🗸	Show

Select one of the AP, and then click the button "Show", "Active Wireless Client Table – AP1" windows pops up.

C Acti	tive Wireless Client Ta	ible - Window	vs Internet Explo	otet				
🥭 http	p://192.168.100.1/wlstatbl_	vap.asp?id=1						~
	Active Wire This table shows the M. client.					d status for each	associated wirele	as
	MAC Address	Mode	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)	
	None							
<	Refiresh Close							
Done					9	Internet	•	100%:

2. Active Wireless Client Table

This is the window that pops up after clicking the

Show Active Clients button.

🖉 Active Wireless Client Table - Windows Internet Explorer http://192.168.100.1/wlstatbl.asp v Active Wireless Client Table MAC Tx Rate Power Expired Mode Tx Packet Rx Packet Saving Address (Mbps) Time (s) Close Refresh

3.5.2 Advanced Settings

You can set advanced wireless LAN parameters for this router. We recommend not changing these parameters unless you know what changes will be on this router.

Wireless Advanced Settings These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have				
on your Access Point,				
Fragment Threshold:	2346 (256-2346)			
RTS Threshold:	2347 (0-2347)			
Beacon Interval:	100 (20-1024 ms)			
Preamble Type:	● Long Preamble ● Short Preamble			
IAPP:	• Enabled • Disabled			
Protection:	Enabled O Disabled			
Aggregation:	• Enabled • Disabled			
Short GI:	Enabled Disabled			
WLAN Partition:	Enabled O Disabled			
RF Output Power:	●100% ●70% ●50% ●35% ●15%			
Apply Changes Re	set			

Items	Information
Fragment Threshold	This value should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase your fragmentation threshold within the value range of 0 to 2346. Setting the fragmentation threshold too low may result in poor performance.
RTS Threshold	Request To Send Threshold. This value should remain at its default setting of 2347. If you encounter inconsistent data flow, only minor modifications to the value range between 1 and 2347 are recommended.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. Default (100ms) is recommended.
Preamble Type	The length of CRC blocks in the frames during the wireless communication.
IAPP	To enables multiple AP to communicate and pass information regarding the location of associated Stations.
Protection	Some 802.11g wireless adapters support 802.11g protections, which allows the adapter search for 802.11b/g singles only. Select "Enabled" to support protection or select "Disabled" to disable this function.
Aggregation	To aggregate lots of packets into a big one before transmitting packets. This can reduce control packet overhead.
Short GI	Indicates that the 802.11g network is using a short slot time because there are no legacy (802.11b) stations present
WLAN Partition	WLAN Partition controls your inter-client communication. Enabling WLAN Partition prevents associated wireless clients from communicating with each other.
RF Output Power	Select the signal strength for the wireless network.

* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

3.5.3 Security

The Security function protects your wireless network from invasion. We provide WEP and WPA encryption to secure your wireless network. Please select Disable, WEP, WPA, WPA2, and WPA-Mixed in the drop list. If you select none, any data will be transmitted without encryption and any station can access the router.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:	Root AP - Wireless-11	In-Router 💌	Apply Changes	Reset	
Encry	ption:	Disable	~		
802.1	x Authentication:				

Items	Information
Select SSID	Please choose a SSID you have set for this router in the <u>Wireless ></u> <u>Basic Settings</u> from the drop-down list. The SSID will be shown on the wireless network for recognizing.
Encryption	There are 5 modes for you to select: Disable, WEP, WPA, WPA2, and WPA-Mixed. Please refer to the following description.
802.1x Authentication	Users that do not use this function or connecting to an open-wireless network please skip this part. Please configure the settings in accordance with the Certificated Server.

1. Security Mode -- WEP

Wireless Security Setup						
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.						
Select SSID: Root AP - Wireless-11n-	Router 🖌 Apply Changes Reset					
Encryption:	WEP					
802.1x Authentication:						
Authentication:	● Open System ● Shared Key ● Auto					
Key Length:	64-bit 🔽					
Key Format:	Hex (10 characters) 💽					
Encryption Key:	*****					
RADIUS Server IP Address						
RADIUS Server Port:	1812					
RADIUS Server Password:						

Items	Information		
Encryption	Select a security encryption mode for this router.		
802.1x Authentication	Users that do not use this function or connecting to an open-wireless network please skip this part. Please configure the settings in accordance with the Certificated Server.		
Authentication	There provide three options for selecting: Open System, Shared Key, Auto		
Key Length	Select 64-bit or 128-bit as the key encryption length.		
Key Format	Select ASCII ¹ or Hex ² to setup the key value.		
Encryption Key	Enter the key according to the key format you select.		

* Please click on the Apply Changes button or the Reset button to save/reset the configurations.

2. Security Mode – WPA / WPA 2

Wireless Security Sec	etup
This page allows you setup the wireless se any unauthorized access to your wireless n	curity. Turn on WEP or WPA by using Encryption Keys could prevent etwork.
Select SSID: Root AP - Wireless-11r	n-Router 💌 Apply Changes Reset
Encryption:	WPA2
Authentication Mode:	 Enterprise (RADIUS) Personal (Pre-Shared Key)
WPA2 Cipher Suite:	TKIP 🗹 AES
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

Items	Information		
Authentication Mode	There are two items, "Enterprise (RADIUS)" and "Personal (Pre-Shared Key)". You can select the mode by clicking the item.		
WPA Cipher Suite	Select the WPA Cipher Suite to be TKIP or AES.		
Pre-Shared Key Format	To decide the format, select Pass phrase or Hex in the drop list.		
Pre-Shared Key	Enter the Pre-shared Key according to the pre-shared key format you select. This is the shared secret between AP and STA. This field must be filled with character longer than 8 and less than 64 lengths.		

* Please click on the Apply Changes button or the Reset button to save/reset the configurations.

¹ ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. ² Hexadecimal digits consist of the numbers 0-9 and the letters A-F.

3. Security Mode – WPA-Mixed

Wireless Security Setup					
This page allows you setup the wineless se any unauthorized access to your wireless n	curity. Turn on WEP or WPA by using Encryption Keys could prevent etwork.				
Select SSID: Root AP - Wireless-11	n-Router 🖌 🛛 Apply Changes 🔹 Reset				
Encryption:	WPA-Mixed				
Authentication Mode:	Enterprise (RADIUS) • Personal (Pre-Shared Key)				
WPA Cipher Suite:	TKIP 🖾 AES				
WPA2 Cipher Suite:	TKIP 🖾 AES				
Pre-Shared Key Format:	Passphrase				
Pre-Shared Key:					

Items	Information			
Authentication Mode	There are two items, "Enterprise (WPA-Radius)" and "Personal (Pre-Shared Key)". You can select the mode by clicking the item.			
WPA / WPA2 Cipher Suite	Select the WPA/WPA2 Cipher Suite to be TKIP or AES.			
Pre-Shared Key Format	To decide the format, select Passphrase or Hex in the drop list.			
Pre-Shared Key	Enter the Pre-shared Key according to the pre-shared key format you select. This field must be filled with character longer than 8 and less than 64 lengths.			

* Please click on the **Apply Changes** button or the **Reset** button to save/reset the configurations.

3.5.4 Access Control

To restrict the clients of Access authentication of Stations, set up the control list in this page.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Comment:	
	Comment:

Items	Information		
Wireless Access Control Mode	Click on the drop list to choose the access control mode. You may select "Allow listed" to allow those allowed MAC addresses or select "Deny Listed" to ban those MAC addresses from accessing to this device or select "Disable".		
MAC Address & Comment	Fill in the MAC address that you wish to control, and give a definition to it.		
Current Access Control list	Lists the MAC Access Control Settings you have added before. Click on the list to change configuration. To Delete the station on the list, mark the check box in the select item and click the "Delete Selected". If you want to delete all stations on the list, click "Delete All" to remove all of them.		

* Please click on the Apply Changes button or the Reset button to save/reset the configurations.

3.5.5 WDS Settings

When you use this device as WDS or AP+WDS mode, "WDS Setting" function can be operated. Wireless Distribution System allows the router to communicate with other APs wirelessly. To make it work, you must ensure that these APs and the Router are in the same channel. Please add these APs MAC address and comment values into the WDS list. Don't Forget to Enable the WDS by click the check box of "Enable WDS" and press "Apply Changes" button to save. To Delete the AP on the list, Click the check box in the select item and click the "Delete Selected". If you want to delete all APs on the list, click "Delete All" to remove all of them.

WDS Setti	ings			
does. To do this, you	must set these .	rireless media to comm APs in the same chann : table and then enable	el and set MAC addre	s, like the Ethernet ss of other APs which
Enable WDS				
MAC Address:				
Data Rate:	Auto 🔽			
Comment:	-			
Apply Changes	Reset	Set Security	Show Statistics	1
Current WDS AP	List:			
MAC Addre	ess Ti	Rate (Mbps)	Comment	Select
Delete Selected	Delete Al	I Reset		

Items	Information			
Enable WDS	Click to enable WDS.			
MAC Address & Comment	Fill in the MAC address that you wish to control, and give a definition to it.			
Data Rate	The transmit limitation of data packets of this wireless rout The wireless router will use the highest possible select transmission rate to transmit the data packets.			
Current WDS AP List	Lists the WDS Settings you have added before. Click on the list to change configuration. To Delete the station on the list, mark the check box in the select item and click the "Delete Selected". If you want to delete all stations on the list, click "Delete All" to remove all of them.			

3.5.6 Mesh Settings

A Wireless Mesh Network (WMN) is a communications network made up of radio nodes organized in a mesh topology. Mesh networking allows for continuous connections and reconfiguration around broken or blocked paths by "hopping" from node to node until the destination is reached.

Wireless Mesh Network Setting

Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.

Mesh ID:	Wireless-mesh
Encryption:	None
Pre-Shared Key Format:	Passphrase
re-Shared Key:	

Items	Information		
Enable Mesh	Click this checkbox to enable mesh.		
Mesh ID	A character string ranging form 1 to 32 that will be used in the mesh node beacons.		
Encryption	Select a security encryption mode for this router.		
Pre-Shared Key Format	To decide the format, select Passphrase or Hex in the drop list.		
Pre-Shared Key	Enter the Pre-shared Key according to the pre-shared key format you select. This is the shared secret between AP and STA. This field must be filled with character longer than 8 and less than 64 lengths.		

3.5.7 Site Survey

This page shows available wireless network information. When you use this device as a client station (STA), you may connect to other AP or Router. Select one of the lists in the site survey

table and click on Connect to other wireless network nearby. The Refresh button

can be used to scan nearby Router and AP again.

Wireless Site	Survey			
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.				
List of APs				
CII22	BSSID	Channel	Туре	Encrypt Signal
None				
Refresh Connect				

3.5.8 WPS Settings

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This Router supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

Wi-Fi Protected Setup		
This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.		
Disable WPS		
WPS Status:	O Configured 💿 UnConfigured	
	Reset to UnConfigured	
Self-PIN Number:	24266505	
Push Button Configuration:	Start PBC	
Apply Changes Reset		
Client PIN Number:	Start PIN	

Items	Information
Disable WPS	Click this checkbox to undo WPS.
WPS Status	You cannot manually select the items here. The WPS Status will change from "UnConfigured" to "Configured" after you enable WPS function and setup a wireless security key for this device.
Self-PIN Number	If you use this device as a client, you can use this code when trying to connect this device to other AP by using the PIN method.
Push Button Configuration	Push Button Communication (PBC) method use a simple action of pushing a button on both the AP and the new STA to reach the function of easy setup WPS connection. You can simply click the Start PBC button in this GUI page. After click on the button, please run the client's WPS and push the PBC button within 2 minutes.
Client PIN Number	Personal Identification Number (PIN) method. Users have to fill in the PIN code of enrollee device and click on the communication with other AP. After click on the button, please run the client's WPS and push the PIN button within 2 minutes.

*Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

3.5.9 Schedule

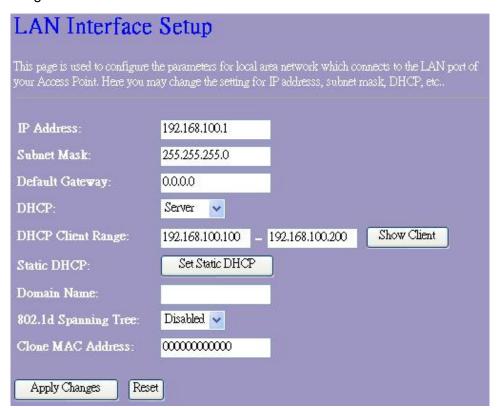
You can configure the schedule via this page. Click "Enable Wireless Schedule", then configure days or time which you want. Wireless will start or stop at your scheduled time. Please do not forget to configure system time before enabling this feature.

Wireless Schedule
This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.
Enable Wireless Schedule
Days : Everyday Sun Mon Tue Wed Thu Fri Sat
Time : 24 Hours
Apply Changes Reset

3.6 TCP/IP Settings

3.6.1 LAN Interface Setup

To set up the configuration of LAN interface, private IP of your router LAN port and subnet mask for your LAN segment.



Items	Information
IP Address	The IP of your Router LAN port (default 192.168.100.1).
Subnet Mask	Subnet Mask of you LAN (default 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.
Default Gateway	Enter the IP Address of the router in your network.
DHCP	DHCP stands for Dynamic Host Configuration Protocol. It is a protocol for assigning dynamic IP addresses "automatically." You can select to use this router as a DHCP client or DHCP server. To give your LAN client an IP, you have to enable "DHCP Server". If not, manual setting up your client IP is necessary when you want to use the router as your client's default gateway.
DHCP Client Range	Specify the DHCP Client IP address range (default start from 150 and end to 200). You can also click the "Show Client" button to list those connected DHCP clients.
Static DHCP	This function is only available when you use this router as a DHCP server. This router may automatically assign the static DHCP address to the specific clients.
Domain Name	(Optional) The name of your local domain.
802.1d Spanning Tree	To prevent from network loops and preserve the quality of bridged network
Clone MAC Address	Your ISP may require a particular MAC address in order to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. MAC cloning feature allows the MAC address reported by WAN side network interface card to be set to the MAC address already registered with the ISP eliminating the need to register the new MAC address with the ISP. This feature does not change the actual MAC address on the NIC, but instead changes the MAC address reported by Wireless Router to client requests. To Change the MAC address, enter it in the text box.

* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

1. Active DHCP Client List

This is the window that pops up after clicking the Show Client button. It shows the information of IP/MAC address and expire time of the DHCP clients that have connected with this device.

92.168.100.1/dhcptbl.a	sp		
Active DHO	CP Client Table		
	igned IP address, MAC address	and time expired for each DHCP lease	1
This table shows the ass lient.	igned IP address, MAC address	and time expired for each DHCP lease	4
	igned IP address, MAC address	and time expired for each DHCP lease	9
	igned IP address, MAC address MAC Address	and time expired for each DHCP lease Time Expired(s)	1

2. Static DHCP Setup

This is the window that pops up after clicking the

Set Static DHCP

button. Click on the list to

change configuration. To delete the station on the list, mark the check box in the select item and click the "Delete Selected". If you want to delete all stations on the list, click "Delete All" to remove all of them.

Static DHCP Setup			
This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address and assign the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.			
Enable Static DHCP			
IP Address:			
MAC Address:			
Comment:			
Apply Changes Reset			
Static DHCP List:			
IP Address	MAC Address	Comment	Select
Delete Selected Delete All	Reset		

3.6.2 WAN Interface Setup

This page allows users to configure those parameters for connecting to Internet. You may select the Internet connection type from the "My Connection type" drop list and configure parameters for each mode. Five modes for selection: Static, DHCP, PPPoE, L2TP, and PPTP mode.

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, PPTP or L2TP by click the item value of WAN Access type.	
WAN Access Type:	DHCP Client
Host Name:	
MTU Size:	1492 (1400-1492 bytes)
• Attain DNS Automatically	
• Set DNS Manually	
DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	0000000000
📃 Enable uPNP	
Enable IGMP Proxy	
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	
Apply Changes Reset	

1. Static Mode (fixed IP)

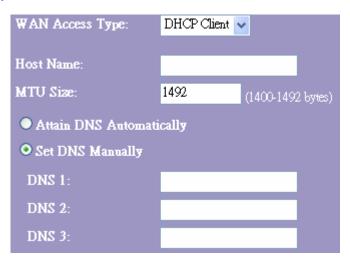
Devices that are assigned the same IP address may not be visible on the network. Enter the IP address of the DNS server. The DNS server translates domain names into IP addresses.

WAN Access Type:	Static IP 🐱
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:	

Items	Information
IP Address, Subnet Mask and Default Gateway	Fill in the IP address, Subnet Mask and Default Gateway that provided by your Internet Service Provider (ISP).
MTU Size	To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter the MTU number in the blank to set the limitation (default 1500 bytes).
DNS 1~3	To specify the Domain Name System (DNS). The DNS server translates domain names into IP addresses. Enter the DNS provided by your ISP in first, second and third server.

* Please click on the Apply Changes button or the Reset button at the bottom to save/reset the configurations.

2. DHCP (Auto Config)



Items	Information	
Host Name	The name of this device.	
MTU Size	To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter your MTU number in the text-box to set the limitation (default 1492 bytes).	
Attain DNS Automatically	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically	
Set DNS ManuallyTo specify the Domain Name System (DNS). The server translates domain names into IP addresse Enter the DNS provided by your ISP in first, second third server.		

3. PPPoE (ADSL)

WAN Access Type:	PPPoE	~		
User Name:	-			
Password:				
Service Name:				
Connection Type:	Continuous	*	Connect	Disconnect
Idle Time:	5	(1-1000 m	dinutes)	
MTU Size:	1452	(1 <i>36</i> 0-149	2 bytes)	
• Attain DNS Automat	icall y			
• Set DNS Manually				
DNS 1:				
DNS 2:				
DNS 3:	-			

Items	Information		
Username, Password and Service Name	Fill in the User Name, password and service name that provided by your ISP.		
	There are three connection types:		
	"Continuous": always keep connection.		
Connection Type	" Connect on demand ": bill by connection time. You can set up the idle time for the value. Specifies the number of time that elapses before the system automatically disconnects the PPPoE session.		
	"Manual": To connect to ISP, click "Connect" manually from the WEB user interface. The WAN connection will not lose its connection even the idle time is out. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.		
Idle Time	The value specifies the number of idle time that elapses before the system automatically disconnects the PPPoE session.		
MTU Size	To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance.		
	Enter your MTU number in the text-box to set the limitation (default 1452 bytes).		
Attain DNS Automatically	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically		
Set DNS Manually	To specify the Domain Name System (DNS). The DNS server translates domain names into IP addresses. Enter the DNS provided by your ISP in first, second and third server.		

4. PPTP

WAN Access Type:	PPTP 💽
IP Address:	172.1.1.2
Subnet Mask:	255.255.255.0
Server IP Address:	172.1.1.1
User Name:	
Password:	
Connection Type:	Continuous Connect Disconnect
Idle Time:	5 (1-1000 minutes)
MTU Size:	1460 (1400-1460 bytes)
Request MPPE En	cryption 📃 Request MPPC Compression
• Attain DNS Autom	tically
• Set DNS Manually	
DNS 1:	
DNS 2:	
DNS 3:	

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks (VPNs).

Items	Information			
IP address & Subnet MaskFill in IP address & Subnet Mask that match subnet provided by your Internet Service Provid				
Username and Password	Fill in Username and Password that provided by your Internet Service Provider (ISP).			
Idle Time	The value specifies the number of idle time that elapses before the system automatically disconnects the PPTP session.			
MTU Size	To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter the MTU number in the blank to set the limitation (default 1460 bytes).			

Request MPPE Encryption	Mark to enable the Microsoft Point-to-Point Encryption function. MPPE compresses data across PPP or VPN links.	
Request MPPC Compression	Mark to enable the Microsoft Point-to-Point Compression function. MPPC can only be used in products that implement the Point to Point Protocol AND for the sole purpose of interoperating with other MPPC and Point to Point Protocol implementations.	
Attain DNS Automatically	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically	
DNS 1~3	To specify the Domain Name System (DNS). The Dispervent translates domain names into IP addresses. Entite DNS provided by your ISP in first, second and the server.	

5. L2TP

The Layer Two Tunneling Protocol (L2TP) provides a standard method for transporting the link layer of the Point-to-Point Protocol (PPP) between a dial-up server and a Network Access Server, using a network connection in lieu of a physical point-to-point connection.

WAN Access Type:	L2TP	~		
IP Address:	172.1.1.2			
Subnet Mask:	255.255.255.	0		
Server IP Address:	172.1.1.1			
User Name:				
Password:				
Connection Type:	Continuous	~	Connect	Disconnect
Idle Time:	5	(1-1000 n	uinutes)	
MTU Size:	1460	(1400-146	50 bytes)	
 Attain DNS Automat Set DNS Manually 	iicall y			
DNS 1:				
DNS 2:				
DNS 3:	198 <u>-</u>			

Items	Information			
IP address & Subnet Mask	Fill in IP address & Subnet Mask that match the same subnet provided by your Internet Service Provider (ISP).			
Username and Password	Fill in the Username and Password that provided by your Internet Service Provider (ISP).			
MTU Size	To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter the MTU number in the blank to set the limitation (default 1460bytes).			
Attain DNS Automatically	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically			
DNS 1~3	To specify the Domain Name System (DNS). The DNS server translates domain names into IP addresses. Enter the DNS provided by your ISP in first, second and third server.			

6. Common configurations for WAN interface

Clone MAC Address: 00000000000
Enable uPNP
Enable IGMP Proxy
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
Apply Changes Reset

There are some settings are able to be configured on each WAN access type:

Items	Information
Clone MAC Address	When ISP use MAC address authentication (with DHCP), then the MAC address of the Ethernet card attached to your Cable modem must be registered with the ISP before connecting to the WAN (Internet). If the Ethernet card is changed, the new MAC address must be registered with the ISP.

	MAC cloning feature allows the MAC address reported by WAN side network interface card to be set to the MAC address already registered with the ISP eliminating the need to register the new MAC address with the ISP. This feature does not change the actual MAC address on the NIC, but instead changes the MAC address reported by Wireless Router to client requests. To Change the MAC address, enter it in the text box.	
Enable uPNA	Click to enable Universal Plug and Play for dynamically attaching devices directly to a computer, enabling clients that recognize the types of the devices to immediately begin using the device.	
Enable IGMP Proxy	Enable IGMP proxy for the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts.	
Enable Ping Access on WAN	Click to enable your WAN IP address to be pingable.	
Enable Web Server Access on WAN from port	To Enable the user to access this Router with WAN port IP address from Internet	
Enable IPsec pass through on VPN connection	Mark the check box to enable IPsec pass through on VPN connection and clear the checkbox to disable.	
Enable PPTP pass through on VPN connection	Mark the check box to enable PPTP pass through on VPN connection and clear the checkbox to disable.	
Enable L2TP pass through on VPN connection	Mark the check box to enable L2TP pass through on VPN connection and clear the checkbox to disable.	

3.7 Firewall Settings

3.7.1 Port Filter

The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users. Port filter restricts certain type of data packets from your LAN to Internet through the router.

Wireless 11n Router

Port Filtering			
Entries in this table are used to through the Gateway. Use of s			
Enable Port Filtering	1		
Port Range: 🗾 –	Protocol: Both	Comment:	
Apply Changes Rec	Both TCP UDP		
Current Filter Table:			
Port Range	Protocol	Comment	Select
Delete Selected Del	ete All Reset		

Items	Information
Enable Port Filtering	Mark to enable the configuration, and clear to disable.
Port Range	Fill in the port range that you wish to filter. The valid numbers are 1~65535.
Protocol	Select the protocol type of TCP, UDP or Both.
Comment	Input any text to describe this mapping
Current Filter Table	Lists the Port Filter Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.

* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

3.7.2 IP Filter

The Wireless Router could filter the outgoing packets for security or management consideration.

IP Filtering			
Entries in this table are used to rea through the Gateway. Use of such			
Enable IP Filtering			
Loal IP Address:	110(0001.	<mark>h 🔽</mark> Comment:	
Apply Changes Reset		P	
Current Filter Table:			
Local IP Address	Protocol	Comment	Select
Delete Selected Delete	All Reset		

Items	Information
Enable IP Filtering	Mark to enable the configuration, and clear to disable.
Local IP Address	Fill in the IP address that you wish to filter.
Protocol	Select the protocol type of "TCP", "UDP" or both.
Comment	Input any text to describe this mapping,
Current Filter Table	Lists the IP Filter Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.

* Please click on the Apply Changes button or the Reset button at the bottom to save/reset the configurations.

3.7.3 MAC Filter

The Wireless Router could filter the outgoing packets for security or management consideration.

MAC Filtering		
Entries in this table are used to restrict certain types through the Gateway. Use of such filters can be he		
Enable MAC Filtering		
MAC Address: Com	ument:	
Apply Changes Reset		
Current Filter Table:		
MAC Address	Comment	Select
Delete Selected Delete All Reset		

Items	Information
Enable MAC Filtering	Mark to enable the configuration, and clear to disable.
MAC Address	Fill in the MAC address that you wish to filter.
Comment	Input any text to describe this mapping.
Current Filter Table	Lists the MAC Filter Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.

Please click on the Apply Changes button or the Reset button at the bottom to save/reset the configurations.

3.7.4 Port Forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address.

Port Forward	ding			
Entries in this table allow NAT firewall. These setti server on the private local	ngs are only necessa	ry if you wish to host	some sort of server	
Enable Port For	warding			
IP Address:	TTOROGOL.	Both <mark>></mark> Port Ran, Both	ge:	Comment:
Apply Changes	Reset	TCP UDP		
Current Port Forward Local IP Address	ing Table: Protocol	Port Range	Comment	Select
Delete Selected	Delete All	leset		

Items	Information	
Enable Port Forwarding	Mark to enable the configuration, and clear to disable.	
IP Address	Fill in the IP address that you wish to forward.	
Protocol	Select the protocol type of TCP, UDP or Both.	
Port Range	Fill in the port range that you wish to forward. The valid numbers are 1~65535.	
Comment	Input any text to describe this mapping.	
Current Port Forwarding Table	Lists the Port Forward Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.	

Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

3.7.5 URL Filter

The URL Filter allows users to prevent certain URL from accessing by users in LAN. This filter will block those URLs that contain certain keywords.

URL Filtering	
URL filter is used to deny LAN users from accessing the inter keywords listed below.	net. Block those URLs which contain
Enable URL Filtering	
URL Address:	
Apply Changes Reset	
Current Filter Table:	
URL Address	Select
Delete Selected Delete All Reset	

Items	Information
Enable URL Filtering	Mark to enable the configuration, and clear to disable.
URL Address	Fill in the URL address that you wish to filter.
Current Filter Table	Lists the URL Filter Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.

* Please click on the Apply Changes button or the Reset button at the bottom to save/reset the configurations.

3.7.6 DMZ

To configure it, mark to enable virtual DMZ and then enter the Host IP (private IP address) and

click	Apply Changes to enact the setting.
	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.
	Enable DMZ DMZ Host IP Address:
	Apply Changes Reset

3.7.7 VLAN

VLAN(Virtual LAN), is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. Click Enable VLAN to make the configuration for the ports and virtual APs.

				lity, security, and r		
Ena	ble VLAN					
inable	Ethernet/Wireless	WAN/LAN	Tag	VID (1~4090)	Priority	CF
	Ethemet Port1	LAN		3022	7 🗸	V
	Ethemet Port2	LAN		3030	0 👻	
	Ethemet Port3	LAN		500	3 👻	
	Ethernet Port4	LAN		1	0 🗸	V
	Wireless Primary AP	LAN		1	0 👻	
	Virtual AP1	LAN		1	0 👻	
	Virtual AP2	LAN		1	0 🛩	M
	Virtual AP3	LAN		1	0 🗸	
	Virtual AP4	LAN		1	0 👻	V
-	Ethernet Port5	WAN		1	0 🗸	~

3.8 QoS

The QoS (Quality of Service) Settings page provides different priority to different users.

QoS
Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized ove other network traffic, such as FTP or Web.
Enable QoS
Automatic Uplink Speed
Manual Uplink Speed (Kbps): 512
Automatic Downlink Speed Manual Downlink Speed (Kbps): ⁰
QoS Rule Setting:
Address Type: IP MAC
Local IP Address:
MAC Address:
Mode: Guaranteed minimum bandwidth 😪
Uplink Bandwidth (Kbps):
Downlink Bandwidth (Kbps):
Comment:
Apply Changes Reset
Current QoS Rules Table:
Local IP Address MAC Address Mode Uplink Downlink Bandwidth Bandwidth Comment Select
Delete Selected Delete All Reset

3.9 Management

3.9.1 Status

This information page shows the current settings of this device. You could check if the parameters match your configuration.

System		
Uptime	Oday:2h:39m:4s	
Firmware Version	v1.41	
Build Time	Thu May 27 12:34:34 CST 2010	
Wireless Configuration		
Mode	AP	
Band	2.4 GHz (B+G+N)	
SSID	Wireless-11n-Router	
Channel Number	11	
Encryption	Disabled	
BSSID	00:e0:4c:81:96:b1	
Associated Clients	0	
TCP/IP Configuration		
Attain IP Protocol	Fixed IP	
IP Address	192.168.100.1	
Subnet Mask	255.255.255.0	
Default Gateway	192.168.100.1	
DHCP Server	Enabled	
MAC Address	00:e0:4c:81:96:b1	
WAN Configuration		
Attain IP Protocol	Getting IP from DHCP server	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Default Gateway	0.0.0	
MAC Address	00:e0:4c:81:96:b9	

3.9.2 Statistics

This page allows users to get information of data transferring condition, and monitor the status and performance of this router including receiving and sending packets. To see the latest report,

click Refresh button.

is page shows the pa works.	cket counters for transmissio	n and reception regar	ding to wireless and Ether
ewolka.			
Wireless LAN	Sept Packets	4563	
A HEIC22 L'HIM	Received Packets	211881	
	Sent Packets	2725	
Ethernet LAN	Received Packets	7941	-
	Sept Packets	426	-
Ethernet WAN	Received Packets	0	

3.9.3 DDNS Settings

DDNS (Dynamic Domain Name Server) service allows users to connect to this device via a fixed and easy-to-remember hostname. This router supports DDNS service of following service providers:

DynDNS (http://www.dyndns.org), TZO (http://www.tzo.com)

Please go to one of DDNS service provider's web page listed above, and get a free DDNS account by the instructions given on their web page.

Dynamic DN	NS Setting
	e, that provides you with a valid, unchanging, internet domain name (an URL) everchanging) IP-address.
Enable DDNS	
Service Provider :	DynDNS w
Domain Name :	host,dyndns.org
User Name/Email:	
Password/Key:	
	a 30 days free trial <u>bere</u> or manage your TZO account in <u>control panel</u> reate your DynDNS account <u>bere</u>
Apply Change	Reset

Items	Information	
Service Provider	The website that provides DDNS service. Please select from the drop-down list.	
Domain Name	The hostname that you have applied for the device.	
User Name/Email	DDNS login account. For DynDNS users, please fill in your user name; for TZO users, please fill in your email address.	
Password/Key	The password of your DDNS service account.	

3.9.4 Time Zone Setting

This page allows users to configure the time of the router. To specify manually, fill in the blanks in "Current Time" and click the "Apply Change" button. To synchronize time from a timeserver, please mark the "Enable NTP client update" checkbox, select a NTP server from the drop list or manually enter a NTP server. Click the "Apply Change" button after your configuration.

Time Zone	Setting
You can maintain the sys	tern time by synchronizing with a public time server over the Internet.
Current Time :	Yr 2010 Mon 6 Day 18 Hr 16 Mn 29 Sec 59 Copy Computer Time
Time Zone Select :	(GMT+08:00)Taipei
Enable NTP clip	ent update
Automatically A	Adjust Daylight Saving
NTP server :	192.5.41.41 - North America
	(Manual IP Setting)
Apply Change	Reset Refresh

3.9.5 Denial-of-Service

A DoS (Denial of Service) attack attempt to disrupt the network and information system by sending abnormal packets to overload your Internet connection. DoS protect function helps to detect and

Wireless 11n Router

block those malevolent DoS attack. It is strongly recommended that this setting be left enabled. Please mark to enable the DoS protection function. Manually adjust the value of packet threshold

Apply Changes and click to enact the setting. Denial of Service A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service. Enable DoS Prevention Whole System Flood: SYN Packets/Second Whole System Flood: FIN Packets/Second Whole System Flood: UDP Packets/Second Whole System Flood: ICMP Packets/Second Per-Source IP Flood: SYN Packets/Second Per-Source IP Flood: FIN Packets/Second Per-Source IP Flood: UDP Packets/Second Per-Source IP Flood: ICMP Packets/Second Low TCP/UDP PortScan Sensitivity ICMP Smurf IP Land IP Spoof IP TearDrop PingOfDeath TCP Scan TCP SynWithData UDP Bomb UDP EchoChargen Clear ALL Select ALL Enable Source IP Blocking Block time (sec) Apply Changes

3.9.6 Log

This System Log page shows the information of the current activities on the router. To enable system log function:

- 1. Mark the "Enable Log" checkbox.
- 2. To see all information of the system, select the "system all" checkbox.

To see wireless information only, select the "wireless" checkbox.

To send the log information to a certain note, select the "Enable Remote Log" checkbox and fill in the IP address in the "Log Server IP Address" box.

3.	Click the Apply Changes button to activate. You could also click the Refresh button	to
refre	sh the log information or click the Clear button to clean the log table.	
	System Log	

This page can be used to set remote log server a	nd show the system log,		
 Enable Log system all wireless Enable Remote Log 	DoS Log Server IP Address:	1 1s	
Apply Changes			
			×
Refresh Clear			

Wireless 11n Router

3.9.7 Upgrade Firmware

Sometimes a new firmware may be issued to upgrade the system of this device. You could upgrade the firmware you got in this page. To upgrade the firmware, please click on the

Browse... button, locate the firmware in your computer and then click the Upload button to execute.

Upgrade Firmwa	ire
This page allows you upgrade the the device during the upload becau	Access Point firmware to new version. Please note, do not power off se it may crash the system.
Select File:	Browse
Upload Reset	

3.9.8 Save/Reload Setting

The Save/Reload Setting page allows users to backup and download the configuration status of the device or restore the factory default configuration.

Save/Reload Se	tings	
	settings to a file or reload the setting	
previously. Besides, you could re	set the current configuration to factor	y default.
Save Settings to File:	Save	
Load Settings from File:		Browse Upload
Reset Settings to Default:	Reset	

Items	Information
Save Settings to File	Click on the Save button to save the currently configure settings.
Load Settings from File	Click Browse to select the file that you save, and then click Upload to start the process. Please wait for it to complete.
Reset Settings to Default	Click Reset to start the process and it will be completed till the status LED starts blinking.

Wireless 11n Router

3.9.9 Password

To set up the Administrator Account information, enter the Username, New password, and reenter

the password on the text box. Don't forget to click the Apply Changes to save the configuration.

Password Setu	נף
This page is used to set the ac password will disable the prot	count to access the web server of Access Point. Empty user name and tection.
User Name:	
New Password:	
Confirmed Password:	
Apply Changes R	रेक्षस

3.9.10 Logout

Click Apply Change then you will save the settings and log off the management interface.



Appendix A: Product Specifications

Standard	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
	Wireless 11n 2T2R Router:
	LAN: 4 ports 10/100 Mbps Ethernet, RJ-45
	WAN: One RJ-45 port
	2* reverse SMA detachable antennas (Standard 2 dB)
	1* reset to factory default button
	1* WPS button
Interface	Wireless 11n 1T1R Router:
	LAN: 4 ports 10/100 Mbps Ethernet, RJ-45
	WAN: One RJ-45 port
	1* reverse SMA detachable antenna (Standard 2 dBi)
	1* reset to factory default button
	1* WPS button
	Antenna type: Dipole
Antenna	Antenna connector type: Reverse SMA
WAN Connection	Ethernet 10/100 Mbps
	RJ-45 (10BASE-T): Category 3,4,5 UTP
Cable Connections	RJ-45 (100BASE-TX): Category 5 UTP
Transmission Mode	Auto-Negotiation (Full-duplex, Half-duplex)
Security	64/128-bit WEP, WPA, WPA2
	802.11b: 1,2,5.5, and 11Mbps
Network Data Rate	802.11g: 6,9,12,18,24,36,48 and 54Mbps
	802.11n: up to 150 / 300 Mbps
	802.11n Typical -68 dBm
Receiver Sensitivity	802.11g Typical -73 dBm
······	802.11b Typical -84 dBm
	16dBm typically @ 802.11b
Transmit Power	14dBm typically @ 802.11g
	13dBm typically @ 802.11n
	Wireless 11n 2T2R Router:
	1*PWR, 1*SYS, 1*WAN, 4*LAN, 1*WLAN
LED indications	
	Wireless 11n 1T1R Router:
	1*PWR, 1*SYS, 1*WAN, 4*LAN, 1*WLAN
Channel	USA 11, Europe 13, Japan 14
Bango Covorago	Indoor: 35~100 meters
Range Coverage	Outdoor: 100~300 meters
	FCC,CE CLASS B
Emission	FCC Part 15.247 for US (2.412~2.462MHz)
Emission	ETS 300 328 for Europe (2.400~2483.5MHz)
	DGT LP0002 for Taiwan (2.412~2.462MHz)
Temperature	Operating: 0°C ~ 40°C (32°~104°F); Storage: -20°C ~ 70°C (-4°~158°F)
Humidity	Operating: 10% ~ 90% RH, non-condensing
	Storage: 5%~90% RH, non-condensing
Certification	FCC, CE, VCCI Class B

Appendix B: Glossary

- 802.11b The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- 802.11g specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- 802.11n 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **DDNS** (Dynamic Domain Name System) The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- DHCP (Dynamic Host Configuration Protocol) A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server
- **DMZ** (**Dem**ilitarized **Z**one) A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- DNS (Domain Name System) An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- DoS (Denial of Service) A hacker attack designed to prevent your computer or network from operating or communicating.
- DSL (Digital Subscriber Line) A technology that allows data to be sent or received over existing traditional phone lines.
- ISP (Internet Service Provider) A company that provides access to the Internet.
- MTU (Maximum Transmission Unit) The size in bytes of the largest packet that can be transmitted.
- NAT (Network Address Translation) NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (Point to Point Protocol over Ethernet) PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- SSID A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to

communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

- WEP (Wired Equivalent Privacy) A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- WLAN (Wireless Local Area Network) A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.