



Wireless N 300 Gigabit Green Router Model # AR695W User's Manual Ver. 1A

Copyright

Copyright © Airlink101, 2010. The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC 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 radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

Table of Contents

CHAPTER 1 PRODUCT INFORMATION	1
1.1 INTRODUCTION AND SAFETY INFORMATION	1
1.2 PACKAGE CONTENTS	2
1.3 FAMILIAR WITH YOUR NEW GIGABIT ROUTER	3
CHAPTER 2 CONFIGURE THE ROUTER	5
2.1 CONNECT THE ROUTER TO YOUR NETWORK	5
2.2 CONFIGURE THE ROUTER WITH EZ SETUP WIZARD	7
2.3 CONFIGURE THE ROUTER WITH WEB CONFIGURATION UTILITY	15
2.4 Connect to Router Wirelessly	23
CHAPTER 3 ADVANCED CONFIGURATION	25
3.1 BASIC SETTING	27
3.1.1 Primary Setup	
3.1.2 DHCP Server	
3.1.3 Wireless	
3.1.4 Change Password	
3.2 Forwarding Rules	53
3.2.1 Virtual Server	53
3.2.2 Special Applications	55
3.2.3 Miscellaneous	
3.3 Security Setting	
3.3.1 Packet Filtering	
3.3.2 Domain Blocking	61
3.3.3 URL Blocking	
3.3.4 Internet Access Control	64
3.3.5 Miscellaneous	
3.4 Advanced Setting	72
3.4.1 System Time	72
3.4.2 System Log	74
3.4.3 Dynamic DNS	
3.4.4 QoS Rule	77
3.4.5 SNMP	
3.4.6 Routing	

3.4.7 Schedule Rule	83
3.5 Toolbox	85
3.5.1 View Log	86
3.5.2 Firmware Upgrade	87
3.5.3 Backup Setting	
3.5.4 Reset to Default	
3.5.5 Reboot	
3.5.6 Miscellaneous	
<u>συλρτερ / στλτυς</u>	91
CHAI 1EK 4 5 1A1 05	
4.1 System Status	
4.1 System Status 4.2 Wireless Status	
4.1 System Status 4.2 Wireless Status 4.3 Statistics Information	
4.1 System Status 4.2 Wireless Status 4.3 Statistics Information 4.4 NAT Status	
4.1 System Status 4.2 Wireless Status 4.3 Statistics Information 4.4 NAT Status CHAPTER 5 APPENDIX	92
4.1 System Status 4.2 Wireless Status 4.3 Statistics Information 4.4 NAT Status CHAPTER 5 APPENDIX 5.1 Hardware Specification	92

Chapter 1 Product Information

1.1 Introduction and safety information

Congratulations on your purchase of the Airlink101® AR695W Wireless N 300 Gigabit Green Router. This Router is recommended to be used with AirLink101® Wireless N 300 products to provide the best performance. The high bandwidth combined with extended wireless coverage delivers fast and reliable connections for all of your networking applications. The built-in gigabit switch highly increases the wired Ethernet speed.

The Green power saving technology intelligently reduces power consumption when no network activity is detected. A full range of security features such as WEP, WPA-PSK, and WPA2-PSK provide the highest level of wireless network security. The bundled EZ Setup Wizard allows you to set up the router with an easy-to-use user interface. Best of all, AR695W works with all 802.11n / g / b network devices which ensures compatibility with your existing wireless products.

Other features of this router including:

- Highest wireless data rate of up to 300Mbps* with 802.11n standard
- Built-in 4-port full-duplex 10/100/1000Mbps Switch to connect your wired network up to gigabit speeds
- Two 3dBi antennas for wider coverage and stronger signal strength to eliminate dead spots
- Advanced NAT+SPI firewall with DoS detection prevents your network from outside attacks
- Wirelessly connect to another 4 AR695W routers with WDS (Wireless Distribution System) supported
- Establish secured wireless connection via Easy Setup Button
- QoS (Quality of Service) designed for prioritizing multimedia data transmission (i.e. VoIP, online gaming or movie streaming, etc.)

1.2 Package Contents

Before you start using this router, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

- 1. Wireless N 300 Gigabit Green Router
- 2. Two Antennas
- 3. Power Adapter
- 4. Setup CD
- 5. Quick Installation Guide
- 6. Ethernet Cable

1.3 Familiar with your new Gigabit Router

A. Front Panel



LED	Status	Description	
Status	Blinking (Green)	Device status is working properly.	
On/Sloop	On (Green)	Router is on.	
On/Sieep	Off	Router is at power saving mode.	
WAN	On (Green)	Network device is connected	
	Blinking	Data access	
	On (Green)	Network device is connected	
LAN 1~4	Blinking	Data access	
	On (Green)	Wireless feature is on	
Wirolooo	Blinking	Data access	
vvireless	Blinking Rapidly	Device is in WPS PBC mode	
	Off	Wireless feature is disabled	

Button	Description
	Reset router to factory default settings or start security synchronization
Reset/WPS	function (WPS). Press this button and hold for 6 seconds to restore all
	settings to factory default. Press this button and hold no longer than 1
	second to start security synchronization.
WLAN On/Off	Switch on/off router's wireless radio.

B. Back Panel



Item Name	Description
Antennas	These antennas are detachable 3dBi dipole antennas.
ON/OFF	Switch on/off the router.
1 - 4	Local Area Network (LAN) ports 1 to 4.
WAN	Wide Area Network (WAN / Internet) port.
PWR	Power connector, connects to A/C power adapter.

Chapter 2 Configure the Router

2.1 Connect the Router to your network

Note: Prior to connecting the router, be sure to power off your computer, DSL/Cable modem, and the router.

Step 1 Connect one end of a network cable to the **WAN** port of the router and connect the other end of the cable to the DSL/Cable modem.



Step 2 Power on the modem.

Step 3 With another network cable, connect one end of the cable to your computer's **Ethernet** port and connect the other end to one of the **LAN** ports of the router. (After setup finishes, you can remove the network cable between the computer and router if you want to use wireless connection.)



Step 4 Plug the power adapter to the router and connect it to an electrical outlet. Make sure the power switch at the back is "On".



Step 5 Power on your computer.

Step 6 Check LEDs of the router: make sure **Status, WAN**, **Wireless**, and the **LAN** port that the computer is connected to are lit.

2.2 Configure the Router with EZ Setup Wizard



Step 1 Insert the Setup CD into CD-ROM drive.

Step 2 When the autorun menu pops up, click EZ Setup Wizard.



Note: If the autorun menu does not show up on your monitor, please go to **Computer** → **CDROM drive** → **Wizard**, and execute "**EZWizard.exe**".



Step 3 Select your language and click Next.

Step 4 Click on Wizard.



Step 5 Please make sure your computer is connected to the LAN port of the router, and your modem is connected to the WAN port of the router.

🞣 Airlink101 EZ Setup Wizard – AR695W	×
Prepare Setup This step will make sure connection can be established between your PC and Router	
Please make sure the following items. 1. Make sure the Router is powered on. 2. Make sure your network adapter is connected to the LAN port of the Router. 3. Make sure your network adapter has an IP address. 4. Make sure your Cable/DSL modem is connected to the WAN port of the Router.	
Help < Back Next > C	ancel

Step 6 Click Next to configure the basic wireless settings.



Step 7 Configure the SSID (wireless network name, i.e. myHome), Channel, Security and Key. It is suggested to select **WPA2-PSK** for best wireless security. Enter 8~63 characters into Key box, then click **Next**.

🚀 Airlink101 EZ Setu	p Wizard – AF	R695W
This step will se	tup your basic	wireless network settings.
Please assign the par to the Router's config	rameters to you juration page.	ur wireless networking. If you need more settings, please login
	SSID: Channel:	Airlink 101
	Security:	WPA2-PSK -
	Key:	••••••
🔲 Do not set at i	this time.	
Help		< Back Next > Cancel

Step 8 Click **Next** and the wizard will detect your WAN settings, or you can select your WAN type manually by checking "Let me select WAN service by myself".

🛃 Airlink101 EZ Setup Wizard – AR695W	x
Auto Detect WAN Service This step will automatically detect one suitable WAN service for Router	
Please make sure the WAN cable connection is working between your Router and broadband modern.	
You can set it manually if you know your WAN service type.	
Let me select WAN service by myself	
Help Cancel	

Step 9 Enter the settings based on your WAN service type.

Cable (Dynamic IP)

If you are using cable Internet service, your WAN type is "Dynamic IP". You do not need to configure anything here, then click **Next** to continue.

🞣 Airlink101 EZ Setup Wizard – AR695W
Auto Detect WAN Service This step will automatically detect one suitable WAN service for Router
A dynamic IP service has been found for your WAN. The following setup steps will be based on this setting.
If dynamic IP is not your expected WAN service, please select the correct one manually.
Let me select WAN service by myself
Help Cancel

DSL (PPPoE or Dynamic IP)

For DSL users, your WAN type is either PPPoE or Dynamic IP. You can try both types and determine which one works for you.

🞣 Airlink101 EZ Setup Wizard – AR	695W	
WAN Setting PPPoE Service		
Please input the WAN service infom	nation.	
User:	user@sbcglobal.net	
Password:	•••••	
Service:	AT&T	(Optional):
Help	< Back	Next > Cancel

For PPPoE settings, please enter the username and password provided by your ISP (Internet Service Provider).

Note: Depending on the ISP, you may need to include the domain name with your username.

Example: username@sbcglobal.net

Step 10 Verify the settings you have configured. Click **Next** to save the settings and reboot the router. This will take about 30 seconds.

💁 Airlink1	01 EZ Setup Wizard – AR695W	— ×-
Save S	ettings	
The settir	gs will be saved to the Router and reboot at the next step. Wireless Setting SSID:Airlink 101	
	Channel:11 Security:WPA2-PSK WAN Setting (Dynamic IP Service)	
		Modify Settings
Help	< Back	Next > Cancel

Step 11 Click **Next** to test the Internet Connection, or you can ignore the test, just open the Internet browser and verify if you are connected to the Internet.

🞣 Airlink101 EZ Setup Wizard – AR695W 🧮
WAN Service Test
This step will test the internet connection to make sure you can surf the internet.
Ignore Test
Help Cancel

If you cannot connect to the Internet, please go to Section 4, Troubleshooting.

Step 12 After the WAN service test completed, click **Finish**. The wizard will open the web configuration page for the router automatically unless you uncheck the checkbox below "Open the default web browser to access the advanced configuration".

🞣 Airlink101 EZ Setup Wizard – AR695W	×
Setup Completed	
The Router's configuration is complete, and the WAN service is functioning property.	
Open the default web browser to access the advanced configurations.	
Finish	

You will see the status of the router on the web configuration page brought up by the web browser. Valid numbers should be assigned to IP Address, Subnet Mask and Gateway, instead of all 0's.

🥖 AR695W - A	Airlink101 Wireless I	N 300 Gigabit Router - W	indows Internet Exp	lorer								×
	🤌 http:// 192.168 .2	2.1/				- ₹	🗟 😽 🗙	Google 🚼				ب م
🚖 Favorites	88 - 📢 MSN	l.com	🏉 AR695W - Airl	nk101 Wi 🗆	×		👌 🔻	N • E	• • <u>P</u> age •	<u>S</u> afety	▼ Tools ▼	•9
			AR695	W Wire	less N 300 (Əigabit R	Router		Englis	h 🕶		
	D ADMINISTR	ATOR'S MAIN MENU	-1 Sta	tus	Wizard	MI Adva	nced		→ Lo	gout		
	System	Status							[HELP	1		
		Item			WAN Status			Sidenote				
		Remaining Lease Time	9		999:58:46			Renew]			
		IP Address			192.168.20.121			Release				Ξ
		Subnet Mask			255.255.255.0							
		Gateway			192.168.20.1							
		Domain Name Server		206.1	3.28.12, 206.13.31	.12						
		MAC Address		00	0-50-18-21-D4-38							
	Wireles	s Status										
		Item			WLAN Status			Sidenote				
		Wireless mode			Enable							
		SSID			Airlink101							
		Channel			11							
		Security			WPA2-PSK			(AES)				
		MAC Address		00	0-50-18-21-D4-39							
	Statistic	cs Information										-
1						😜 Inter	net Protec	ted Mode: On		- (h)	100% 🔍	•

2.3 Configure the Router with Web Configuration Utility

Another approach to configure the router is using the Wizard in the Web Configuration Utility. The wizard will guide you setting up the basic settings of this router. You do not need to go through the wizard again if you have finished *2.2 Configure the Router with EZ Setup Wizard*.

In order to enter the Web Configuration Utility, you need to first log in to the router from your web browser. Please follow the steps below:

Step 1 Go to the computer connected to the router, open the web browser (i.e. Internet Explorer or Mozilla Firefox) and type **192.168.2.1** or the IP address you assigned to this router in the address bar and press **Enter**.



Step 2 Enter the system password and click Login. (The default password is "admin".)



Step 3 When you see this page coming up, you have successfully logged in to the router. Select **Wizard** and click on **Enter** to start the setup wizard.

	NK:	AR695W	Wireless N 300 Gigabit Router	English 💌
ADMIN	ISTRATOR'S MAIN MENU	🚽 Status		▶ Logout
	Please Select the Operation	ons		
			 Wizard 	
			Advanced Setup	
	* T	his screen remind	s you to configure until the Wizard is finished.	
-		Do no	t display this screen after login	
			Enter	

Step 4 Click Next to start the Setup Wizard.

Setup Wizard	[EXIT]
Setup Wizard will guide you through a basic configuration procedure step by step.	
Step 1. Setup Login Password.	
► Step 2. WAN Setup.	
Step 3. Wireless Setup.	
Step 4. Summary.	
Step 5. Finish.	
<pre><back <u="" [="">Start > Password > WAN > Wireless > Summary > Finish!]</back></pre>	Next >

Step 5 Change System Password. Enter the current password, new password and reconfirm the new password. (The default password is 'admin'.) If you do not wish to change the password, please leave all fields blank. Click **Next**.

Setup Wizard - Setup Login Passw	vord		[EXIT]
	 Old Password New Password Reconfirm 		
< Back [S	tart > <u>Password</u> > WAN >	• Wireless > Summary > Finish!]	Next >

Step 6 Select Auto Detecting WAN Type to let the wizard detect which Internet connection you use or select Setup WAN Type Manually to select the Internet connection type manually. Click **Next**.



If you select Setup WAN Type Manually, please specify a WAN type you are using.

For Cable Users:

Please select Obtain an IP address from ISP automatically (Dynamic IP Address).



For DSL Users:

You may select either Obtain an IP address from ISP automatically (Dynamic IP

Address) or Some ISPs require the use of PPPoE to connect to their services (PPP over Ethernet) depending on the type of modem provided by your ISP (Internet Service Provider). You can try both settings and determine which one works for you.

Setup Wizard - Select WAN Type	[EXIT]
 ISP assigns you a static IP address. (Static IP Address) 	
Obtain an IP address from ISP automatically. (Dynamic IP Address)	
O Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)	
Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)	
 Some ISPs require the use of PPTP to connect to their services. (PPTP) 	
 Some ISPs require the use of L2TP to connect to their services. (L2TP) 	
<pre><back [="" start=""> Password > WAN > Wireless > Summary > Finish!]</back></pre>	Next >

Click Next.

Step 7 Configure the WAN settings according to the WAN type you selected.

Dynamic IP Address: Click on Clone MAC.

Setup Wizard - WAN Setting	js - Dynamic IP Address	[EXIT]
LAN IP Address	192.168.2.1	
Host Name	GigaRouter (optional)	
WAN's MAC Address	00-50-18-21-D4-38 Clone MAC	
< Back	[Start > Password > <u>WAN</u> > Wireless > Summary > Finish!]	Next >

tup Wizard - WAN Settings - PPP o	ver Ethernet		[EXI
LAN IP Address	192.168.2.1		
Account	user1@sbcg	lobal.net	
Password	•••••		
Primary DNS	0.0.0.0		
Secondary DNS	0.0.0.0		
PPPoE Service Name		(optional)	
Assigned IP Address	0.0.0.0	(optional)	
- Deals	t > Decoword > WA	N > Wireless > Summary > Finish11	Novta

PPP over Ethernet: Enter the Account and Password provided by your ISP.

Note: Depending on the ISP, you may need to include the domain name with your username.

Example: username@sbcglobal.net

Step 8 Keep the default SSID (wireless network name) or change it to a desired name, so you can always recognize your wireless network with it, for example 'myHome'. Select a channel number for your wireless network. Click **Next**.

Setup Wizard - Wireless set	tings	[EXIT]
 Wireless function 	⊙ Enable ◯ Disable	
Network ID(SSID)	Airlink101	
Channel	11 💌	
< Back	[Start > Password > WAN > <u>Wireless</u> > Summ	ary > Finish!] Next >

Step 9 Set up Wireless Security for your router. It is recommended to select **WPA2-PSK (AES)** for security to protect your wireless network from unauthorized users.

Setup Wizard - Wire	less Security	[EXIT]
► Security	None None WPA2-PSK (AES)	
< Back	[Start > Password > WAN > <u>Wireless</u> > Summary > Finish!]	Next >

Type in 8~63 characters into **Preshare Key**. Click **Next**.

Setup Wizard - Wireless Security	[EXIT]
 Security Preshare Key Mode Preshare Key 	WPA2-PSK (AES) ASCII Please input either 8 to 63 ASCII characters or 64 Hexadecimal digits as Pre-share key. Hexadecimal(0, 1, 28, 9, A, BF)
< Back [Start > Pa	ssword > WAN > <u>Wireless</u> > Summary > Finish!] Next >

WPA2-PSK (AES) is the most secured encryption mode for general users but some older wireless adapters might not support it. Therefore, please make sure all wireless devices on your network support this security type.

Step 10 Verify the information you have configured. If everything is correct, click **Apply Settings** to save the settings and reboot router.

Please confirm	n the information below.	
[WAN Setting]		
WAN Type	Dynamic IP Address	
Host Name	GigaRouter	
WAN's MAC Address	00-50-18-21-D4-38	
[Wireless Setting]		
Wireless	Enable	
SSID	Airlink101	
Channel	11	
Security	WPA-Personal / WPA2-Personal	
🗹 Do you want :	to proceed the network testing?	

Step 11 When you see window like below, you are successfully connected to the Internet. Click **Finish**.

Setup Wizard - WAN Connection Te	est			[EXIT]
	Congra The Internet con	atulations!! nection is established.		
	Connectio	on information is		
	WAN Type	Dynamic IP Address		
	IP Address	192.168.20.121		
	Subnet Mask	255.255.255.0		
	Gateway	192.168.20.1		
	Domain Name Server	206.13.28.12, 206.13.31.12		
			-	
< Back [St	art > Password > WAN >	• Wireless > Summary > <u>Fi</u>	nish!]	Finish

Congratulations! Your router configuration has been finished. Please go to 2.4 Connect to the Router Wirelessly.

2.4 Connect to Router Wirelessly

You must configure your wireless computer in order to establish a wireless connection to the router. In this section, you can find the instructions of how to connect to the router wirelessly with your **Windows 7** computer. You can also refer to the manual of your wireless device on how to connect to the router.

Step 1 Click on the wireless icon in the system tray on your desktop. A list of available network will pop up. Select the one you want to connect to and click **Connect**.

Not connected	÷7
Connections are available	
Wireless Network Connection 6	^
airlink101	lle.
	nect
trigger	.ull
Fossa	.11
SCA	.11
Other Network	.all
Open Network and Sharing Cente	er
▲ R = 10 3:0! → R = 10 7/2	5 PM /2009

Step 2 Enter the key you configured for the router if you have enabled the wireless security, then click **OK**. The wireless connection should be now established.

💋 Connect to a Network	×
Type the network security key	
Security key:	
Hide characters	
You can also connect by pushing the button on the router.	
ОК	Cancel

Chapter 3 Advanced Configuration

You can make advanced configurations on this router through Web Configuration Utility to meet your network's needs, such as: Virtual Server, Access Control, Network Security, etc. If you have already gone through the Setup Wizard, you do NOT need to configure anything here for you to start using the Internet.

In order to enter the Web Configuration Utility of your router, you need to first log in to the router from your web browser. Please follow the steps below:

Step 1 Go to the computer connected to the router, open the web browser (i.e. Internet Explorer or Mozilla Firefox) and type **192.168.2.1** or the IP address you assigned to this router in the address bar and press **Enter**.

p!	Tools	Help	
	۵ (192.168.2.1	
Home			

Step 2 Enter the system password and click Login. (The default password is "admin".)

	AR695W Wireless N 300 Gigabit Router	
USER'S MAIN MENU	- Status	_
	System Password : ••••• (default:admin) Login	

Step 3 When you see this page coming up, you have successfully logged in to the router. Select **Advanced Setup** and click **Enter** to access the complete features/settings of this router.

INK :	AR695W	Wireless N 300 Gigabit Router	English 💌
IISTRATOR'S MAIN MENU	🚽 Status		► Logout
Please Select the Operation	ons		
		Wizard	
		O Advanced Setup	
*	This screen reminds	s you to configure until the Wizard is finished. t display this screen after login	
	20110	Enter	

3.1 Basic Setting

You can configure LAN, Internet connection type, DHCP, wireless settings and system password for the router in this page.



3.1.1 Primary Setup

This page allows you to specify an IP address for your router, and configure the Internet connection settings.

Primary Setup [HEL]	
Item	Setting
LAN IP Address	192.168.2.1
• WAN Type	Dynamic IP Address Change
Host Name	GigaRouter (optional)
WAN's MAC Address	00-50-18-21-D4-38 Clone MAC
Renew IP Forever	Enable (Auto-reconnect)
▶ IGMP	Enable
	Save Undo Virtual Computers

Parameter	Description
LAN IP Address	The local IP address of this router. You can change it if necessary.
WAN Type	Displaying the current WAN (Wide Area Network , i.e. Internet) connection type you configured for the router. Click " Change " to modify. Please see Section 3.1.1.1. If you are not sure which WAN type you are using, please contact your ISP.
IGMP	The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.
Virtual Computers	Please find detailed instructions in Section 3.1.1.2.

3.1.1.1 WAN Type

If you need to change router's WAN type, please click **Change** in the Primary Setup menu. You will see the following page.

	Туре	Usage
۲	Static IP Address	ISP assigns you a static IP address.
0	Dynamic IP Address	Obtain an IP address from ISP automatically.
0	Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)	
0	PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services
0	PPTP	Some ISPs require the use of PPTP to connect to their services.
0	L2TP	Some ISPs require the use of L2TP to connect to their services.

Select a WAN type from the list and click **Save**.

- A. Static IP Address: Click on Static IP Address if your ISP (Internet Service Provider) has provided you a set of IP addresses for your Internet connection.
- B. Dynamic IP Address: Click on Dynamic IP if you are connecting to Internet through a cable modem.
- C. Dynamic IP Address with Road Runner Session Management: This setting only works when you are using Telstra Big Pond's network service in Australia.
- D. PPP over Ethernet (PPPoE): Click on PPP over Ethernet if you are connecting to Internet through a DSL modem.

Note: For DSL users, your WAN type is either **Dynamic IP Address** or **PPP over Ethernet**. If you are not sure which one you use, it is suggested to select PPP over Ethernet for your WAN type, and if you cannot connect to the Internet with this setting, try to select Dynamic IP instead. Otherwise, you can call your ISP to confirm which WAN type you are using.

- E. PPTP: Some ISPs require the use of PPTP to connect to their services.
- F. L2TP: Some ISPs require the use of L2TP to connect to their services

Please see the following instructions for settings of each WAN type:

A) Static IP Address

Enter the WAN IP address, WAN Subnet Mask, WAN Gateway, Primary DNS, and Secondary DNS addresses provided by your ISP.

Primary Setup [HELP	
Setting	
192.168.2.1	
Static IP Address Change	
0.0.0.0	
255.255.255.0	
0.0.0.0	
0.0.0.0	
0.0.0.0	
Enable	

After you finished all settings, click **Save** to save the settings and click **Reboot**. The change will take effect after rebooting the router.

Save Undo Virtual Computers... Reboot

Saved! The change doesn't take effect until router is rebooted.

B) Dynamic IP Address

Primary Setup	[HELP]
Item	Setting
LAN IP Address	192.168.2.1
• WAN Type	Dynamic IP Address Change
Host Name	GigaRouter (optional)
WAN's MAC Address	00-50-18-21-D4-38 Clone MAC
Renew IP Forever	Enable (Auto-reconnect)
▶ IGMP	Enable
	Save Undo Virtual Computers

Parameter	Description
Host Name	Please input the host name of your router; this is optional and only required if your service provider asks you to do so.
WAN's MAC Address	Please input MAC address of your computer here if your ISP only permits computer with certain MAC address to access Internet. If you are using the computer which used to connect to Internet via cable modem, you can simply press ' Clone MAC ' button to fill the WAN's MAC address field with the MAC address of your computer.
Renew IP Forever	Check Enable to let router reconnect to your ISP when the connection is dropped.

After you finished all settings, click **Save** to save the settings and click **Reboot**. The change will take effect after rebooting the router.



C) Dynamic IP Address with Road Runner Session Management:

Item	Setting
LAN IP Address	192.168.2.1
WAN Type	Dynamic IP Address Change
Account	
Password	
Login Server	(optional)
Renew IP Forever	Enable (Auto-reconnect)
IGMP	Enable

Please enter the account and password provided by your Telstra Big Pond ISP.

Parameter	Description
Account	Please input user name of your account assigned by Telstra.
Password	Please input the password assigned by Telstra.
Login Server	Please input the IP address of login server here. (Optional)

After you finished all settings, click **Save** to save the settings and click **Reboot**. The change will take effect after rebooting the router.



Saved! The change doesn't take effect until router is rebooted.
D) PPP Over Ethernet (PPPoE)

Primary Setup	[HELP]
Item	Setting
LAN IP Address	192.168.2.1
WAN Type	PPP over Ethernet Change
PPPoE Account	user1@sbcglobal.net
PPPoE Password	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Maximum Idle Time	300 seconds
Connection Control	Auto reconnect(Always-on)
PPPoE Service Name	(optional)
Assigned IP Address	0.0.0.0 (optional)
MTU	1492
IGMP	Enable
	Save Undo

Parameter	Description
PPPoE Account	Enter the User Name for your DSL account, you can obtain this information from your ISP.
PPPoE Password	Enter the Password for your DSL account, you can obtain this information from your ISP.
Primary DNS	This feature allows you to assign a Primary DNS Server. You can obtain this information from your ISP. If your ISP does not provide this information, you can leave it blank.
Secondary DNS	This feature allows you to assign a Secondary DNS Server. You can obtain this information from your ISP. If your ISP does not provide this information, you can leave it blank.
Maximum Idle Time	The amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.
Connection Control	There are 3 modes for you to control the Internet connection: Connect-on-demand: Router will connect to the ISP when its client send outgoing packets. Auto Reconnect (Always-on): Router will keep the connection

	to the ISP after the connection is established. Manually: Router will not connect to the ISP until user clicks the Connect button on the Status-page.
PPPoE Service Name	Enter the DSL service company. This is optional.
Assigned IP Address	Input the IP address you wish to use. This is optional.
MTU (Maximum Transmission Unit)	The most common MTU value is 1492. You can configure it as your ISP suggested.

After you finished all settings, click **Save** to save the settings and click **Reboot**. The change will take effect after rebooting the router.



Saved! The change doesn't take effect until router is rebooted.

<u>E) PPTP</u>

Item	Setting
LAN IP Address	192.168.2.1
WAN Type	PPTP Change
P Mode	Dynamic IP Address 🗸
My IP Address	0.0.0.0
My Subnet Mask	0.0.0.0
Gateway IP	0.0.0.0
Server IP Address/Name	
PPTP Account	
PPTP Password	
Connection ID	(optional)
Maximum Idle Time	300 seconds
Connection Control	Auto reconnect(Always-on) 💌
MTU	1460
IGMP	Enable

Parameter	Description
IP Mode	Select the type of how you obtain IP address from your service provider here: Static IP Address or Dynamic IP Address.
My IP Address	Enter the IP address assigned by your ISP if you select Static IP Address.
My Subnet Mask	Enter the Subnet Mask assigned by your ISP if you select Static IP Address.
Gateway IP	Enter the Gateway IP address assigned by your ISP if you select Static IP Address.
Server IP Address/Name	Enter the IP address of the PPTP server.
PPTP Account	Enter the User Name for your PPTP account here. You can obtain this information from your ISP.
PPTP Password	Enter the password for your PPTP account here. You can obtain this information from your ISP.
Connection ID	Enter the connection ID if your ISP requires it. This is optional.
Maximum Idle Time	The amount of time of inactivity before disconnecting your PPTP session. Set it to zero or enable "Auto-reconnect" to disable this feature.
Connection Control	There are 3 modes for you to control the Internet connection: Connect-on-demand: Router will connect to the ISP when its client send outgoing packets. Auto Reconnect (Always-on): Router will keep the connection to the ISP after the connection is established. Manually: Router will not connect to the ISP until user clicks the Connect button on the Status-page.
Maximum Transmission Unit (MTU)	Most ISPs offer MTU value to users. The default MTU value is 0 (auto).

<u>E) L2TP</u>

Primary Setup	[HELP]
Item	Setting
LAN IP Address	192.168.2.1
WAN Type	L2TP Change
▶ IP Mode	Static IP Address
IP Address	0.0.0.0
Subnet Mask	255.255.255.0
WAN Gateway IP	0.0.0.0
Server IP Address/Name	
L2TP Account	
L2TP Password	
Maximum Idle Time	300 seconds
Connection Control	Auto reconnect(Always-on)
MTU	1460
▶ IGMP	Enable
Saved! The cl	Save Undo Reboot nange doesn't take effect until router is rebooted.

Parameter	Description
IP Mode	Select the type of how you obtain IP address from your service provider here: Static IP Address or Dynamic IP Address.
My IP Address	Enter the IP address assigned by your ISP if you select Static IP Address.
My Subnet Mask	Enter the Subnet Mask assigned by your ISP if you select Static IP Address.
Gateway IP	Enter the Gateway IP address assigned by your ISP if you select Static IP Address.
Server IP Address/Name	Enter the IP address of the L2TP server.
L2TP Account	Enter the User Name for your L2TP account here. You can obtain this information from your ISP.
L2TP Password	Enter the password for your L2TP account here. You can obtain this information from your ISP.
Maximum Idle Time	The amount of time of inactivity before disconnecting your L2TP

	session. Set it to zero or enable "Auto-reconnect" to disable this feature.
Connection Control	There are 3 modes for you to control the Internet connection: Connect-on-demand: Router will connect to the ISP when its client sends outgoing packets. Auto Reconnect (Always-on): Router will keep the connection to the ISP after the connection is established. Manually: Router will not connect to the ISP until user clicks the Connect button on the Status-page.
Maximum Transmission Unit (MTU)	Most ISPs offer MTU value to users. The default MTU value is 0 (auto).

3.1.1.2 Virtual Computers

Virtual Computer enables you to use the original NAT feature, and allows you to set up the one-to-one mapping of multiple global IP addresses and local IP addresses.

	DHCP clients Select one	Copy to ID	🔽
ID	Global IP	Local IP	Enable
1		192.168.2.	
2		192.168.2.	
3		192.168.2.	
4		192.168.2.	
5		192.168.2.	

Parameter	Description
Global IP	Enter the global IP address assigned by your ISP.
Local IP	Enter the local IP address (virtual IP address) of your LAN computer corresponding to the global IP address.
Enable	Check Enable box to enable the Virtual Computer mapping rule.

3.1.2 DHCP Server

This page allows you to configure the DHCP settings for your router.

DHCP Server	[HELP]
Item	Setting
DHCP Server	O Disable I Enable
▶ Lease Time	0 Minutes
IP Pool Starting Address	100
IP Pool Ending Address	199
Domain Name	
Save	e Undo More>> Clients List
 Primary DNS 	0.0.0.0
Secondary DNS	0.0.0.0
Primary WINS	0.0.0.0
 Secondary WINS 	0.0.0.0
▶ Gateway	0.0.0.0 (optional)
	Save Undo Clients List

Parameter	Description
DHCP Server	Select Disable or Enable the DHCP server.
Lease Time	DHCP lease time to the DHCP client. Please enter a number between 5 to 10080. 10080 Minutes = 7 days.
IP Pool Starting/Ending Address	Whenever there is a request from a network client, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify a range by entering the starting / ending address of the IP address pool.
Domain Name	This is optional, this information will be passed to the client.
Press "More>>" for more options	

Primary DNS/Secondary DNS	This is optional. This feature allows you to assign a Primary / Secondary DNS Server.
Primary WINS/Secondary WINS	This is optional. This feature allows you to assign a WINS Server.
Gateway	This is optional. Gateway address can be the IP address of an alternate Router.
Client List	Click on Client List to view DHCP clients.

Click **Save** to save the settings you made.

3.1.3 Wireless

You can set parameters that are used for wireless clients to connect to this router. The parameters include SSID, Channel Number, Encryption etc.

[HELP
Setting
● Enable ○ Disable
(00)Always 💌 O Enable O Disable Schedule Setting
Airlink101
● 11b/g/n mixed ○ 11g only ○ 11b only ○ 11n only
● Enable ○ Disable
11 💌
Enter
Enter
None

Parameters	Default	Description
Wireless	Enable	Enable or disable wireless function.
Wireless On/Off by Time schedule	Disable	Select a pre-defined schedule rule from the drop-down menu (click on Schedule Setting to add a new rule) and select Enable, then the router will turn on/off wireless function according to the schedule rule. Click on Disable to disable this feature if you want to keep wireless function always on.
Schedule Setting		Please refer to Section 3.4.7, Schedule Rule.
Network ID (SSID)	Airlink101	This is the name of your wireless network. You can type any alphanumeric characters here, maximum 32 characters. SSID is used to identify your own wireless router from others when there are multiple wireless

		routers in the same area. It's recommended to change default SSID value to the one which is meaningful to you, like myhome, office_room1, etc.
Wireless Mode	11b/g/n mixed	Please select the wireless mode from one of the following options:
		11b/g/n mixed: 2.4GHz band, allows 802.11b, 802.11g, and 802.11n wireless network clients to connect to this router (maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 300Mbps for 802.11n clients*).
		11g Only: 2.4GHz band, only allows 802.11g wireless network clients to connect to this router (maximum transfer rate 54Mbps*).
		11b Only: 2.4GHz band, only allows 802.11b wireless network clients to connect to this router (maximum transfer rate 11Mbps*).
		11n Only: 2.4GHz band, only allows 802.11n wireless network clients to connect to this router (maximum transfer rate 300Mbps*).
SSID Broadcast	Enable	Select Enable to broadcast the SSID so that your wireless client can detect it on the available wireless network list.
Channel	11	Please select a channel from the drop-down list of 'Channel Number' for broadcasting. You can choose any channel number you want to use.
WDS		Please see 3.1.3.1 for WDS settings.
WPS		Please see 3.1.3.2 for WPS settings.
Security		You can choose None, WEP, 802.1x and RADIUS, WPA-PSK, WPA2-PSK, WPA, WPA2 for encryption mode. The detailed settings will appear after you choose an encryption. Please see below instructions for each Security type for more details.
Wireless Client List		Please see 3.1.3.3 for Wireless Client List information.

Configuring Security - WEP

Note: IEEE802.11n only supports WPA2-PSK or WPA-PSK AES encryption. If you use WEP as your encryption, wireless data rate will drop to 54Mbps (802.11g standard).

▶ Security	WEP 🔽
▶ Key Mode	HEX M
▶ WEP	
▶ Key 1	
▶ Key 2	0
▶ Key 3	0
▶ Key 4	0
Save Undo Wireless Client List	

Key Mode: Select HEX or ASCII. You can select ASCII (alphanumeric format) or Hexadecimal (in the "a~f" and "0~9" range) for the key format.
 WEP: Select 64 bits or 128 bits key length.

Key 1~4: Select a WEP Key you wish to use and enter key value.

If you select HEX and 64 bits, enter a 10-digit Hex key, for example, "12345abcde".

If you select ASCII and 64 bits, enter a 5-digit ASCII key, for example, "xyz01".

If you select HEX and 128 bits, enter a 26-digit Hex key, for example, "12345abcde67890bcdef123456".

If you select ASCII and 128 bits, enter a 13-digit ASCII key, for example, "wepkeyexample".

Configuring Security - WPA-PSK / WPA2-PSK

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key (PSK) to authenticate wireless stations and encrypt data during

communication, so the encryption key is not easy to be broken by hackers. This can greatly improve your wireless security.WPA2-PSK AES is the most secured setting for general users.

▶ Security	WPA2-PSK	
Encryption	O TKIP ⊙ AES	
Preshare Key Mode	ASCII 🕶	
 Preshare Key 		
Save Undo Wireless Client List		

Security:	Select WPA-PSK or WPA2-PSK
Encryption:	Select either AES or TKIP. It is suggested to select AES if all your
	wireless computers / devices support this encryption mode.
	Note: IEEE802.11n only supports AES encryption. If you use TKIP as your
Preshare Key:	<i>encryption, wireless data rate will drop to 54Mbps (802.11g standard).</i> Enter 8~63 characters as the security key of your wireless network.
	5 5 5

Configuring Security – 802.1x and RADIUS

When the 802.1x function is enabled, wireless users must authenticate to this router first to use the network service. The most common method of implementing 802.1x is by having a RADIUS Server (contain an authentication database) on your LAN, so the router can work simultaneously with it and get user's authentication profile for comparison.

▶ Security	802.1x and RADIUS	
Encryption Key Length	€4 bits □ 128 bits	
RADIUS Server IP	0.0.0.0	
RADIUS port	1812	
RADIUS Shared Key		
Save Undo Wireless Client List Reboot Saved! The change doesn't take effect until router is rebooted.		

Encryption Key Length: You can select either 64 bits or 128 bits.

RADIUS Server IP: The RADIUS server's IP address.

RADIUS port: The RADIUS server's service port.

RADIUS Shared Key: Key value shared by the RADIUS server and this router. This key value should be consistent with the one in the RADIUS server.

Configuring Security - WPA / WPA2

Wi-Fi protected Access (WPA) is designed to improve data protection and implement access control for Wireless LAN system. It encrypts frames transmitted through wireless module using the key dynamically obtained from RADIUS Server.

▶ Security	WPA2
Encryption	O TKIP @ AES
RADIUS Server IP	0.0.0.0
RADIUS port	1812
RADIUS Shared Key	
Save Undo Wireless Client List	

Encryption: Select either AES or TKIP. It is suggested to select AES if all your wireless computers / devices support this encryption mode.

RADIUS Server IP: The RADIUS server's IP address.

RADIUS port: The RADIUS server's service port.

RADIUS Shared Key: Key value shared by the RADIUS server and this router. This key value should be consistent with the one in the RADIUS server.

After you finished all settings, click **Save** to save the settings and click **Reboot**. The change will take effect after rebooting the router.

Save	Undo	Wireless Client List	Reboot

Saved! The change doesn't take effect until router is rebooted.

3.1.3.1 WDS

The Wireless Distribution System (WDS) provides wireless point-to-point, and point-to-multipoint bridging for deployment over large area. With the WDS feature, the Wireless LAN coverage can be easily extended.

Note: WDS-enabled routers or APs from different manufacturers are not guarantee to work with AR695W. It is recommended to deploy WDS with solely Airlink101 AR695W.

	[HELP]	
	Setting	
Hybrid 💌		
00-21-2F-37-4A-AA		
Scaned AP's MAC Select one Copy to Remote AP MAC V		
Channel	MAC Address	
1	00-03-7F-BE-F0-88	
6	00-11-A3-0A-95-96	
6	00-1D-6A-BE-26-1B	
Save Undo Scan AP Back Reboot Saved! The change doesn't take effect until router is rebooted.		
	Hybrid 00-21-2F-37-4A-AA 00-21-2F-37-4A-AA Channel Channel 1 6 6 ve Undo Scan AP e change doesn't take effe	

Before you set up WDS bridging:

- 1) Make sure your wireless computer can associate with individual router/AP.
- 2) Configure the same channel for every router/AP.
- 3) Configure a unique different SSID for every router/AP in order to distinguish each unit on your wireless LAN.
- 4) Configure a static IP address for every router/AP. Make sure all IP addresses are based on the same subnet mask, and out of your DCHP client range.

Parameters	Description
AP Mode	AP Only: WDS function is disabled. WDS Only: The router is functioning as a bridge to connect with other WDS enabled AP/Router. Wireless client is not able to connect to the router at WDS Only mode. Hybrid: The router is functioning as a bridge as well as an AP that allows wireless client association at the same time. (Note: the data throughput is halved with Hybrid mode.)
Remote AP MAC	Enter the MAC address of other WDS enabled AP/Router into MAC 1 ~ MAC4. This feature allows you to bridge up to 4 AR695W routers. It is suggested to use "Copy to" function to avoid any typo.
Scanned AP's MAC	Click on the drop-down menu to select a AP you wish to bridge to, select a number from the drop-down menu of Remote AP MAC and click Copy to , the MAC address will be automatically filled into the corresponding MAC address field above.
Scan AP	Click Scan AP to find the available wireless Router/AP that you wish to bridge. If the wireless router/AP is not showing in the list, it may be out of range, and you need to move it closer in order to build the bridge connection.

After you finished all settings, click **Save** to save the settings and click **Reboot**. The change will take effect after rebooting the router.



Saved! The change doesn't take effect until router is rebooted.

3.1.3.2 WPS (Easy Setup Button)

The AR695W Wireless N 300 Gigabit Green Router has a built-in Easy Setup Button (WPS) which allows you to build secured wireless connection between your wireless computers and the router quickly and easily. **Please make sure your wireless device support this feature as well.** If not, you will need to set up the wireless security manually and you can skip this section.

In the instructions below, we are going to use the AWLL6077v2 Airlink101 Wireless N 300 USB Adapter as an example.

Note: You may have different wireless adapter installed in your computer, you can refer to the user's manual from the manufacturer. Different adapters have different ways to trigger WPS configuration.

Step 1 Go to the computer with Airlink101 Wireless N 300 USB adapter, AWLL6077v2 installed.

Step 2 Push and hold the Easy Setup Button on the Adapter until you see the following window pops up on the screen.





Step 3 Within the following 2 minutes, push the WPS Button on the Router and hold for 1 second. The wireless LED will start blinking quickly.



Step 4 The Router will now start the handshake with the wireless adapter which will take about 30 seconds. When you see the window similar to the one below, the connection has been established.

About(A) General Profile Availab	Nonitor	Status	Statistics	Wi-Fi Protect Setu	4
Status: Speed: Type: Encryption: SSID: Signal Strength: Link Quality: Network Address:	Associated Tx:150 Mb Infrastruct AES Airlink MAC Addre IP Addre Subnet Ma Gatewa	nps Rx:3 mps Rx:3 mss: 00 mss: 19 mssk: 25 may: 19 ReNew	:E0:4C:01 2.168.1.1 5.255.255 2.168.1.1 w IP	:04:11 02 5.0	86%
Show Tray Icon				🔲 Disable Ada	apter
Ready					NUM

To configure the WPS settings of the router, go to **Advanced > Basic Setting > Wireless**, then click on **WPS** button.

There are two methods to activate WPS – PIN and PBC.

1) PIN (Persona	I Identification	Number)
-----------------	------------------	---------

Wi-Fi Protected Setup		
Item	Setting	
▶ WPS	Inable O Disable	
▶ Setup	Current AP PIN Configure Wireless Station	
Current PIN of the device	18583199 Generate New PIN	
 WPS state 	Idle	
▶ WPS status	Configured Release	

You can choose to enter the numbers generated by this router displaying in "Current PIN of the device" to the wireless client computer, or

Wi-Fi Protected Setup		
Item	Setting	
• WPS	Inable O Disable	
▶ Setup	Current AP PIN Onfigure Wireless Station	
Method	 Enrollee PIN : 00000000 Software button 	
 WPS state 	Idle	
▶ WPS status	Configured Release	
Save Trigger Back		

enter the PIN generated by the wireless client computer into **Enrollee PIN**, and click **Trigger** button to start WPS.

2) PBC (Push Button Configuration)

You can choose to press the hardware button on the front panel of the router, or select Configure Wireless Station, Software button, and click **Trigger** button to start WPS.

Wi-Fi Protected Setup		
ltem	Setting	
• WPS		
▶ Setup	Current AP PIN Configure Wireless Station	
Method	Enrollee PIN : 00000000 Software button	
 WPS state 	Idle	
 WPS status 	Unconfigured	
Save Trigger Back		

Parameters

Description

WPS

Select Enable or Disable WPS function.

WPS State	It displays "Idle" when there is no WPS session going on, "Processing" when WPS is in progress, or "Complete" when WPS is finished.
WPS Status	It displays "Configured" if WPS setup is successful, or "Unconfigured" if WPS setup fails.

Click **Save** after you finished all settings.

3.1.3.3 Wireless Client List

This table displays the wireless clients that are currently associated to the router. You can click **Back** to go back to the Wireless page, or click **Refresh** to refresh the list.

Wireless Client List				
Connected Time1	MAC Address			
Mon Jun 01 00:00:00 2009	00-15-00-36-87-5E			
Back Refresh				

3.1.4 Change Password

You can change the password required to log in to the Router's web configuration utility. The default password is "admin". It is suggested to change the administrator's default password as soon as you start to use the Router, and store it in a safe place. The password consists of 0 to 9 alphanumeric characters, and is case sensitive

Item	Setting	
Old Password		
New Password		
Reconfirm		

Parameters	Description
Old Password	Enter the current password of the router.
New Password	Enter the new password.
Reconfirm	Enter the new password again for verification purposes.
	Note : If you forget your password, you'll have to reset the router to the factory default (the default password is 'admin') by pushing and holding the WLAN/Reset button on the front panel of the router for 6 seconds.

Click **Save** after you finished all settings.

3.2 Forwarding Rules

3.2.1 Virtual Server

If you want to host a HTTP/FTP server or allow remote access to your IP camera on the LAN from the Internet, you must set up port forwarding rules on the router in order to direct incoming traffic to the server or IP Camera. This page allows you to set up to 20 port forwarding rules for the specified applications.

Virtual Server	🗆 Virtu	al Server				[HELP
Special AP		Well known Schedule	services select one rule (00)Always 💌 🕻	Copy to ID	~	
macchaneous	ID	Server IP	Service Ports	Protocol	Enable	Schedule Rule#
	1	192.168.3.50	21	Both 💌		1
	2	192.168.3.51	80	Both 🔽		0
	3	192.168.3.		Both 💌		0
	4	192.168.3.		Both 💌		0
	5	192.168.3.		Both 💌		0
	6	192.168.3.		Both 🔽		0
	7	192.168.3.		Both 💌		0
	8	192.168.3.		Both 💌		0
	9	192.168.3.		Both 💌		0
	10	192.168.3.		Both 💌		0

Parameter	Description
Well known services	You can select a pre-defined service from the list of well known services, then select a schedule rule, and the ID you wish to fill the settings in. Click Copy to and the settings you selected will be filled into the specific ID.
Server IP	This is the private IP address of the server behind the NAT firewall. Note: You must give your LAN client a fixed/static IP address for Virtual Server to work properly.
Service Ports	The range of ports to be forwarded to the Server IP. You can fill in a single port, such as 21, 80 or a range, such as 2000-2999.

Protocol	This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only or select "Both" to forward both "TCP" and "UDP" packets.
Enable	Check to enable this forwarding rule.
Schedule Rule#	Enter a Schedule Rule number to enable the forwarding rule only within the desired time frame. Please refer to 3.4.7 Schedule <i>Rule</i> for detailed setting instructions. You can set 0 to enable the forwarding rule always. If you assign a schedule rule (for example, 9am to 5pm) to ID#1, users are only allowed to access the FTP server from 9am to 5pm.
Next>> / Previous<<	Access the next/previous 10 port forwarding rules.

Click **Save** after you finished all settings.

3.2.2 Special Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger" field, then enter the public ports associated with the trigger port to open them for inbound traffic. The range of the Trigger port is 1 to 65535.

Virtual Server	Special	[HELP]			
Special AP		Popular applications MSN Gaming Zone 💌 Copy to ID 2			
 Miscellaneous 	ID	Trigger	Incoming Ports	Enable	
	1	6112	6112		
	2	47624	2300-2400,28800-29000		
	3	65535	0		
	4	65535	0		
	5	65535	0		
	6	65535	0		
	7	65535	0		
	8	65535	0		

Parameter	Description
Popular applications	You can select a pre-defined application from the list of Popular applications, and the ID you wish to fill the setting in. Click Copy to and the setting you selected will be filled into the specific ID.
Trigger	Enter an outbound port number assigned by the application.
Incoming Ports	When the trigger packet is detected, the inbound packets to the specified port numbers are allowed to pass through the NAT firewall. Type in a range of incoming ports to be triggered. For instance, "5000-5300" or "9091, 9093-9100", it depends on the special application's requirement.
Enable	Check to enable this Special Application rule.

Note: Only one PC can use each Special Application tunnel at same time. If the mechanism of Special Applications fails to make an application work, try setting your computer as the **DMZ** host instead.

Click **Save** after you finished all settings.

3.2.3 Miscellaneous

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going from your WAN port IP address to a particular IP address in your LAN. You can configure DMZ at this page, as well as UPnP and other settings.

Virtual Server	Miscellaneous Items		
Special AP	Item	Setting	Enable
Miscellaneous	▶ IP Address of DMZ Host	192.168.3.	
	 Super DMZ(IP Passthrough) 	0	
	▶ Non-standard FTP port		QQ.
	► UPnP setting		
	Xbox Support		
		Save Undo	

Parameter	Description		
IP Address of DMZ Host	Enter the local IP address that you wish to open DMZ. If the application still doesn't work on your computer after you open DMZ, you can try to enable Super DMZ for that computer.		

Super DMZ (IP Passthrough)	Select Super DMZ when your computer or server on the Local Area Network needs to allow access from the Internet with a real public IP address. With IP Passthrough configured, all IP traffic, not just TCP/UDP, is forwarded back to the host computer. This can be necessary with certain types of software that do not function reliably through Network Address Translation.
Non-standard FTP Port	Enter the FTP port number if the FTP server's port you try to access is not 21.
UPnP	Check the Enable box to enable UPnP feature. After you enable the UPnP feature, all client systems that support UPnP, like Windows 7, can discover this router automatically.
Xbox Support	Xbox is a video game console produced by Microsoft Corporation.

Click **Save** after you finished all settings.

3.3 Security Setting

This function allows you to configure Internet access rules for your local computers based on the IP address, MAC address, URL or keywords.

3.3.1 Packet Filtering

Packet Filtering allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination. Outbound Filter applies on all outbound packets but Inbound Filter applies only on packets that are destined to Virtual Servers or DMZ host.

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.) by their IP addresses, you can set up the filtering rules here. Packet filters can be helpful in securing or restricting your local network.

Example:

acket Filters	D Outb		[HELP				
omain Filters	Item		Setting				
RI Blocking	▶ Outbound Filter		Enable	Enable			
nternet Access Control	 Allow all to pass except those m Deny all to pass except those m 		e match the following rules. Match the following rules.	match the following rules. match the following rules.			
liscellaneous		E Schedule rule	llock List select one 💌 e (00)Always 💌 Copy to ID	2 🗸			
	ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#		
	1	.100-192.168.2.199	:21-110		0		
	2	3.2.20-192.168.2.50	:		0		
	3		•		0		
	4		•		0		
	5		-		0		
	6				0		
	7		:		0		
	8				0		

Computers with IP addresses between 192.168.2.20 to 192.168.2.50 have no restriction on accessing any network services, while others computers are all blocked. Meanwhile, computers with IP addresses between 192.168.2.100 to 192.168.2.199 are allowed to send Email (port 25), receive E-mail (port 110), and browse Internet (port 80).

For each rule, you can define:

- Source IP address
- Destination IP address
- Destination port address
- Protocol: TCP or UDP or both.

Parameters	Description
Outbound/Inbound Packet Filter	Check/uncheck Enable to enable/disable the Packet Filtering. Outbound Filter applies on all outbound packets but Inbound Filter applies only on packets that are destined to Virtual Servers or DMZ host.
Allow / Deny all to pass except those match the following rules	Please select "Allow" or "Deny" to decide the behavior of packet filtering table. If you select allow, all traffic will be allowed except the Source IP addresses listed in filtering table will be rejected to connect to the destination IP addresses and ports. If you select deny, all traffic will be denied except the Source IP address listed in filtering table will be allowed to connect to the destination IP addresses and ports.
Block List	Select a network service you wish to block, a schedule rule and ID#, click " Copy to ". The settings you selected will be filled into the specific ID.
Source IP	Please input the client's IP address you wish to apply the filtering rule. You can input a single IP address (192.168.2.10) or a range of IP addresses (192.168.2.10-192.168.2.50). Leaving this field blank indicates all IP addresses.
Destination IP	Please input the Destination IP address (i.e. an FTP site, Email server, etc.) you wish to apply the filtering. You can input a single IP address (192.168.2.10) or a range of IP addresses (192.168.2.10-192.168.2.50). Leaving this field blank means all IP addresses.

Port	Please input the port number here. You can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol, for example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. Leaving this field blank indicates all ports.
Enable	Check/uncheck Enable to enable/disable each Packet Filtering rule.
Schedule Rule#	Enter a Schedule Rule number to activate the filtering rule only within the desired time frame. Please refer to 3.4.7 Schedule <i>Rule</i> for detailed setting instructions. Set 0 to let the filtering rule always take effect.
Inbound Filter	Click Inbound Filter button to go to Inbound Packet Filter settings.

Click on **Save** after you finished all settings.

3.3.2 Domain Blocking

You can block users from accessing specific domains on the internet. This feature can help parents to manage the Internet usage for their children (i.e. Parental Control).

Packet Filters	Doma Doma	ain Filter				[HELP]	
Domain Filters	Item			Setting]		
URL Blocking	▶ Doma	in Filter	Enable				
Internet Access Control	► Log DI	▶ Log DNS Query		Enable			
Miscellaneous	Privilege IP Addresses Range		From 10	From 10 To 20			
moonarioodo	ID	Domain Suffix		Action	Enable	Schedule Rule#	
	1	xyz.com		Drop Log	~	0	
	2	www.abc.com		Drop 🗹 Log		0	
	3	msn.com		Drop Log	~	0	
	4					0	
	5					0	
	6					0	
	7					0	
	8					0	
	9					0	
	10 * (all others)			2	0		

Parameter	Description
Domain Filter	Check/Uncheck Enable to enable/disable Domain Filter.
Log DNS Query	Check/Uncheck Enable to enable/disable logging DNS Query.
Privilege IP Address Range	Enter an IP address range that has privilege to access any network service without restriction. For example, From 10 To 20.
Domain Suffix	You can enter a domain suffix of URL to be restricted, for example, ".com" or "xxx.com".
Action	Check Drop or Log or both to determine the actions of router, when user attempts to access the restricted domain. According to the settings in the screenshot above:

	Link request to xyz.com will be dropped and recorded in log file. Link request to www.abc.com will be allowed but will be recorded in log file. Link request to msn.com will be dropped and will not be recorded in log file. However, IP Address from 192.168.2.10 to 192.168.2.20 will not be restricted.
Enable	Check/Uncheck Enable to enable/disable each rule individually.
Schedule Rule#	Enter a Schedule Rule number to activate the filtering rule only within the desired time frame. Please refer to 3.4.7 Schedule <i>Rule</i> for detailed setting instructions. Set 0 to let the filtering rule always take effect.

Click on **Save** after you finished all settings.

3.3.3 URL Blocking

You can block access to certain websites or web contents from local PCs by entering a full URL address or just keywords. The major difference between "Domain Filter" and "URL Blocking" is that Domain Filter requires user to input a suffix (like .com or .org, etc), while URL Blocking requires user to input a **keyword** only. In other words, Domain Filter can block specific websites, while URL Blocking can block any website that contains the specific keyword. This feature can also help parents to manage the Internet usage for their children (i.e. Parental Control).

Packet Filters	URL Blo	cking			[HELP]
Domain Filtare		Item		Setting	
	▶ URL Bloc	cking	Enable		
URL Blocking	ID		URL	Enable	Schedule Rule#
Internet Access Control	1				0
Miscellaneous	-				
	2				0
	3				0
	4				0
	5				0
	6				0
	7				0
	8				0
	9				0
	10				0

Parameter	Description
URL Blocking	Check/Uncheck Enable to enable/disable URL Blocking.
URL	You can enter the full URL address of a website or any keyword you want to block, for example "XXX".
Enable	Check/Uncheck Enable to enable/disable each rule individually.
Schedule Rule#	Enter a Schedule Rule number to activate the filtering rule only within the desired time frame. Please refer to 3.4.7 Schedule

Click on **Save** after you finished all settings.

3.3.4 Internet Access Control

MAC Access Control will help you to prevent unauthorized users from connecting to your wireless router. Only those network devices with MAC addresses you specified here are allowed to access your wireless router. You can utilize this function with other security measures described in previous sections together to enhance the safety of your wireless network.

Packet Filters	Administrator MAC Co	ntrol	[HELP]	
Domain Filters	DHCP clients Sel	ect one	Copy to ID 🗸	
URL Blocking	ID	MAC Address	Enable	
Internet Access Control	1			
Miscellaneous	2			
	3			
	Save Undo			
	Internet Access Contr	ol		
	Item	Set	ting	
	▶ Access Control Type	MAC Access Control Group MAC Access Control Interface Access Control		
		Next >>		

Before you configure any MAC control settings, you can set up to 3 administrative computers that will not be restricted by MAC Control rules.

In the Administrator MAC Control section, select a DHCP client computer from the

drop-down list and select an ID, click "Copy to". The MAC address of the computer you selected will be automatically filled into the specific ID. Make sure the Enable box is checked. Click on **Save** after you finished all settings.

Administrator M	AC Control	[HELP]
DHCP clients	Select one 🖍 Cop	oy to 🛛 ID 🔳 💌
ID	MAC Address	Enable
1	00-14-2A-4C-BA-4C	
2		
3		
	Save Undo	

This router offers 3 types of Internet Access Control:

- MAC Address Control: allow or deny Internet access from specific MAC address. See 3.3.4.1.
- Group MAC Address Access: define user groups and map with schedule control to allow Internet access within specific time schedule. See 3.3.4.2.
- Interface Access Control: allow or deny Internet access based on each LAN Port and Wireless LAN within specific time schedule. See 3.3.4.3.

Item	Setting	
 Access Control Type 	 MAC Access Control Group MAC Access Control Interface Access Control 	

Select the desired setting and click **Next>>** for detailed configuration.

3.3.4.1 MAC Address Control

This feature allows you to control Internet access based on MAC address and time schedule.

Packet Filters	D MAC	Address Control				[HELP]
Domain Filters	Item		Setting			
URL Blocking	► MAC Address Control		Enable			
Internet Access Control Miscellaneous		ection control	Wireless and wired clients with C checked can connect to this device; a allow v unspecified MAC addresses to connect.		his device; and	
	Asso	ciation control	Wireless clients with A checked can ass deny w unspecified MAC addresses t Note: Association control has no effect	ociate to the o associate. on wired cli	wirele ents.	ess LAN; and
		DHCP clients Sch	edule rule (00)Always 💌 Copy to II) ¥	~	8
	ID	ID MAC Address	IP Address	С	A	Schedule Rule#
	1		192.168.3.			0
	2		192.168.3.			0
	3		192.168.3.			0
			102 168 3			0

Parameters	Description
MAC Access Control	Check this box to enable the MAC filtering function. All settings in this page will take effect only when Enable is checked.
Connection Control	Check this box to enable the rule that wireless or wired clients whose MAC addresses are in the table can connect to the router. Choose "allow" or "deny" to determine whether the router allows or denies connection from other clients whose MAC addresses are not in the table.
Association Control	Check this box to enable the rule that only the wireless clients whose MAC addresses are in the table can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means it cannot send or receive any data via this router. Choose "allow" or "deny" to determine if the router allows or denies wireless association from clients whose MAC addresses are not in the table.

DHCP Clients	Select a DHCP client from the drop down list. Select an ID number and click Copy To . The client's MAC address will be copied to the ID you selected; you do not need to enter it manually.
MAC Address	Input the MAC address of your computer / network device.
c	Check this box to allow the wired/wireless client connecting to the router.
Α	Check this box to allow the wireless client associating to the wireless network.
Previous / Next	You can set up to 32 MAC control rules for this router. Click Previous or Next to reach the previous or next 4 entries.
Schedule Rule#	Enter a Schedule Rule number to activate the filtering rule only within the desired time frame. Please refer to 3.4.7 Schedule <i>Rule</i> for detailed setting instructions. Set 0 to let the filtering rule always take effect.

Click on **Save** after you finished all settings.

3.3.4.2 Group MAC Access Control

This feature allows you to define user groups and map them with schedule control to allow Internet access within specific time frame.

In the example below, two groups have been added with different schedule rule: Group List 1 has two computers with Schedule Rule 1. The two computers in Group 1 can only access network within the time frame of Schedule Rule1. Under the group list, you can modify Schedule 1 by clicking on **Modify Schedule 1** (see section 3.4.7 Schedule Rule), and remove any member by clicking the **Delete** button.

	Group MAC Access Control			LUELD1
Packet Filters				[HELP]
Domain Filters	Item Setting			
URL Blocking	► Group MAC Access Control			
Internet Access Control	Save Undo			
Miscellaneous	Add Member to Group List	1		
	Add MAC Address -	<< Copy Select	t one	~
	2 to Group 1 💌 a Add	and apply schedule rule (00)Alw MAC : 00-16-A4-01-52-DD to Gro	ays 🔽 Add 🗸	
	2 to Group 1 💌 a Add Group List 1 - use Schedule Rule	and apply schedule rule (00)Alw I <u>MAC : 00-16-A4-01-52-DD</u> to <u>Gro</u> e 1	ays 💌 Add 4	Schedule 1]
	2 to Group 1 💌 a Add Group List 1 - use Schedule Rul MAC Address	and apply schedule rule (00)Alw MAC : 00-16-A4-01-52-DD to Gro e 1 Host Name	ays Add 4 oup 1 ! [Modify ! IP Address	Schedule 1]
	2 to Group 1 💌 a Add Group List 1 - use Schedule Ruk MAC Address 00-14-2A-4C-BA-4C	and apply schedule rule (00)Alw I MAC : 00-16-A4-01-52-DD to Gro e 1 Host Name user-Win7	Add 4 Add 4 Oup 1 ! [Modify : IP Address 192.168.3.129	Schedule 1] Action Delete
	2 to Group 1 💌 a Add Group List 1 - use Schedule Rule MAC Address 00-14-2A-4C-BA-4C 00-16-A4-01-52-DD	and apply schedule rule (00)Alw MAC : 00-16-A4-01-52-DD to Gro e 1 Host Name user-Win7 UA105307637	Add 4 Add 4 Add 4 IP Address 192.168.3.129 192.168.3.186	Schedule 1] Action Delete Delete
	2 to Group 1 💌 a Add Group List 1 - use Schedule Rule MAC Address 00-14-2A-4C-BA-4C 00-16-A4-01-52-DD Group List 2 - use Schedule Rule	and apply schedule rule (00)Alw MAC : 00-16-A4-01-52-DD to Gro e 1 Host Name user-Win7 UA105307637 e 2	Add 4 Add 4 Add 4 (Modify 1) (Modify 1) 192.168.3.129 192.168.3.186 (Modify 1)	Schedule 1] Action Delete Delete Schedule 2]
	2 to Group 1 💌 a Add Group List 1 - use Schedule Rule MAC Address 00-14-2A-4C-BA-4C 00-16-A4-01-52-DD Group List 2 - use Schedule Rule MAC Address	and apply schedule rule (00)Alw MAC : 00-16-A4-01-52-DD to Gro e 1 Host Name User-Win7 UA105307637 e 2 Host Name	Add 4 Add 4 Add 4 Add 4 (Modify 3 192.168.3.129 192.168.3.186 [Modify 3 IP Address	Schedule 1] Action Delete Delete Schedule 2] Action

Parameters	Description
Group MAC Access Control	Check this box to enable Group MAC Access Control and then click Save . All settings in this page will take effect only when Enable is checked.
Add MAC Address	Follow the steps below to add an MAC address to a designated group:
1. Enter MAC address manually or select one from the DHCP client list, and click "**<<Copy**" to copy the MAC address of the client computer / network device.

2. Assign a group number by selecting a number from the drop-down list.

- 3. Select a time schedule rule from the drop-down list.
- 4. Click Add.

3.3.4.3 Interface Access Control

Interface Access Control allows you to control the network access based on each LAN Port and Wireless LAN within specific time schedule.

Packet Filters	Interface Access Control INTERP INTERPORT			
Domain Filters	Item	Setting		
• URL Blocking	▶ Interface Access Control	Enable		
Internet Access Control	Interface	Schedule Rule	Deny	
Miscellaneous	Port 1	(00)Always	V	
	Port 2	(00)Always	V	
	Port 3	(00)Always		
	Port 4	(00)Always	v	
	Wireless	(00)Always		
		Save Undo		

Parameters	Description
Interface Access Control	Check this box to enable Interface Access Control. All settings in this page will take effect only when Enable is checked.
Interface	The physical Interface of router: LAN Port 1~4 and Wireless LAN.

Schedule Rule	Select a Schedule Rule from the drop-down list. Please refer to 3.4.7 Schedule Rule for detailed setup instructions.
Deny	Check/Uncheck Deny to deny/allow network access from an Interface within the selected schedule rule.

3.3.5 Miscellaneous

Packet Filters	Miscellaneous Items [HELP]				
Domain Filters	Item	Setting	Enable		
URI Blocking	Remote Administrator Host / Port	0.0.0.0 / 88			
Internet Access Control	Administrator Time-out	0 seconds (0 to disable)			
Miscellaneous	▶ Discard PING from WAN side				
moconditions	▶ SPI mode				
	DoS Attack Detection				
	▶ VPN PPTP Pass-Through	V			
	▶ VPN IPSec Pass-Through				
	Save Undo				

Parameters	Description
Remote Administrator Host/ Port	This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. Setting the specified IP address as 0.0.0.0 indicates any host can connect with this product to perform administration task. You can specify a port number for remote administrator; the default value is 88.
Administrator Time-out	The system will log out the administrator after no activity for a

	period of time. You may set the time-out period to zero to disable this feature.
Discard PING from WAN side	Check this box to enable Discard PING from WAN side. When you enable this feature, your router will not respond to a "ping" request from any host on the WAN side.
SPI Mode	Stateful Packet Inspection mode is a firewall that keeps track of the state of network connections (such as TCP, UDP communication) travelling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.
DoS Attack Detection	Check this box to enable the DoS Attack Detection. Router will block the DoS once it is detected. Denial of Service (DoS) is a common attack measure, by transmitting a great amount of data or request to your Internet IP address and server, the Internet connection will become very slow, and server may stop responding because it is not capable to handle too much traffic.
VPN PPTP Pass-Through	Check this box and the router will enable PPTP packets pass through the router for VPN connection
VPN IPSec Pass-Through	Check this box and the router will enable IPsec packets pass through the router for VPN connection.

3.4 Advanced Setting

This page allows you to set up system time, log, DDNS, routing, QoS, schedule rule, and other advanced settings.

3.4.1 System Time

Specify correct system time for your router is very important. It will affect the schedule rule and system logs. This router provides 3 ways to configure the system date and time:

- 1) Synchronize with time server. (The router must connect to the Internet.)
 - > Select Get Date and Time by NTP Protocol
- 2) Synchronize with PC.
 - > Select Set Date and Time using PC's Date and Time
- 3) Manually configure the time
 - > Select Set Date and Time manually

System Time	System Time	System Time			
System Log	Item	Item Setting			
Dynamic DNS	► System Time	Tuesday, October 19, 2010 2:29:17 PM			
QoS Rule	▶	Get Date and Time by NTP Protocol Sync Now !			
SNMP	Time Server	time.nist.gov			
Routing	Time Zone	(GMT-08:00) Pacific Tir	ne (US & Canada)	×	
Schedule Rule	► O Set Date and Tim	ne using PC's Date and Time	1		
	PC Date and Time	e Tuesday, October 19, 2	010 3:29:17 PM		
	► O Set Date and Tim	ne manually			
	Date	Year : 2009 🗸	Month : Jun 🔽	Day : 01 💌	
	Time	Hour : 0 (0-23)	Minute : 0 (0-59)	Second : 0 (0-59)	
	Daylight Saving	O Enable 💿 Disab	le		
	Start	Month : Jan 💌	Day : 01 🗸	Hour : 00 💌	
	End	Month : Jan 💌	Day : 01 💌	Hour : 00 💌	
		Sav	e Undo		

Parameter	Description
System Time	Displaying the current system time of router.
Sync Now	Click this button to synchronize the system time with the desired time server. (The router must be connected to the Internet to be able to synchronize time.)
Time Server	Select a time server here.
Time Zone	You can select your local time zone here. The router will synchronize time according to your time zone selection.
PC Date and Time	Select "Set Date and Time using PC's Date and Time", router will automatically copy the date and time from your PC.
Date / Time	Select Year, Month, Day, Hour, Minute, Second if you wish to set the system date and time manually.
Daylight Saving	Select Enable or Disable for daylight saving according to where you are located.
Start / End	If you enabled daylight saving, please specify the first and last days of daylight saving time.

3.4.2 System Log

You can enable this function to log all important system events for your router. This page supports two methods to export system logs to specific destination by means of syslog (UDP) and SMTP (TCP).

System Time	System Log	System Log [HELP]			
System Log	Item	Setting	Enable		
Dynamic DNS	► IP Address of Syslog Server	192.168.3.			
QoS Rule	▶ E-mail Alert	Send Mail Now			
SNMP	SMTP Server IP/Port				
Routing	• E-mail addresses				
Schedule Rule					
	• E-mail Subject				
	• User name				
	Password				
	⊁ Log Type	 System Activity Debug Information Attacks Dropped Packets Notice 			
		View Log Save Unde			

Parameters	Description
IP Address of Syslog Server	Enter the host IP of destination where system log will be sent to. Check Enable to enable this feature
Email Alert	Check Enable if you want to enable Email alert (send syslog via Email). Email alert will work only if the router connects to Internet.
Send Mail Now	Click Send Mail Now to email system log to the account you set up now.
SMTP Server/Port	Input the SMTP server IP and port, which are connected with '/'. If

	you do not specify port number, the default value is 25. For example, "mail.abc.com" or "192.168.1.100/25".
Email Addresses	Enter the Email addresses of the recipients who will receive these logs. You can assign more than 1 recipient by using ';' or ',' to separate these Email addresses.
Email Subject	The subject of email alert, this setting is optional.
Username	Input the user name of the Email account.
Password	Input the password of the Email account.
Log Type	Check the types of communication you wish to log.
View Log	Click View Log to view all system logs.

3.4.3 Dynamic DNS

BASIC	SETTING 🤣 FORWARDING RULI	es 🚱 security setting	ADVANCED SETTING	TOOLBOX
System Time	Dynamic DNS			[HELP]
System Log	Item		Setting	
Dynamic DNS	> DDNS	💿 Disable 🔘 Enable		
QoS Rule	▶ Provider	DynDNS.org(Dynamic) V Provider website		
SNMP	Host Name			
Routing	▶ Username / E-mail			
Schedule Rule	▶ Password / Key			
		Save	Undo	

Parameter	Description
DDNS	Select Disable or Enable DDNS function.
Provider	A DDNS provider provides service for you to bind your IP (even private IP) with a certain Domain name. Choose a desired provider.
Provider Website	Click Provider Website to go to the selected DDNS provider's website.
Host Name	You can register a domain name at the DDNS provider's website. The full domain name is concatenated with host name (you specify) and a suffix (DDNS provider specifies). For example, ABChome.dyndns.org.
Username / E-mail	This field is required by DDNS provider to authenticate its users. Input username you registered to the DDNS provider.
Password / Key	This field is required by DDNS provider to authenticate its users, too. Input password or key according to the DDNS provider you select.

3.4.4 QoS Rule

Quality of Service provides an efficient way for computers on the network to share the Internet bandwidth with a promised quality of Internet service. Without QoS, all computers and devices on the network will compete with one another to get Internet bandwidth, and some applications which require guaranteed bandwidth (like video streaming and network telephone) will be affected; therefore, an unpleasing result will occur, like interruption of video / audio streaming.

System Time	Qo S	Rule			_	
System Log		Item		Setting		
Dynamic DNS	+ QoS C	Control	Enable			
QoS Rule		Sch	Well known services selec nedule rule (00)Always 💌 🕻	Well known services select one V ule rule (00)Always V Copy to ID V		
Souting	ID	Local IP	Remote IP : Ports	QoS Priority	Enable	Schedule Rule#
	1			Normal 🛩		0
	2			Normal 🛩		0
	3			Normal 🖌		0
	4		-	Normal 💌		0
	5		-	Normal 💌		0
	6		-	Normal 💌		0
	7			Normal 💌		0
	8		1	Normal 💌		0

Parameter	Description
QoS Control	Check Enable to enable QoS function.
Well known services	Select a network service, a schedule rule and ID#, click " Copy to ". The settings you selected will be filled into the specific ID.
Local IP	Specify a local (source) IP address that will be affected by this
	rule.

Remote IP Address	Specify a remote (destination) IP address that will be affected by this rule.
Ports	Please input the range of remote (destination) port number that will be affected by this rule. If you want to apply this rule on port 80 to 90, please input "80-90"; if you want to apply this rule on a single port, just input the port number, such as 80. If the remote (destination) IP address and /or port number is universal, just leave it blank.
QoS Priority	Assign High, Normal, or Low priority to the specific network client.
Enable	Check to enable individual QoS rule.
Schedule Rule#	Enter a Schedule Rule number to activate the QoS rule only within the desired time frame. Please refer to 3.4.7 Schedule <i>Rule</i> for detailed setting instructions.

3.4.5 SNMP

System Time	SNMP Setting	(HEL
* System Log	Item	Setting
Dynamic DNS	▶ Enable SNMP	☑ Local □ Remote
QoS Rule	► Get Community	public
* SNMP	▶ Set Community	private
Routing	▶ IP 1	
Schedule Rule	▶ IP 2	
	▶ IP 3	
	▶ IP 4	
	SNMP Version	○ V1

Parameter	Description
Enable SNMP	You must check either Local or Remote or both to enable SNMP function. If <i>Local</i> is checked, this device will response request from LAN. If <i>Remote</i> is checked, this device will response request from WAN.
Get Community	Setting the community of GetRequest your device will response.
Set Community	Setting the community of SetRequest your device will accept.
IP 1~4	Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.
SNMP Version	Please select proper SNMP Version that your SNMP Management software supports.

3.4.6 Routing

Routing Table allows you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or unchecking the Enable checkbox.

System Time	Routing Table			[HELP]		
System Log		Item		Setting		
Dynamic DNS	Dynamic Routing		⊙ Disable ○ RIPv1 ○	RIPv2		
Oos Pule	Static Routing		Oisable O Enable			
SNMD	ID	Destination	Subnet Mask	Gateway	Нор	Enable
Deuting	1					
Rouung	2					
Schedule Rule	3					
	4					
	5					
	6					
	7					
	8					
			Save	0		

For Example:



Configuration on Static Routing

Destination	Subnet Mask	Gateway	Нор	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	\checkmark
192.168.0.0	255.255.255.0	192.168.123.103	1	\checkmark

When Client3 wants to send an IP data gram to 192.168.0.2, it will use the above table to determine that it has to go via 192.168.123.103 (a gateway), and if it sends packets to 192.168.1.11, it will go via 192.168.123.216

Parameter	Description
Dynamic Routing	Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

Static Routing	Select Enable or Disable to enable or disable Static Routing function.
Destination	Enter a destination IP address. The Destination IP is the address of the remote network or host to which you want to assign a static route.
Subnet Mask	Enter the subnet mask. The Subnet Mask determines which portion of a Destination IP address is the network portion, and which portion is the host portion.
Gateway	Enter the gateway IP address. This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.
Нор	Specify the number of next hop.
Enable	Check or uncheck Enable to enable or disable the static routing rule.

3.4.7 Schedule Rule

BASIC	C SETTING 🤣 FORWAR	RDING RULES 🙆 SEC	URITY SETTING	ADVANCED SETTING	TOOLBOX	
System Time	Schedule R	ule				[HELP]
System Log	Item			Setting		
Dynamic DNS	▶ Schedule		Enable	Enable		
QoS Rule	Rule#	Rule Na	ime		Action	
SNMP	1	FTP		E	dit Delete	
Routing	2	Weeke	nd	E	dit Delete	
Schedule Rule			Save Add	I New Rule		

You can configure schedule rules to control the time frame of network access.

Parameter	Description
Schedule	Check or uncheck Enable to enable or disable the schedule rule.
Rule#	Displaying rule numbers.
Rule Name	Displaying rule names that have been added to the schedule rule table.
Action	Click on Edit to modify the schedule rule or Delete to remove the rule from the schedule rule table.
Add New Rule	Click on Add New Rule to add a new rule to the schedule rule table. Please see <i>3.4.7.1</i> for detailed instructions.

3.4.7.1 Add New Rule

System Time	Schedule Rule Setting [HELP]			
System Log	Item Setting		etting	
Dynamic DNS	▶ Name of Rule 3			
QoS Rule	▶ System Time	Wednesday, October 20, 2010 12:18:30 PM		
SNMP	Week Day	Start Time (hh:mm)	End Time (hh:mm)	
Routing	Sunday		•	
Schedule Rule	Monday		÷	
	Tuesday		-	
	Wednesday		÷	
	Thursday		-	
	Friday		:	
	Saturday		:	
	Every Day		:	
		Save Undo Back		

You can add a new schedule rule in this page.

Parameter	Description
Name of Bulat	Enter a name for the new rule
Name of Rule#	
System Time	Displays the current system time of the router for you to verify if this matches with the date/time of where you are located. You can see <i>3.4.1</i> on how to modify the system time.
Week Day	You can set time schedule for each day or everyday.
Start Time/End Time (hh:mm)	Enter the start and end time of a time schedule. For example, Start Time 01:00, End Time 23:00. Please note that End Time should not be prior to Start Time.

Click on **Save** after you finished all settings, and click **Back** to go back to Schedule Rule page.

3.5 Toolbox

The Toolbox page allows you to view system logs, upgrade firmware, save/reload configuration settings, reset factory default settings, reboot the router, and perform ping test.



3.5.1 View Log

View Log	System Log		
Firmware Upgrade	Item	Info	
	WAN Type	Dynamic IP Address (V0.27a0 20100812)	
Backup setting	Display time	Wed Oct 20 13:50:11 2010	
Reset to Default	Time	Log	
Reboot	Wednesday, October 20, 2010	10:50:57 AM DOD:triggered internally	
 Miscellaneous 	Wednesday, October 20, 2010 10:50:57 AM, DHCP:discover(GinaRouter)		

You can view, download, and clear the system logs stored in the router here.

3.5.2 Firmware Upgrade

You can view the current firmware version of router in this page.

To upgrade the firmware for the router, you must use a computer that is wired connected to the router. Firstly, you need to download the firmware from <u>www.airlink101.com</u> and save it to your local hard disk first. You may need to unzip it if it is a .zip file.

BASIC SETTING	S FORWARDING RULES	SECURITY SETTING	ADVANCED SETTING	TOOLBOX
* View Log	Firmware Upgrade			
Firmware Upgrade	Firmware Filename			
Backup Setting			Browse	
Reset to Default	Current firmware version is V0.27a0 20100812. The upgrade procedure takes about 20 seconds.			s about 20 seconds.
• Reboot				
Miscellaneous	Note! Do not power off the unit when it is being upgraded.			
	When the upgrade is done successfully, the unit will be restarted automatically.			
		Upgrade	Cancel	

Click on **Browse** to select the firmware you just downloaded/unzipped, then click **Upgrade** to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete).

NOTE: Never interrupt the upgrade process by closing the web browser or disconnect your computer from router. If the firmware you uploaded is corrupt, the firmware upgrade will fail, and you may contact Technical Support for help.

3.5.3 Backup Setting

You can save the router's configuration settings to your local hard disk by clicking on Backup Setting and save it as a .bin file. Once you need to restore the settings, please go to Firmware Upgrade page and load the .bin file you saved.

	Opening config.bin	X
 View Log 	You have chosen to open	
• Firmware Upgrade	config.bin	
 Backup Setting 	which is a: Binary File from: http://192.168.2.1	
 Reset to Default 	What should Firefox do with this file?	7
 Reboot 	O Open with Browse	
 Miscellaneous 	 Save File Do this automatically for files like this from now on. 	
	OK Cancel]

3.5.4 Reset to Default

To restore the router settings to factory default, click on Reset to Default, and you will be prompted:

The page at http://192.168.2.1 says:			
?	Reset all settings to factory default?		
	OK Cancel		

Click OK to continue or Cancel to exit.

3.5.5 Reboot

To reboot the router, click on Reboot, and you will be prompted:

The pa	The page at http://192.168.2.1 says:		
?	Reboot right now?		
	OK Cancel		

Click OK to continue or Cancel to exit.

3.5.6 Miscellaneous

ViewLog	Miscellaneous Items		[HELF	
Firmware Upgrade	Item		Setting	
Backup Setting	▶ MAC Address for Wake-on-LAN		Wake up	
Reset to Default	▶ Domain Name or IP address for Ping Test		Ping	
Reboot	Save	ndo		
Miscellaneous				
Miscellaneous	-			
Miscellaneous				

Parameter	Description
MAC Address for Wake-on-LAN	Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to use this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device. Enter the MAC address of the device and click Wake Up . The router will send wake-up frame to the target device immediately and the device can be powered up remotely.
Domain Name or IP Address for Ping Test	Enter an domain name (i.e. google.com) or IP address to perform ping test. If you can ping a remote website, it means the Internet is connected.

Chapter 4 Status

The Status section allows you to monitor the current status of your router. You can use the Status page to monitor: the Internet connection, Wireless, NAT status, and the statistics information of the Router.

ADMINISTRATOR'S MAIN MENU	📲 Status	W Wizard	Advanced		+ Lo
System Status					[HELP
Item		WAN Status		Sidenote	
Remaining Lease Time		00:00:00		Reconfiguring	
IP Address		0.0.0.0			
Subnet Mask		0.0.0.0			
Gateway		0.0.0.0		Unreachable	
Domain Name Server		192.168.2.1			
MAC Address		00-50-18-21-D4-38			
U Wireless Status					
Item		WLAN Status		Sidenote	
Wireless mode		Enable			
SSID		Airlink101			
Channel		11			
Security		None			
MAC Address		00-50-1 <mark>8</mark> -21-D4-39	0		
Statistics Information					
Statistics of WAN		Inbound	1	Outbound	
Octets		25399713		4601549	
Unicast Packets		42057		28365	
Non-unicast Packets		52237		18955	
Vie	ew Log Clients	s List NAT Statu	us Refresh		

4.1 System Status

You can view the status of current Internet connection. By clicking Renew and Release, you can renew and release the WAN IP address obtained from the ISP (Internet Service Provider).

System Status			
Item	WAN Status	Sidenote	
Remaining Lease Time	999:59:54	Renew	
IP Address	192.168.20.121	Release	
Subnet Mask	255.255.255.0		
Gateway	192.168.20.1		
Domain Name Server	206.13.28.12, 206.13.31.12		
MAC Address	00-50-18-21-D4-38		

4.2 Wireless Status

You can view the Wireless LAN status of your router, including SSID (the name of your wireless network), Channel number, Security, and Wireless MAC address of the router.

U Wireless Status				
Item	WLAN Status	Sidenote		
Wireless mode	Enable			
SSID	Airlink101			
Channel	11			
Security	None			
MAC Address	00-50-18-21-D4-39			

4.3 Statistics Information

You can view the statistics information of your router, including inbound and outbound packets.

Statistics Information						
Statistics of WAN	Inbound	Outbound				
Octets	25399713	4605653				
Unicast Packets	42057	28365				
Non-unicast Packets	52237	18967				

4.4 NAT Status

Click NAT Status on the bottom of the Status page to view NAT Status.

ID Internal Protocol External NAT Time-o Page: 1/1 (Active Session Number:0)	I NAT SU	atus				12
Page: 1/1 (Active Session Number:0)	ID	Internal	Protocol	External	NAT	Time-out
Page: 1/1 (Active Session Number:0)						
	age: 1/1 (/	Active Session Numbe	er:0)			

Chapter 5 Appendix

5.1 Hardware Specification

Standards

- IEEE 802.11b / g / n
- IEEE 802.3, 802.3u, 802.3ab

Ports

- 1 x Gigabit WAN port
- 4 x Gigabit LAN port

Antenna type

Two 3dBi detachable dipole
 antennas

Operation Modes

- AP
- WDS Bridge
- AP+WDS Bridge

Security

- WEP 64/128-bit
- WPA2-PSK, WPA-PSK
- Radius Server

LEDs

 Power, Status, WAN, WLAN, LAN1~4, On/Sleep

System Requirement

- Windows®, Mac®, or Linux® operating system
- Installed Ethernet adapter
- Recommended use with Airlink101 Wireless N 300 products

Power

• DC 12V / 1A

Dimensions

• 185 x 110 x 27 mm (L x W x H)

Temperature

• Operating: 0°C to 40°C

Humidity

• Operating: 10% to 90% Non-Condensing

Warranty

• Limited 1-year warranty

Certification

• FCC, CE

Technical Support

E-mail: support@airlink101.com

Toll Free: 1-888-746-3238

Website: www.airlink101.com

*Theoretical maximum wireless signal rate derived from IEEE standard 802.11 specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, mix of wireless products used, radio frequency interference (e.g., cordless telephones and microwaves) as well as network overhead lower actual data throughput rate. Compatibility with 802.11n devices from other manufactures is not guaranteed. Specifications are subject to change without notice. Photo of product may not reflect actual content. All products and trademarks are the property of their respective owners. Copyright ©2010 Airlink101®