

GW-300R

Wireless 2T2R 300Mbps Giga Router

User's Manual

www.airlive.com





Copyright & Disclaimer

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.



CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

The specification is subject to change without notice.



Bluetooth © 2009 OvisLink Corporation, All Rights Reserved

Table of Contents

1.Introduction 1
1.1 Packing List2
1.2 Spec Summary Table
1.3 Hardware Configuration4
1.4 LED indicators5
1.5 Procedure for Hardware Installation6
2.Getting Start
3.Making Configuration14
3.1 Login to Configure from Wizard15
3.2 System Status
3.3 Advanced 20
3.3.1 Basic Setting
3.3.2 Forwarding Rules
3.3.3 Security Settings
3.3.4 Advanced Settings
3.3.5 Toolbox
Appendices and Index70
802.1x Setting
WPA Settings75
FAQ and Troubleshooting84
What can I do when I have some trouble at the first time?
How do I connect router by using wireless?87





Congratulations on your purchase of this outstanding Wireless Broadband Router. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing, and is easy to configure and operate even for non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.



1.1 Packing List

items	Description	Contents	Quantity
1	WiFi Gigabit Router		1
2	Power adapter 12V 1A	A CON	1
3	CD	All Lucs	1



1.2 Spec Summary Table

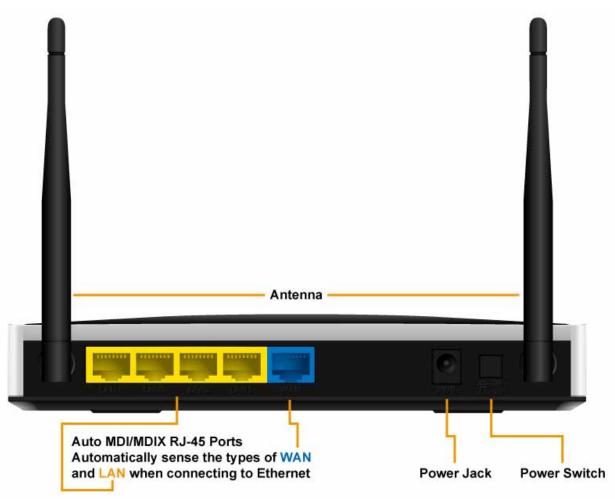
Device Interface		
Ethernet WAN	RJ-45 port, 10/100/1000Mbps, auto-MDI/MDIX	1
Ethernet LAN	RJ-45 port, 10/100/1000Mbps, auto-MDI/MDIX	4
Antenna	3 dBi detachable antenna	2
WPS Button	For WPS connection	1
Wireless	To enable or disable Wireless Radio	1
Enable/disable		
LED Indication	Power/Status / WAN / LAN1 ~ LAN4/ WiFi	•
Power Jack	DC Power Jack, powered via external DC 12V/1A	1
T OWET BACK	switching power adapter	1
Wireless LAN (WiFi)		
Standard	IEEE 802.11b/g/n compliance	•
SSID	SSID broadcast or in stealth mode	•
Channel	Auto-selection, manually	•
Security	WEP, WPA, WPA-PSK, WPA2, WPA2-PSK	•
WPS	WPS (Wi-Fi Protected Setup)	•
WMM	WMM (Wi-Fi Multimedia)	•
Functionality		
Ethernet WAN	PPPoE, DHCP client, Static IP, PPTP, L2TP	•
WAN Connection	Auto-reconnect, dial-on-demand, manually	•
One to Many NAT	Virtual server, special application, DMZ, Super	
One-to-Many NAT	DMZ (IP Passthrough)	•
NAT Session	Support NAT session	20000
SPI Firewall	IP/Service filter, URL blocking, MAC control	•
DoS Protection	DoS (Deny of Service) detection and protection	•
Routing Protocol	Static route, dynamic route (RIP v1/v2)	•
Management	SNMP, UPnP IGD, syslog, DDNS	•
Administration	Web-based UI, remote login, backup/restore setting	•
Performance	NAT up to 700Mbps and Wireless up to150Mbps	



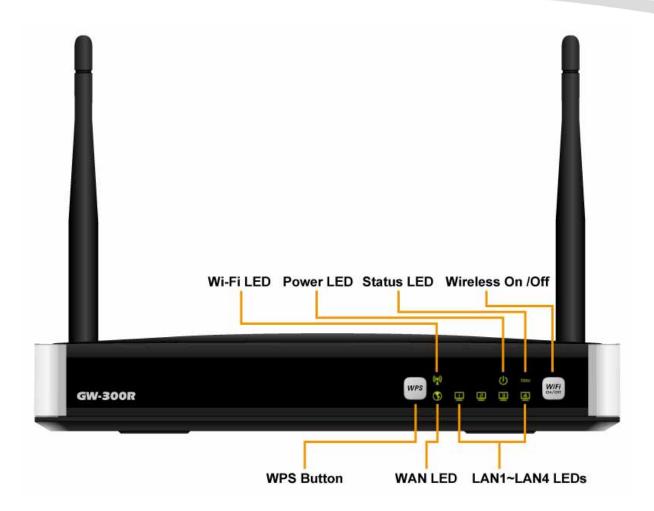
Environment & Certific	Environment & Certification					
Package Information	Package dimension (mm)					
Fackage information	Package weight (g)					
Operation Tomp	Temp.: 0~40oC, Humidity 10%~90%					
Operation Temp.	non-condensing	•				
Storago Tomp	Temp.: -10~70oC, Humidity: 0~95%					
Storage Temp.	non-condensing	•				
EMI Certification	CE/FCC compliance	•				
RoHS	RoHS compliance	•				

1.3 Hardware Configuration

Figure 2-1 Front Panel





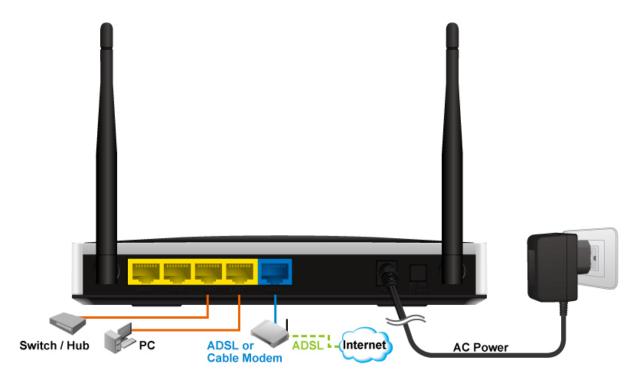


1.4 LED indicators

	LED status	Description
Status	Green in flash	Device status is working.
WAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
LAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
	Green	WLAN is on
WiFi LED	Green in flash	Data access
	Green in fast	Device is in WPS PBC mode
	flash	
	Green in dark	Wi-Fi Radio is disabled



1.5 Procedure for Hardware Installation



Step 1. Attach the antenna.

1.1. Remove the antenna from its plastic wrapper.

1.2. Screw the antenna in a clockwise direction to the back panel of the unit.1.3. Once secured, position the antenna upward at its connecting joint. This will ensure optimal reception.



1.Turn off the Power Switch first.

Step 2 Insert the Ethernet cable into LAN Port:

Insert the Ethernet patch cable into LAN port on the back panel of Router, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.







Step 3 Insert the Ethernet patch cable into Wired WAN port:

Insert the Ethernet patch cable form DSL Modem into Wired WAN port on the back panel of Router.

Step 4. Power on Router:4.1. Connect the power adapter to the receptor on the back panel of yourRouter and Push Power switch



Step 5. Complete the setup. 5.1. When complete, the Status LED will flash.

2. Getting Start



2

Getting Start

Insert the CD into CD reader on your PC. The program, AutoRun, will be executed automatically. And then you can click the Easy setup Icon for this utility. Configure the settings by the following steps.

2.1.Select Language then click "Next" for continues.





2.2 Setup mode

You can select Wizard mode to run the setup step-by-step or run advanced mode to diagnose the network settings of the router.



2.3 Advanced mode Setup.Check the PC, Router or Internet icons for the Status of PC, Router or Internet.





2.4 Quick Wizard Install mode Setup

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.

Click "Next" for continues



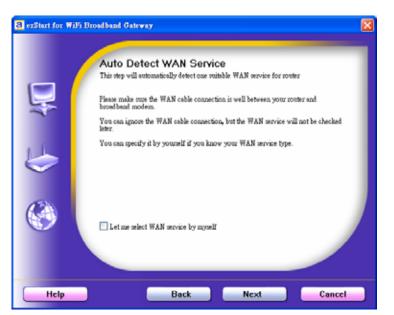
2.5. Wireless Setting.Key in the SSID, Channel and Security options, and then click "Next" for continues.





2.6 Auto Detect WAN Service.Click "Next" for continue.Click the button, "Let me select WAN service by myself", to disable this function.

Note: The Item supports to detect the Dynamic and PPPoE WAN Services only



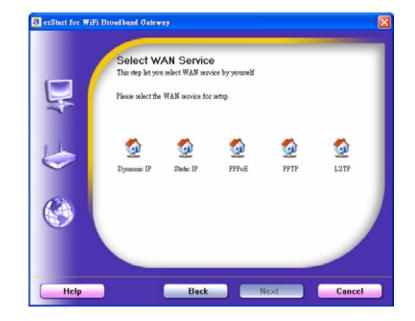
Example, the Dynamic WAN type is detected.





2.7. Manual select WAN Service In the manual mode, Click the any icons for continues.

2.8 Summary of the settings and Next to "Reboot" Click "Next" for continue.



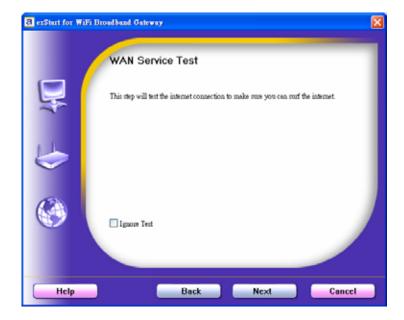
2.9 Apply the Settings or Modify. Click "Next" for continue.





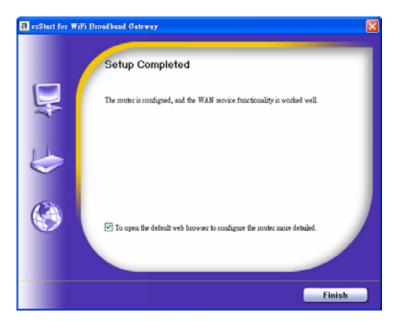
2.10 Test the Internet connection.Test WAN Networking service. Click"Next" for continue.

You can ignore the by select the "Ignore Test".



2.11 Setup Completed.

The EzSetup is finish, you can open the default web browser to configure advanced settings of the Router. Click "Finish" to complete the installation.

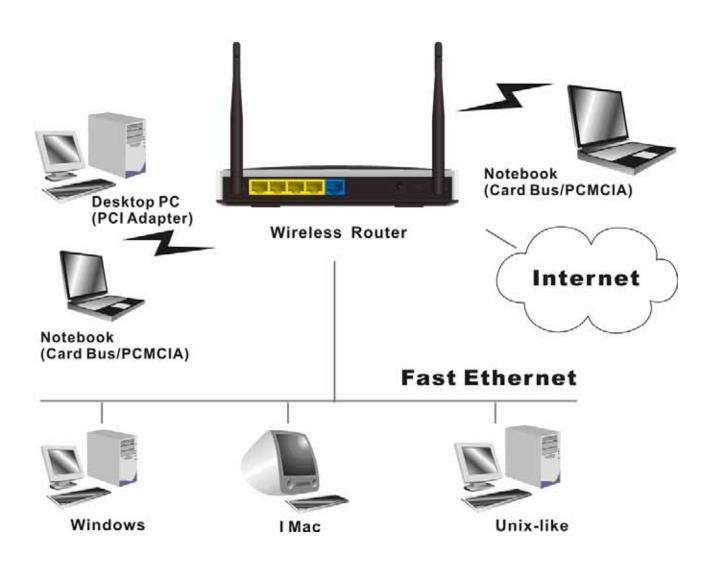




3

Making Configuration

This product provides Web based configuration scheme, that is, configuring by your Web browser, such as Mozilla Firefox or or Internet Explorer. This approach can be adopted in any MS Windows, Macintosh or UNIX based platforms.





3.1 Login to Configure from Wizard

Type in the IP Address (http://192.168.1.254)

WiFi Broadband Router Web-Console - Windows Internet Explorer

 Image: State of the state of t

Type password, the default is "airlive" and click 'login' button.

Press "Wizard" for basic settings with simple way.

Air Live	-	GW-300R Wireless 212R 300Mbps Giga Router
O. USER'S RAUN RENUS	- Status	
	System Patroned .	Idetautt annet Logn

Air Live	GW-300R Wireless			Centre Al Pre con 2R 300Mbps Giga Rout
ADMANESTRATORY MAIN MENU	-B Status	W Waard	CII Advanced	+ Logout English
A_				
O System Status				THEFT
tem		WAN Status	1	Sidenote
IP Addrewii		192.158.0.154		That c IP
Subnet Mapk.		256 255 255.0		
Gateway		192 158 0 254		
Domain flame Server		158 95 1 1		
MAC Addrese		00-50-18-21-04-57		

Press "Next" to start wizard.





Step 1: Set up your system password.

Air Live	Live GW-300R Wireless 21				
> ADMINISTRATOR'S MAIN MENU	-fi Status	W Wtrant		+ Logout English	
🔉 Selup Wizant - Selup Login Pasev	ront			[1347	
	 Gid Password 	_			
			-		
	* New Password	-			
	+ Recordim				
<bad (="" 1.1.1)<="" td=""><td>> Passward > WAW)</td><td>Wirslash > Sur</td><td>malary a Tiniate 1</td><td>tiet></td></bad>	> Passward > WAW)	Wirslash > Sur	malary a Tiniate 1	tiet>	
		<pre>control 0.0.25</pre>	en a societar Aresta t		

Step 2: Select Wan Type.

Auto Detecting or Setup Manually.

Air Live Administratory Man Menu	-D Status	Witard	UI Athanced	2R 300Mbps Gigs Rot + Logout English
Access of the root of the sector		W WILLIAM	Con Parameters	- stopped / stopped
a Setup Wizard - WAII Type Setup				(D
is beind sustain survey slibe peints				10
R				
	(Au	to Delecting WARETyp		
	On	Aug 7/4/4 Tigte Manua	ev.	
	-3-11	1701////////////////	190	



AirLive GW-300R User's Manual





Step 3: Setup the LAN IP and WAN Type.



Step 4: Please fill in PPPoE service information which is provided by your ISP.

Step 5:

Set up your Wireless.

Example:

Air Live	-th Status	W Witard	SIL Advanced	2T2R 300Mbps Giga R + Lopout Englis
Setup Waard - WAN Settings - PPP	coar Ethernal			
LANIP Address	192.168.1	754		
Account	100.000			
· Passourd				
Primary Dist	8800			
· Secondary Drift	0.000			
PPPoE Bentce Name	1	(0050	CAR	
Assigned IP Address	0.0.0.0	(optimat)		
	> Passwort > <u>WAN</u>	> Wireless > Summ	ary a Haiabr J	Next >
Air Live		GW-3	OOR Wireless	Growalds 272R 300Mbps Giga R
	 Passwork > WAN A Statue 			(more ald be
Air Live		GW-3	OOR Wireless	Growalds 272R 300Mbps Giga R
Air Live		GW-3	OOR Wireless	Growalds 272R 300Mbps Giga R
Air Live Dunistrutory wan denu Setup Willing - Wieness settings	- Status	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Air Live Outrestructory Manuality	- Status - Enstein	GW-3	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Setup Witard - Wiveless settings • Wireless function • Network (D(SSID)	- Status © Ensitive (Sebuat	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Air Live Outrestructory Manuschu Setup Wizard - Wireless settings • Wireless function	- Status - Enstein	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Setup Witard - Wiveless settings • Wireless function • Network (D(SSID)	- Status © Ensitive (Sebuat	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Setup Witard - Wiveless settings • Wireless function • Network (D(SSID)	- Status © Ensitive (Sebuat	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Setup Witard - Wiveless settings • Wireless function • Network (D(SSID)	- Status © Ensitive (Sebuat	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Setup Witard - Wiveless settings • Wireless function • Network (D(SSID)	- Status © Ensitive (Sebuat	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Setup Witard - Wiveless settings • Wireless function • Network (D(SSID)	- Status © Ensitive (Sebuat	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Setup Witard - Wiveless settings • Wireless function • Network (D(SSID)	- Status © Ensitive (Sebuat	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis
Setup Withing Surgers Settings	- Status © Ensitive (Sebuat	GW-3 ₩ Wated	OOR Wireless	272R 300Mbps Gips R Lopout Englis

GW-300R Wireless 212R 360Mbps Gigs Router

[EXUT]



Set up your Authentication and Encryption.

GW-300R Windows 212R 300Mbps Gigg Rout and CO Advanced + Lopoid English Air Live W Witcord ADMINISTRATOR'S MAIN MENU -il Status Đ. -a Setup Wipard - Wireless Security 110071 WEP * + Security + WEP @ 54 bits O 129 bits 0 + Hay 1 0 + Key2 0 + Kay 3 0 ► Ker 4 diffure 26 for 128bits or 10 for 64 bits hexadecimal (0, 1, 2_8, 9, A, B_F) Please ci digits. < Ilacit [Start > Passanist + WAli > Wireless > Summary > Simult] fight >

W Waard

Please confirm the information below.

Dynamic IP Address

00-60-18-21-04-67

Enable

detault 11

None

-B Status

(WAN Setting) WAN Type

(Wroless Setting) Wireless

Host Name WAN's MAC Address

5510

Channel Security

Step 6:

Then click Apply Setting. And then the device will reboot. Air Live

ADDRESTRATOR'S MARI MENU

Setup Witard - Summery

Step 7: Click Finish to complete it.



3.2 System Status

Air Live		the second se		(www.airlive.c T2R 300Mbps Giga Rot	
ADMINISTRATOR'S MAIN MENU	-/in Status	W Wizard	Cill Advanced	► Logout English	~
BASIC SETTING	FORWARDING RULES	SECURITY SETTIN	G M ADVANCED SETTI	NG 120 TOOLBOX	
Primary Setup	Basic Setting				
DHCP Server Wireless Change Password	 DHCP Server The settings configuration Wireless Wireless sett Change Passy 	IN IP, and select WAN include Host IP, Sub is. tings allow you to cor	net Mask, Gateway, DNS, a Infigure the wireless configu		
	.,				

This option provides the function for observing this product's working status: WAN Port Status.

If the WAN port is assigned a dynamic IP, there may appear a "Renew" or "Release" button on the Sidenote column. You can click this button to renew or release IP manually.

Statistics of WAN: enables you to monitor inbound and outbound packets



3.3 Advanced

3.3.1 Basic Setting

Please Select "Advanced Setup" to Setup

Air Live			300R Wireless 21	2R 300Mbps Gi	
ADMINISTRATOR'S MAIN MENU	FORWARDING RULES	Wizard		1	inglish 👻
Primary Setup	Basic Setting				
DHCP Server Wireless	Primary Setup	N IP, and select WAN	tunio:		
* Change Password	 DHCP Server The settings configuration Wireless Wireless set Change Passy 	include Host IP, Subi s. tings allow you to con	net Mask, Gateway, DNS, ar figure the wireless configur		
	.,				ļ



3.3.1.1 Primary Setup – WAN Type, Virtual Computers

Press "Change"

Air Live		GW-3	OOR Wireless 272		w.airlive.c Siga Rou	
G ADMINISTRATOR'S MAIN MENU	I - All Status	Wizard	Advanced	I Logout	English	~
BASIC SETTING		SECURITY SETTING	D ADVANCED SETTING	TOOLBOX	c .	
Primary Setup	Primary Setup				[HELP]	
* DHCP Server	Item		Setting			-
* Wireless			192.168.1.254			
Change Password			IP Address Change			
	Host Name		(option	al)		
	WAN's MAC Address	00-50-18	-21-D4-57 Clone MAC			
	Renew IP Forever		le (Auto-reconnect)			
	▶ IGMP	Enab	le			
			Computers Reboo e effect until router is rebo			

This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start. LAN IP Address: the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.

Primary Setup		[HELP]
12 Item	Setting	
LAN IP Address	192.168.1.254	

WAN Type: WAN connection type of your ISP. You can click Change button to choose a correct one from the following four options:

Static IP Address: ISP assigns you a static IP address.

Dynamic IP Address: Obtain an IP address from ISP automatically.

PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services. 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



Static IP Address: ISP assigns you a static IP address:

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

ADMINISTRATOR'S MAIN MENU	J 🚽 🧐 Status	Wizard	Advanced	🕨 Logout English 🛛 👻
	S FORWARDING RULES		M ADVANCED SETTING	G LES TOOLBOX
* Primary Setup	Primary Setup	17		[HELP]
* DHCP Server	Item		Setting	9
+ Wireless	LAN IP Address		192.168.1.254	
Change Password	• WAN Type	Static IP /	Address Change	
	WAN IP Address	0.0.0.0		
	• WAN Subnet Mask	255.255.2	255.0	
-	• WAN Gateway	0.0.0		
	Primary DNS	0.0.0.0		
	Secondary DNS	0.0.0.0		
	▶ IGMP	🗌 Enab	e	
	and the second se		Computers Rebo	

Dynamic IP Address: Obtain an IP address from ISP automatically.

Host Name: optional. Required by some ISPs, for example, @Home.

Renew IP Forever: this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

ADMINISTRATOR'S MAIN MENU		W Wizard	TTING	1979.9	► Logout	English	1
	Primary Setup				-	[HELP]	7
Primary Setup DHCP Server	Item		Setting				
Wireless	LAN IP Address		2.168.1.254				
Change Password	▶ WAN Type		Dynamic IP Address Change				
	▶ HostName		(optional)				
	▶ WAN's MAC Address	ress 00-50-18-21-D4-57 Clone MAC					
-	Renew IP Forever Enable (Auto-reconnect)		nnect)				
	▶ IGMP		Enable				
	Later Contraction		Virtual Computers. n't take effect until				



PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, 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.

Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The most common MTU value is 1492.

Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on): The device will link with ISP until the connection is established.

Manually : The device will not make the link until someone clicks the connect-button in the Staus-page.

ADMINISTRATOR'S MAIN MENU	J 🦂 I Status	Wizard	Advanced	Logout	English	×
BASIC SETTING		SECURITY SETTI	IG M ADVANCED SETTIN	G TEL TOOLBOX		
* Primary Setup	Primary Setup				[HELP]	
* DHCP Server	Item		Settin	2		
* Wireless	LAN IP Address	192.16	8.1.254			
* Change Password	WAN Type	PPP ov	PPP over Ethernet Change			
	PPPoE Account					
	▶ PPPoE Password					-
	Primary DNS		0.0.0.0			-
	Secondary DNS Maximum Idle Time Connection Control		a			-
			300 seconds			-
			ect-on-demand			
	PPPoE Service Name		(optional)			-
	Assigned IP Address	0.0.0.0	0.0.0.0 (optional)			
	▶ MTU	1492	1492			-
	▶ IGMP	En En	able			
	Saved	CALL THE ALL AND	ndo Reboot ake effect until router is re	booted.		

AirLive GW-300R User's Manual



PPTP: Some ISPs require the use of PPTP to connect to their services

First, Please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.

2. Server IP Address: the IP address of the PPTP server.

3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't

want to change the password, keep it empty.

4. Connection ID: optional. Input the connection ID if your ISP requires it.

5. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Staus-page.



Primary Setup	Primary Setup	[HELP]
DHCP Server	ltem	Setting
Wireless	LAN IP Address	192.168.1.254
Change Password	• WAN Type	ppTp Change
	▶ IP Mode	Static IP Address
	My IP Address	0.0.0.0
	My Subnet Mask	255.255.255.0
	Gateway IP	0.0.0.0
	Server IP Address/Name	
	PPTP Account	
	PPTP Password	
	Connection ID	(optional)
	Maximum Idle Time	300 seconds
	Connection Control	Connect-on-demand
	► MTU	1460
	▶ IGMP	Enable
	Saved! The ch	Save Undo Reboot ange doesn't take effect until router is rebooted.

L2TP: Some ISPs require the use of L2TP to connect to their services

First, Please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

For example: Use Static

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned

to you.

2. Server IP Address: the IP address of the PPTP server.

3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't

want to change the password, keep it empty.

3. Connection ID: optional. Input the connection ID if your ISP requires it.

4. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.



Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on): The device will link with ISP until the connection is established.

Manually :The device will not make the link until someone clicks the connect-button in the Staus-page.

		TY SETTING
* Primary Setup	Primary Setup	[HELP]
* DHCP Server	Item	Setting
* Wireless	LAN IP Address	192.168.1.254
* Change Password	► 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	Connect-on-demand
	▶ MTU	1460
	▶ IGMP	Enable
		Save Undo Reboot doesn't take effect until router is rebooted.



Virtual Computers(Only for Static and dynamic IP address Wan type)

BASIC SET	TTING S FORWAR	DING RULES SECURITY SET	TING () ADVANCED SETTING	TOOLBOX
Primary Setup		nputers		[HELP]
DHCP Server		DHCP clients Select one	- Copy to ID -	- ¥
Wireless	ID	Global IP	Local IP	Enable
Change Password	1		192.168.1	
	2		192.168.1	
Allow you to. setup the one-to-	3		192.168.1.	
one mapping of multiple global IP	4		192.168.1	
address and local IP address.	5		192.168.1	() (1) (1) (1) (1) (1) (1) (1) (1) (1) (

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

Global IP: Enter the global IP address assigned by your ISP.

Local IP: Enter the local IP address of your LAN PC corresponding to the global IP address.

Enable: Check this item to enable the Virtual Computer feature.



3.3.1.2 DHCP Server

Primary Setup	DHCP Server	[HELP]
DHCP Server	Item	Setting
• Wireless	DHCP Server	O Disable 🛞 Enable
Change Password	▶ Lease Time	0 Minutes
	IP Pool Starting Address	100
	▶ IP Pool Ending Address	199
	▶ Domain Name	
	▶ 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)

Press "More>>"

DHCP Server: Choose "Disable" or "Enable."

Lease time: This is the length of time that the client may use the IP address it has been Assigned by dhcp server.

IP pool starting Address/ IP pool starting Address: Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

Domain Name: Optional, this information will be passed to the client.

Primary DNS/Secondary DNS: This feature allows you to assign DNS Servers

Primary WINS/Secondary WINS: This feature allows you to assign WINS Servers

Gateway: The Gateway Address would be the IP address of an alternate Gateway.

This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.



DHCP Client List:

DHCP Clients List			NY 14 14 14
er verset versetige ande			[HELP]
IP Address	Host Name	MAC Address	Select
192.168.1.199	airlive-WayneNB	00-16-D4-EB-06-EC	
		192.168.1.199 airlive-WayneNB	192.168:1.199 airlive-WayneNB 00-16-D4-EB-06-FC

3.3.1.3 Wireless

D ADMINISTRATOR'S MAIN MEN	IU 🚽 Status	Wizard	Advanced	Logout	English	*
	FORWARDING RULES	SECURITY SETTING		C. TOOLBOX		
Primary Setup	Wireless Setting				[HELP]	
* DHCP Server	Item		Setting			
* Wireless	▶ Wireless	In Enable ○ I	● Enable ○ Disable			
Change Password	Turn off Wireless depend as Schedule Rule	(00)Always 🗸	O Enable	Schedule Set	ting	
	Network ID(SSID)	default				
	• Wireless Mode	Mixed mode	0 11g only 0 11b only	O 11n only		1
	SSID Broadcast	Enable Disable				
	Channel	11 💌				
	▶ WDS Enter					1
	WPS	Enter				
	Security	None	~			
	Sa	ve Undo W	/ireless Client List			

Wireless settings allow you to set the wireless configuration items. Wireless : The user can enable or disalbe wireless function.

Wireless On/Off by time Schedule: The device can turn off Wireless depend as Schedule.

Network ID (SSID): Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is "default")



SSID Broadcast: The router will Broadcast beacons that have some information, including ssid so that the wireless clients can know how many ap devices by scanning function in the network. Therefore, this function is disabled, the wireless clients can not find the device from beacons.

Channel: The radio channel number. The permissible channels depend on the Regulatory Domain.

WPS (WiFi Protection Setup) WPS is WiFi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

BASIC SE	TTING S FORWARDING RULES	SECURITY SETTING
* Primar Setup	Wi-Fi Protected Setup	
* DHCP Server	Item	Setting
* Wireless	• WPS	Inable O Disable
Change Password	▶ Setup	Current AP PIN Configure Wireless Station
	Current PIN of the device	16842830 Generate New PIN
	• WPS state	Idle
	• WPS status	Configured Release
	Saved! T	Save Trigger Back Reboot The change doesn't take effect until router is rebooted.

WDS(Wireless Distribution System)

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement. Hybrid Mode

It means the device can support WDS and AP Mode simultaneously.



ADMINISTRATOR'S MAIN M	IENU 🥠 Status	Wizard	Advanced	▶ Logout English
	ING 🙁 FORWARDING RULES	SECURITY SETTING	(D) ADVANCED SETTING	TOOLBOX
Primary Setup	U WDS Setting [HELF			[HELP]
* DHCP Server	Item	Setting		
Wireless	AP Mode:	AP Only 💌		
Change Password It is a system that enables the interconnection of access points wirelessly.	Remote AP MAC MAC 1			
	MAC 2			
	MAC 3			
	MAC 4			
	Scaned AP's MAC Select one Copy to Copy to			
	SSID	1		MAC Address
	CL-WLAN		1 00-	1A-1E-C6-5C-90
	CL-GUEST		1 00-	1A-1 <mark>E-C6-</mark> 5C-91
	wmu6500		1 00-	4E-67-03-E0-29
	Air3G_Sam		1 00-	4F-62-2A-06-4C
	CL-WLAN	1	1 00-	1A-1E-8B-95-C1

Security: Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another.

There are several security types to use:

WEP :

When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.

802.1X

Check Box was used to switch the function of the 802.1X. When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service. RADIUS Server

IP address or the 802.1X server's domain-name.

RADIUS Shared Key

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

AirLive GW-300R User's Manual



BASIC SETTIN	G 🥺 FORWARDING RULES 😒	SECURITY SETTING		
Primary Setup	Wireless Setting	[HELP]		
DHCP Server	Item	Setting		
* Wireless	• Wireless	● Enable ○ Disable		
Change Password	Turn off Wireless depend as Schedule Rule	(00)Always 🗸 🔿 Enable 💿 Disable Schedule Setting		
	Network ID(SSID)	default		
	• Wireless Mode	Mixed mode ○ 11g only ○ 11b only ○ 11n only		
	SSID Broadcast	Enable Disable		
	Channel	11 💌		
	• WDS	Enter		
	• WPS	Enter		
	Security	802_1x and RADIUS		
	Encryption Key Length	64 bits 0 128 bits		
	RADIUS Server IP	0.0.0.0		
	▶ RADIUS port	1812		
	RADIUS Shared Key			

WPA-PSK

1. Select Encryption and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of pre-share key is from 8 to 63.



2. Fill in the key, Ex 12345678

BASIC SE	TTING 🥺 FORWARDING RULES 😒	SECURITY SETTING MI ADVANCED SETTING
Primary Setup	Wireless Setting	[HELP]
DHCP Server	Item	Setting
Wireless	• Wireless	
Change Password	Turn off Wireless depend as Schedule Rule	(00)Always 🗸 🔿 Enable 💿 Disable Schedule Setting
	Network ID(SSID)	default
	• Wireless Mode	Mixed mode ○ 11g only ○ 11b only ○ 11n only
	SSID Broadcast	Enable Disable
	Channel	11 💌
	+ WDS	Enter
	• WPS	Enter
	Security	WPA-PSK
	Encryption	© TKIP ◯ AES
	Preshare Key Mode	ASCII 💌
	Preshare Key	(*************************************

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits If ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA2-PSK(AES)

1. Select Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits If ASCII, the length of Pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678



WPA2(AES)

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service. RADIUS Server

IP address or the 802.1X server's domain-name.

Select RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK /WPA2-PSK

The router will detect automatically which Security type the client uses to encrypt.

1. Select Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678

BASIC SE	TTING S FORWARDING RULES	ECURITY SETTING
• Pringhey Setup	Wireless Setting	[HELP
* DHCP Server	Item	Setting
* Wireless	▶ Wireless	●Enable ○Disable
Change Password	Turn off Wireless depend as Schedule Rule	(00)Always 🗸 🔿 Enable 💿 Disable Schedule Setting
	Network ID(SSID)	default
	• Wireless Mode	Mixed mode ○ 11g only ○ 11b only ○ 11n only
	 SSID Broadcast 	⊙Enable ○Disable
	▶ Channel	11 💌
	▶ WDS	Enter
	▶ WPS	Enter
	Security	WPA-PSK/WPA2-PSK
	Encryption	TKIP + AES
	Preshare Key Mode	ASCII 💌
	Preshare Key	



WPA/WPA2

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service. RADIUS Server

The router will detect automatically which Security type(Wpa-psk version 1 or 2) the client uses to encrypt.

IP address or the 802.1X server's domain-name.

Select RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

Wireless Client List

1	TOR'S MAIN MENU	-ii Status	Wizard	Advanced	Logout English	×
² € ⊘	BASIC SETTING				TOOLBOX	
* Primary Setup		Wireless Client List				
* DHCP Server		Connected	I Time1	MAC A	ddress	
* Wireless			Back	Refresh		
• Change Passw	ord					

3.3.1.4 Change Password

O ADMINISTRATOR'S MAIN MEN	ili 🚽 Status	Witard	Cil Advanced	➤ Logout	English	۲
DASIC SETTIN	CORWARDING RULLS	C SECURITY SETTING			1	
Primary Setup	Change Password			- MAI		1
* DRCP Server	Item		Setting			
* Wireless	+ Old Password	1				
Change Password	New Password					1
	+ Reconfirm					
		Save	Undo			

You can change Password here. We strongly recommend you to change the system password for security reason.



3.3.2 Forwarding Rules

FORWARDING RULES					
	SECURITY SETTING		12 TOOLBOX		
Forwarding Rule	95				
Virtual Serve	er.				
000 1000 F 1000 F 1000 F 1000		and other services on your	LAN.		
 Special Appl 	ication				
		lications to connect, and wo	ork with the		
 Miscellaneou 	IS				
		and the second of the second			
	and the second second second second				
		nction, the router will work w	vith UPnP		
	 Virtual Serve Allows othe Special Appli This configu NAT router. Miscellaneou IP Address way communeeded. Non-standa an FTP sen UPnP Settir 	 Special Application This configuration allows some app NAT router. Miscellaneous IP Address of DMZ Host: Allows a co-way communication. Note that, this f needed. Non-standard FTP port: You have to an FTP server whose port number is 	 Virtual Server Allows others to access WWW, FTP, and other services on your Special Application 	 Virtual Server Allows others to access WWW, FTP, and other services on your LAN. Special Application This configuration allows some applications to connect, and work with the NAT router. Miscellaneous IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed. Non-standard FTP port: You have to configure this item if you want to access an FTP server whose port number is not 21 (when Client uses active mode). UPnP Setting: If you enable UPnP function, the router will work with UPnP 	 Virtual Server Allows others to access WWW, FTP, and other services on your LAN. Special Application This configuration allows some applications to connect, and work with the NAT router. Miscellaneous IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed. Non-standard FTP port. You have to configure this item if you want to access an FTP server whose port number is not 21 (when Client uses active mode). UPnP Setting: If you enable UPnP function, the router will work with UPnP

3.3.2.1 Virtual Server

BASIC SETTING	Res FC	RWARDING RULES	SECU	RITY SETTING	TE ADV	ANCED SETT	ING Lee	TOOLBOX
Virtual Server	ö Virtu	al Server						[HELP]
Special AP				vices - selec (e (00)Always		y to ID	~	
	ID	Server IP	8	Service P	orts	Protocol	Enable	Schedule Rule#
	1	192,168,1				Both 🐱		0
	2	192.168.1				Both 💌		0
	3	192.168.1				Both 💌		0
	4	192.168,1.				Both 💌		0
	5	192,168.1				Both 📝		0
	6	192,168,1				Both 🐱		0
	7	192.168.1.				Both 💌		0
	8	192.168.1.	1			Both 👻		0
	9	192.168.1.				Both 🐱		0
	10	192.168.1				Both 👻		0



This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP. Virtual Server can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

3.3.2.2 Special AP

BASIC :		ARDING RULES	ECURITY SETTING	TOOLBOX
Virtual Server	😐 Special	Applications		[HELP]
Special AP		Popular applic	ations Select one 👻 Copy to ID	~
• Miscellaneous	ID	Trigger	Incoming Ports	Enable
	1		-	
	2			
	3			
	4			
	5			
	6			
	7			
	8			

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The Special Applications feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

Trigger: the outbound port number issued by the application..

Incoming Ports: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

This product provides some predefined settings Select your application and click Copy to to add the predefined setting to your list.

Note! At any given time, only one PC can use each Special Application tunnel.

AirLive GW-300R User's Manual

3.3.2.3 Miscellaneous Items

ADMINISTRATOR'S M		Wizard C Advanced	Logout English Logout English Logout English
Virtual Server	Miscellaneous Items		
Special AP	Item	Setting	Enable
Miscellaneous	▶ IP Address of DMZ Host	I192.168.1	
	 Super DMZ(IP Passthrough) 	0	- 3
	Non-standard FTP port		6
	▶ UPnP setting		
	Xbox Support		
		Save Undo	11

IP Address of DMZ Host

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.

Super DMZ (IP Passthrough)

Super DMZ (IP Passthrough) is a useful feature if a host computer or server on the Local Area Network needs to have access into it 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

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

Xbox Support

The Xbox is a video game console produced by Microsoft Corporation. Please enable this function when you play games.



UpnP Setting

The device also supports this function. If the OS supports this function enable it, like Windows Xp. When the user get ip from Device and will see icon as below:



3.3.3 Security Settings

ADMINISTRATOR'S MAIN MENU	📲 Status	Wizard	Cill Advanced	▶ Legout Englis
	S FORWARDING RULES			TOOLBOX
Packet Filters	Security Setting	ig		
Domain Filters	Packet Filte			
* URL Blocking	C. 7350. P. 640.55	19748	twork by analyzing the incon	ning and
Internet Access Control	outgoing p	ackets and letting them p	ass or halting them based (
Miscellaneous		f the source and destinati	on.	
	Domain Filt Let you pr		vice from accessing specific	URIS
	URL Blockin			
	- URL Block	ring will block LAN compu	iters to connect to pre-define	d websites.
	Internet Ad	dress Control		
	Concernment and	research the second	MAC Control" for specific MA	DESCROPTION STREET
			tion. It also provides 3 featur o MAC Control and Interface	
	Classical States of the states	pend as user-defined tim		
	Miscellane	ous		
	the suprover and		eral, only Intranet user can bi	and the second se
		b pages to perform admir dministration task from re	nistration task. This feature e	enables you to
			t of time of inactivity before th	ne device will
	with the second s		or session. Set this to zero to	
	⁻ Discard P	ING from WAN side; When	n this feature is enabled, ho	sts on the
	WAN cann	iot ping the Device.		



3.3.3.1 Packet Filters

ADMINISTRATOR'S MAIN ME	NU	- Status	W v	Vitard	Cil Advanced		Logout	English
BASIC SETTIN	a 😪 ra	RWARDING RULES	(=) SECUR	ITY SETTING			TOOLBOX	
Packet Fillers	O Outb	aund Packet Filter						[HELP]
Domain Filters	1	Item			Set	ting		
IRL Blocking	+ Outbo	and Filter		Enable				
nternet Access Control	1.) Allow all to pass e) Deny all to pass e	10. A 10					
Viscellaneous			Bi	ick List 🗔 🖛 S	electione 💌			
	ID	Source IP		Dest	ination IP : Ports	Enable	Schedu	le Rule#
			1	1	11	1 10	1A	
	1						0	
	1		=	-	1		0	
	-							
	2] []	0	
	2 3						0	
	2 3 4						0	
	2 3 4 5						0	

Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

Allow all to pass except those match the specified rules

Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

Source IP address

Source port address

Destination IP address

Destination port address

Protocol: TCP or UDP or both.

Use Rule#



For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, 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. An empty implies all port addresses. Packet Filter can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

Each rule can be enabled or disabled individually.

Inbound Filter:

To enable Inbound Packet Filter click the check box next to Enable in the Inbound Packet Filter field.

Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

Example 1:

Contract Service	116 S 7	ORWARDING AULES (T) SEC	URITY SETTING	(n) ADVANCED SET	THIS IL	100150X	
Packet Filters	O Out	bound Packet Filter				[HELP]	
Domain Filters	1	llem		Setting			
URL Blocking	Outbound Filter		Enable	Enable			
Internet Access Control		Allow all to pass except thos Deny all to pass except thos		and the second se			
Miscellaneous			Block List - sel	ect one - 💌 Copy to D -			
	iÓ	Source IP	Destin	ation IP : Ports	Enable	Schedule Rule#	
	1	1.2.3.100-1.2.3.149		25-100		0	
	2	123.10-123.20				0	
	3					0	
	4			10		0	
	5	6				0	
		1		H		0	
	6			11	B	0	
	6 7				1 0 1	V .	

(1.2.3.100-1.2.3.149) Remote hosts are allow to send mail (port 25), and browse the Internet (port 80)

(1.2.3.10-1.2.3.20) Remote hosts can do everything (block nothing) Others are all blocked.

AirLive GW-300R User's Manual



Example 2:

R Constant	NG 🔇 N	SRWARDING RULLS	IRITY SETTING	TO ADVANCED SET	11100	TUOLIICK	
Packet Filters	Out	ound Packet Filter				[HELP]	
Domain Filtera		Item		Setting			
· URL Blocking	+ Outbo	 Outbound Filter 		Enable			
Internet Access Control		Allow all to pass except thos Deny all to pass except thos		The second s			
* Miscellaneous			Block List – se ule (00)Atways	lect one - 💌 Copy to ID			
	ID	Source IP	Destin	nation IP : Ports	Enable	Schedule Rule#	
	1 C	1.2.3.100-1.2.3.199	1	21		0	
	2	1.2.3 100-1.2.3 199		199		0	
	100 million 100			11		0	
	3						
	4			1		0	
	_					0	
	4						
	4					0	

(1.2.3.100-1.2.3.119) Remote hosts can do everything except read net news (port 119) and transfer files via FTP (port 21) behind Router Server. Others are all allowed.

After Inbound Packet Filter setting is configured, click the save button.

Outbound Filter:

To enable Outbound Packet Filter click the check box next to Enable in the Outbound Packet Filter field.



Example 1:

Router LAN IP is 192.168.12.254

BASIC SETT	ING 🔗 FO	ORWARDING RULES SEC	URITY SETTING	M ADVANCED SET	TING	TOOLBOX
Packet Filters	 Outb 	oound Packet Filter				[HEL
Domain Filters		Item		Sett	ting	
URL Blocking	> Outbo	und Filter	🖉 Enable	1		
Internet Access Control		Allow all to pass except tho Deny all to pass except tho:				
Miscellaneous			Lotter bits terres	select one 💌 s 👻 Copy to 🛛 ID	~	
	ID	Source IP	Dest	tination IP : Ports	Enable	Schedule Rule
	1	100-192.168.12.149		21-100		0
	2	2.10-192.168.12.20				0
	3			-		0
	4					0
	5			1		0
	1					0
	6					
	6 7					0

(192.168.12.100-192.168.12.149) Located hosts are only allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.12.10-192.168.12.20) Located hosts can do everything (block nothing) Others are all blocked.



Example 2: Router LAN IP is 192.168.12.254

BASIC	SETTING 🥺 FO	DRWARDING RULES SE	CURITY SETTING	Advanced	тіна 🔃	TOOLBOX	
Packet Filters	Outb	ound Packet Filter				[HELF	P]
Domain Filters		Item Setting					
URL Blocking	Outbo	und Filter	-				
Internet Access Contro		Allow all to pass except the Deny all to pass except the		-			
Miscellaneous			Block List s	elect one 👻	- >		
	ID	Source IP	Desti	nation IP : Ports	Enable	Schedule Rule#	6
	1	192.168.12.100		:21		0	
	2	192.168.12.199		; 119		0	
	3					0	
	1941 - 19						-
	4			+		0	
						0	_
	4				-1. 27-26		-
	4					0	

(192.168.12.100 and 192.168.12.119) Located Hosts can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

After Outbound Packet Filter setting is configured, click the save button.



3.3.3.2 Domain filters

and the second s	10 S (1	COMPANYING MALES (2) BC	UNITY SETTING	CONTRACTOR STATES	16	other
· Parket Filtery	G Dom	an filter				THEFAL
- Duman Filtura		Ham		Setting	ř.	
Citil Bocking	+ Doma	un Filter	🗑 Enable			
* Rolenter Access Control	+ Log D	Has Query	🛄 Enjabre			
· Miscellarienus	+ Privile	ige IP Addresses Range	From 1	Tp 10		
	ID.	Domain Suffix		Action	Enable	Schedule Rule#
	1	www.syz.cem		Drop DLog	단	0
	3			Dires Dies		0
	3					D
	4			Drop DLog	D	0
				Drop DLog		D
	.6		1.	Drop Log		0
	7			COrop Clog		D
		1		Drop DLog		0
				Drop DLog	D	0
	10	* (all others)		Drop DLop	1.00	0

Domain Filter

Let you prevent users under this device from accessing specific URLs.

Domain Filter Enable

Check if you want to enable Domain Filter.

Log DNS Query

Check if you want to log the action when someone accesses the specific URLs.

Privilege IP Addresses Range

Setting a group of hosts and privilege these hosts to access network without restriction.

Domain Suffix

A suffix of URL to be restricted. For example, ".com", "xxx.com".

Action

When someone is accessing the URL met the domain-suffix, what kind of action you want. Check drop to block the access. Check log to log these access.

Enable

Check to enable each rule.



Example:

BASIC SET	TING 🤣 FI		RITY SETTING	D ADVANCED SETTIN	G 10 ТО	OLBOX
Packet Filters	Dom	ain Filter	-			[HELP]
Domain Filters		Item		Setting	1	
URL Blocking	► Dom	ain Filter	Enable			
Internet Access Control	Log E	NS Query	Enable			
Miscellaneous	Privile	ege IP Addresses Range	From 100	To 199		
	ID	Domain Suffix		Action	Enable	Schedule Rule#
	1	www.msn.com		Drop Log		0
	2	www.sina.com		Drop Log		0
	3	www.baidu.com				0
	4		11			0
	5					0
	6					0
	7					0
	8					0
	9		1			0
	10	* (all others)		Drop Log	3	0

In this example:

URL include "www.msn.com" will be blocked, and the action will be record in log-file. URL include "www.sina.com" will not be blocked, but the action will be record in log-file. URL include "www.baidu.com" will be blocked, but the action will not be record in log-file. IP address x.x.x.1~x.x.x99 can access Internet without restriction.



3.3.3.3 URL Blocking

HASIC SET	1005 😪 1	ORIVARDING RULES (2) SECUR	ITY SETTING	C ADVANCED SETTING	125,000	ALING R
Packet Filters	O. URL	Blocking	17			[HELP]
Domain Filtera		Item		Setting		
URL Blocking	• URL	Blocking	Enabl	e.	2.5	
Internet Access Control	ID	1	URL		Enable	Schedule Rule#
Miscellaneous	1					0
	2				13	0
	э					0
	4				E	0
	5				D	0
	6					0
	. 7.					0
	8					0
	9					D
	10					0

URL Blocking will block LAN computers to connect to pre-defined Websites. The major difference between "Domain filter" and "URL Blocking" is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a keyword.

URL Blocking Enable

Checked if you want to enable URL Blocking.

URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

Enable

Checked to enable each rule.



De Basic set	rting. 🧐 FOI	INVARIONG RULES	URITY SETTING	ADVANCED SETTING	(Correction)	LBGX
Pecket Fillers	O URL B	locking	- 15			[HELP]
- Domain Filters		item		Setting		
URL Blocking	IURL B	ocking	Enable	8		
· Internet Access Control	1D		URL		Enable	Schedule Rule#
Miscellaneoux	1	man				0
	2	sina			1	0
	3					0
	4)		0
	5				E3	0
	6					0
	7					0
	0					0
	9	6				0
	10					0

In this example:

- 1. URL include "msn" will be blocked, and the action will be record in log-file.
- 2. URL include "sina" will be blocked, but the action will be record in log-file

3.3.3.4 Internet Access Control

The device provides "Administrator MAC Control" for specific MAC to access the device or Internet without restriction. It also provides 3 features to access Internet: MAC Control by host, Group MAC Control and Interface Access Control depend as user-defined time Schedule.

Administrator MAC Control

Regardless the MAC access configuration of administrator, specific MAC can access the device.

BASIC SETT	IIG 🥺 FORWARDING RULE	S 🗇 SECURITY SETTING 🕤 ADVANCED SETT	ING TOOLROX
Packet Filtera	G Administrator MAC C	ontrol	[HELD]
Domain Filters	DHCP clients 00	0-15-D4-EB-05-FG - 192,158 123 151 (autive-nb) 💌	Copy to ID 1 💌
URL Blocking	D	MAC Address	Enable
Internet Access Control	91	00-15-D4-EB-06-FC	2
Miscellanzous	2		
	3		
		Save Undo	



This device can record 3 sets. When the host(should be admin) logins Web management, the device will record MAC address of this host. Before this host configures Internet Access Control, Suggest end-user to enable this feature, first.

ltem	Setting	
 Access Control Type 	MAC Access Control Group MAC Access Control Interface Access Control	

MAC control

ADMINISTRATOR'S MAIN		-II Status	Wizard	Advanced	1	Logo	ti.	4911	
				10		112202.0			
Packet Filters	O MA	C Address Control	97				[H	ELP]	
Domain Filters		Item		Setting					
URL Blocking	MAC Address Control		Enable						
Internet Access Control		nection control		clients with C checked c		to th	is device;	and	
Miscellaneous		mecaon control	allow 🚩 unspecifie	ed MAC addresses to co	nnect.				
			Wireless clients with	A checked can associa	ate to the w	reles	ss LAN; ar	nd	
	Ass	ociation control		ed MAC addresses to as ontrol has no effect on		ts.			
	Ass	DHCP clients		ontrol has no effect on	wired clien	v			
	ID	DHCP clients	Note: Association co	ontrol has no effect on	wired clien	~	Schedule	Rule#	
		DHCP clients Si	Note: Association co	s V Copy to ID -	wired clien	~	Schedule 0	Rule#	
	iD	DHCP clients Si	Note: Association co	IP Address	vired clien	 ✓ A 		Rule#	
	ID 1	DHCP clients Si	Note: Association co	Copy to ID IP Address 192.168.1	vired clien	✓ A	0	Rule#	

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

MAC Address Control Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.

Connection control Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or AirLive GW-300R User's Manual 49



deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device. Association control Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN. Control table

a	MAC Address	IP Address	С	A	Schedule Rule#
1		192.168.1			0
2 3?		192.168.1.			0
3		192.168.1			0
4		192.168.1.			0

"Control table" is the table at the bottom of the "MAC Address Control" page. Each row of this table indicates the MAC address and the expected IP address mapping of a client. There are four columns in this table:

MAC Address	MAC address indicates a specific
	client.
IP Address	Expected IP address of the
	corresponding client. Keep it empty
	if you don't care its IP address.
С	When "Connection control" is
	checked, check "C" will allow the
	corresponding client to connect to
	this device.
A	When "Association control" is
	checked, check "A" will allow the
	corresponding client to associate
	to the wireless LAN.



In this page, we provide the following Combobox and button to help you to input the MAC address.

		-			_	
DHCP clients	select one	•	Copy to	\mathbb{D}		-

You can select a specific client in the "DHCP clients" Combobox, and then click on the "Copy to" button to copy the MAC address of the client you select to the ID selected in the "ID" Combobox.

Previous page and Next Page To make this setup page simple and clear, we have divided the "Control table" into several pages. You can use these buttons to navigate to different pages.

Example:

le-s	l an		1000 000000000000000000000000000000000	Cil Advanced			Ť	
BASIC SETT	TING 😪	FORWARDING RULES	SECURITY SETTING	ADVANCED SETTING	160	TOOL	BOX	<u> </u>
Packet Filters	D MA	C Address Control					, 1944 1977 1977 1977	[HELP]
Domain Filters	Item MAC Address Control			Setting				
URL Blocking			Enable					
Internet Access Control	Rea	nnection control	Wireless and wired o	lients with C checked can co	onnect	to thi	s devic	e; and
Miscellaneous		mection control	allow 🚩 unspecifie	d MAC addresses to conne	ct			
			The second of the second secon					
	Ass	sociation control	deny 🔽 unspecifie	A checked can associate to d MAC addresses to associ ntrol has no effect on wire	iate.		ss LAN;	and
	As	DHCP clients	deny vunspecifie Note: Association co Select one	d MAC addresses to assoc	iate. d clien		s LAN;	and
	ID Ass	DHCP clients	deny vunspecifie Note: Association co Select one	d MAC addresses to assoc ntrol has no effect on wire	iate. d clien	v		and ule Rule#
		DHCP clients	deny vinspecifie Note: Association co Select one nedule rule (00)Always	d MAC addresses to assoc ntrol has no effect on wire Copy to ID V	iate. d clien	v		
	ID	DHCP clients Sch MAC Address	deny vunspecifie Note: Association co Select one nedule rule (00)Always	d MAC addresses to associ ntrol has no effect on wire Copy to ID	iate. d clien	×	Schedi	
	10	DHCP clients Sch MAC Address	deny vunspecifie Note: Association co Select one nedule rule (00)Always	d MAC addresses to associ ntrol has no effect on wire Copy to ID V IP Address 192.168.1.100	iate d clien C	A V	Schedi	

In this scenario, there are three clients listed in the Control Table. Clients 1 and 2 are wireless, and client 3 is wired.

1. The "MAC Address Control" function is enabled.

2."Connection control" is enabled, and all of the wired and wireless clients not listed in the "Control table" are "allowed" to connect to this device.

AirLive GW-300R User's Manual



3."Association control" is enabled, and all of the wireless clients not listed in the "Control table" are "denied" to associate to the wireless LAN.

4.Clients 1 and 3 have fixed IP addresses either from the DHCP server of this device or manually assigned:

ID 1 - "00-12-34-56-78-90" --> 192.168.1.100 ID 3 - "00-98-76-54-32-10" --> 192.168.1.101

Client 2 will obtain its IP address from the IP Address pool specified in the "DHCP Server" page or can use a manually assigned static IP address.

If, for example, client 3 tries to use an IP address different from the address listed in the Control

table (192.168.12.101), it will be denied to connect to this device.

5.Clients 2 and 3 and other wired clients with a MAC address unspecified in the Control table are all allowed to connect to this device. But client 1 is denied to connect to this device.

6.Clients 1 and 2 are allowed to associate to the wireless LAN, but a wireless client with a MAC address not specified in the Control table is denied to associate to the wireless LAN. Client 3 is a wired client and so is not affected by Association control.

Group MAC Access Control

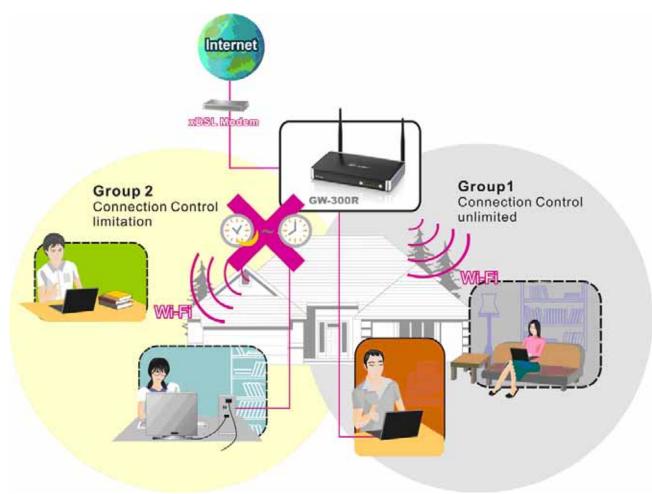
Administrator can define hosts in which Group to allow Internet. For example, Father and Mother are in Group1 without limitation and hosts Brother and Sister are in Group2 to access according as Schedule Rule2.



For example,

Schedule Rule 1 sets "always" everyday with limitation.

ADMINISTRATOR'S MAIN MEN	U -11 Status	Wizard	Advanced	Logout	English
	FORWARDING RULES	SECURITY SETTING	C ADVANCED SETTING		ĸ
Packet Filters	Group MAC Access Contro	bl			[HELP]
Domain Filters	Item		Setting		
* URL Blocking	Group MAC Access Control	Enable			
Internet Access Control		Save	Undo		
Miscellaneous	Add Member to Group List	È			
	Add MAC Address -	1 and apply sched		Add	
	Group List 1 - Always activ	/e.			_
	MAC Address	Host	Name	P Address	Action
	00-16-D4-EB-06-FC	airlive-W	/ayneNB 19	92.168.1.199	Delete



AirLive GW-300R User's Manual



Interface Access Control

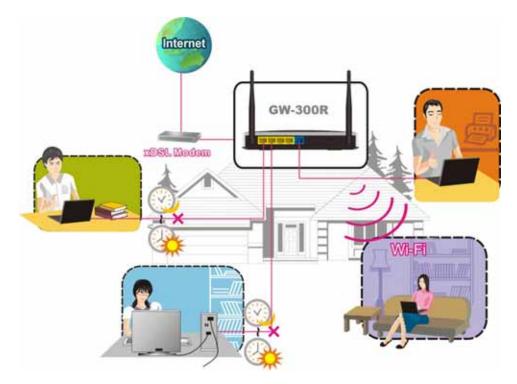
The device defines 5 Interfaces as Lan1,Lan2, Lan3,Lan4 and WiFi. The device allows different interface to access Internet by time schedule For example, Schedule Rule 1 sets "always" everyday with limitation.

Schedule Rule 2 sets 08:00~23:00 Monday ~ Friday.

Administrator can set guests in Lan3 and Lan4 to access Internet according as Schedule Rule

2. Set Friends in Lan1 ,Lan2 and WiFi according as Schedule Rule 1.

BASIC SETT	ING 😪 FORWARDING RULES	S SECURITY SETTING	D ADVANCED SETTING	TOOLBOX
Packet Filters	u Interface Access Control			[HELP]
Domain Filters	Item		Setting	
· URL Blocking	Interface Access Control	E Enable		
Mitemet Access Control	interface	Sch	edule Rule	Deny
Miscellaneous	Pod 1	(00)Always 👱	M
	Port 2	(00))Always 🐱	2
	Port 3	(00	Mways 🐱	2
	Port 4	100	Always 💌	2
	Wireless	(00)	Always 👻	R





3.3.3.5 Miscellaneous Items

ADMINISTRATOR'S MAIN MEN	10 - di Status	Wizard	Advanced	▶ Logout	English	5
BASIC SETTING	S CRWARDING RULES	SECURITY SETTING	ADVANCED SETTING	TOOLBOX	1	
Packet Filters	 Miscellaneous Items 				[HELP]]
Domain Filters	Item		Setting		Enable	
URL Blocking	Remote Administrator Host	Port 0.0	0.0 / 88			
Internet Access Control	Administrator Time-out 600 seconds (0 to disable)			в)		
Miscellaneous	Discard PING from WAN side					
	▶ SPI mode					
	DoS Attack Detection					
	VPN PPTP Pass-Through				4	
	VPN IPSec Pass-Through		~	1		
		Save	Undo			

Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. 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. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 88. You can change web server port to other port, too.

Administrator Time-out

The time of no activity to logout automatically. Set it to zero to disable this feature.

Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

SPI Mode

When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

DoS Attack Detection

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.



VPN IPSec Pass-Through

It is a setting/feature on routers which is required to implement secure exchange of packets at

the IP layer and allow IPSec tunnels to pass through the router.

VPN PPTP Pass-Through

It is a setting/feature on routers which is required in order to connect to a Remote PPTP VPN account.

3.3.4 Advanced Settings

1000				16 Million 10
BASIC SETTING	FORWARDING RULES		M ADVANCED SETTING	100LBOX
* System Time	Advanced Sett	ing		
* System Log		.e.v.		
* Dynamic DNS	 System Tim Allow you t 		y or consult network time fro	m NTP
* QoS Rule	server.			
* SHMP	 System Log 			
* Routing	 Send system Dynamic DN 		or email to specific receipt	s.
Schedule Rule	- To host yo		address, you have to use o	lynamic
	Scatter Course Course	Service can provide differen ee a certain level of perform	nt priority to different users o mance:	or data flows,
		er the capability to remote g terminal values and mon	ly manage a computer netw itoring network events.	vork by polling
	Routing			
	routing tab		d subnets, you may want to proper routing path and allo other.	
	Schedule Ri	ule		
	- Apply sche	edule rules to Packet Filter	s and Virtual Server.	

3.3.4.1 System Time

D ADMINISTRATOR'S MA	AIN MENU - 🗐 Stat	itus 😾 Wizard 🖓 Advanced 🔹 Logout English 💌
BASIC	SETTING	ILES C SECURITY SETTING
 System Time 	G System Time	[HELP]
System Log	Item	Setting
Dynamic DNS	System Time	Friday, December 17, 2010 5:28:18 PM
QoS Rule	▶	me by NTP Protocol Sync Now!
SNMP	Time Server	time.nist.gov
Routing	Time Zone	(GMT-08:00) Pacific Time (US & Canada)
Schedule Rule	Set Date and Time	me using PC's Date and Time
	PC Date and Tin	ne Friday, December 17, 2010 5:28:19 PM
	► O Set Date and Tin	me 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
	Start	Month : Jan 💌 Day : 01 💌 Hour : 00 💌
	End	Month : Jan 👻 Day : 01 🖌 Hour : 00 🖌
		System Time is: Fri Dec 17 17:28:10 2010 Save Undo

Get Date and Time by NTP Protocol

Selected if you want to Get Date and Time by NTP Protocol.

Time Server

Select a NTP time server to consult UTC time

Time Zone

Select a time zone where this device locates.

Set Date and Time manually

Selected if you want to Set Date and Time manually.

Set Date and Time manually

Selected if you want to Set Date and Time manually.

Function of Buttons

Sync Now: Synchronize system time with network time server

Daylight Saving:Set up where the location is.



3.3.4.2 System Log

DASIC SE	FORWARDING RULES	SECURITY SETTING	OOLBOX
System Time	System Log		[HELP]
System Log	Item	Setting	Enable
Dynamic DNS	► IP Address of Syslog Server	192.168.1	
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 	

This page support two methods to export system logs to specific destination by means of syslog(UDP) and SMTP(TCP). The items you have to setup including:

IP Address for Syslog

Host IP of destination where syslogs will be sent to.

Check Enable to enable this function.

E-mail Alert Enable

Check if you want to enable Email alert (send syslog via email).

SMTP Server IP and Port

Input the SMTP server IP and port, which are concated with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

Send E-mail alert to

The recipients who will receive these logs. You can assign more than 1 recipient, using ';' or

',' to separate these email addresses.



3.3.4.3 DDNS Service

	SETTING CONVARIANG RULES	CO RECEIPTING CO ADVANCED SETTING
Byatem Time	G Dynamic DHS	(HELP
System Log	Rem	Setting
Dynamic DIES	+ DDNS	Disable DEnable
Gos Rule	 Provider 	DynDN4S.org/Dynamic: 💌 Provider website
SNMP	 HostName 	
Nouting	+ Username / E-mail	
Schedule Rule	+ Password/Key	

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable Dynamic DNS, you need to register an account on one of these Dynamic DNS servers that we list in provider field.

To enable Dynamic DNS click the check box next to Enable in the DDNS field. Next you can enter the appropriate information about your Dynamic DNS Server. You have to define:

Provider

Host Name

Username/E-mail

Password/Key

You will get this information when you register an account on a Dynamic DNS server.



3.3.4.4 SNMP

ADMINISTRATOR'S MAIN ME		Wizard	Cil Advanced		English
BASIC SETTIN	IG 🥺 FORWARDING RULES	SECURITY SETTING	ADVANCED SETTING	1 tooleox	
System Time	C SNMP Setting	- 1. - 1.			[HELP]
* System Log	Item		Setting		
* Dynamic DNS	Enable SNMP	Local Remote	9		
* QoS Rule	Get Community	public			
* SNMP	Set Community	private			
* Routing	• IP 1				
Schedule Rule	• IP 2				
	• IP 3				
	▶ IP 4				
	SNMP Version	© V1	112		
		Save	Undo		

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Enable SNMP

You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote 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, IP 2, IP 3, IP 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.



3.3.4.5 Routing

BASIC S		FORWARDING RULES		ADVANCED SETTING	C TOOLBOX	
 System Time 	O Rot	iting Table	117			[HELP]
System Log		Item		Setting		
Dynamic DNS	Dyna	amic Routing	⊙ Disable ○ RIPv1 C) RIPv2		
QoS Rule	Stati	c Routing	💿 Disable 🔘 Enable			
* SNMP	ID	Destination	Subnet Mask	Gateway	Нор	Enable
Routing	1			ļ []		
Schedule Rule	2					
	3					
	4					
	5					
	6					
	7					
	8					

Routing Tables allow 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.

Routing Table settings are settings used to setup the functions of static.

Dynamic Routing

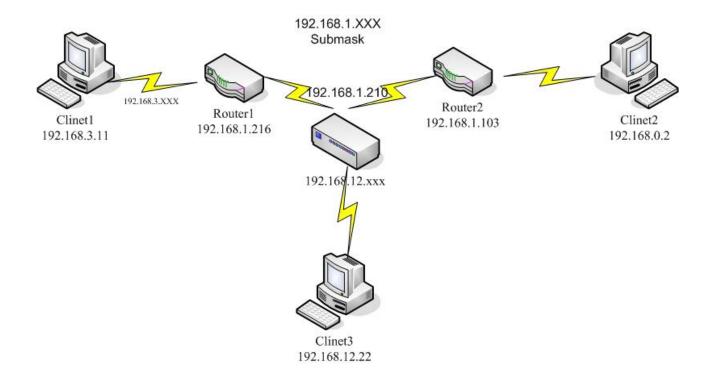
Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network.

Otherwise, please select RIPv1 if you need this protocol.

Static Routing: 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.



Example:



Configuration on NAT Router

Destination	SubnetMask	Gateway	Нор	Enabled
192.168.3.0	255.255.255.0	192.168.1.216	1	v
192.168.0.0	255.255.255.0	192.168.1.103	1	v

So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.1.103 (a gateway), And if it sends Packets to 192.168.3.11 will go via 192.168.1.216 Each rule can be enabled or disabled individually. After routing table setting is configured, click the save button.

3.3.4.6 Schedule Rule

ADMINISTRATOR'S MA	IN MENU	🚽 i Status	Wizard	Advanced	▸ Logout	English	1
BASIC S		ARDING RULES		ADVANCED SETTIN		¢.	
 System Time 	🔍 Schedu	le Rule				[HELP]	
 System Log 		Item		Setting			
 Dynamic DNS 	Schedule		Enab	Enable			
* QoS Rule	Rule#		Rule Name		Action		
* SNMP	16		Save Add	New Rule			
 Routing 							-
Schedule Rule							

You can set the schedule time to decide which service will be turned on or off. Select the "enable" item.

Press "Add New Rule"

You can write a rule name and set which day and what time to schedule from "Start Time" to "End Time". The following example configure "ftp time" as everyday 14:10 to 16:20

ADMINISTRATOR'S MAIN M	IENU 🚽 Status	Wizard 1 Advanced	I I Logout English
BASIC SETT	ING 🥺 FORWARDING RULES		SETTING
System Time	Schedule Rule Setting		[HELP]
System Log	Item	S	etting
Dynamic DNS	Name of Rule 1		
QoS Rule	System Time	Friday, December 17, 2010 5:38	56 PM
SNMP	Week Day	Start Time (hh:mm)	End Time (hh:mm)
Routing	Sunday		÷
Schedule Rule	Monday		
	Tuesday		4.
	Wednesday		
	Thursday		
	Friday		+
	Saturday		
	Every Day		
		Save Undo Back	



Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

To edit the schedule rule.

Delete

To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.

Schedule Rule can be apply to Virtual server and Packet Filter, for example:

Example1: Virtual Server – Apply Rule#1 (ftp time: everyday 14:20 to 16:30)

ADMINISTRATOR'S MAIN ME	ENU	-11 Status	Wizard	Advanced	Þ	Logout English	
BASIC SETTI	IG 🙁 F	ORWARDING RULES		M ADVANCED SET	TING 12	TOOLBOX	
Virtual Server	😐 Virtu	ial Server				[HELP]	
Special AP Miscellaneous	Well known services select one V Schedule rule (00)Always V Copy to ID V						
	ID	Server IP	Service P	orts Protocol	Enable	Schedule Rule#	
	1	192,168,1.1	21	Both 💌		1	
	2	192,168,1		Both 😪		0	
	З	192.168.1.		Both 🛩		0	
	4	192.168.1.		Both 💌		0	
	5	192.168.1.		Both 🛩		0	
	6	192.168.1.		Beth 🛩		0	
	7	192.168.1		Both 💌		0	
	8	192.168.1		Both 🛩		0	
	9	192,168,1.		Both 💌		0	
	10	192.168.1		Both 😪		0	



Exanple2: Packet Filter – Apply Rule#1 (ftp time: everyday 14:20 to 16:30).

ADMINISTRATOR'S MAIN MEN	U	-i Status	57 M	lizard	Advanced	×	Logout	English	~
	1 😵 F	DRWARDING RULES	SECURI	TY SETTING	M ADVANCED SET	TING	тоосвох	1	
* Packet Filters	© Out	ound Packet Filter						[HELP]	
Domain Filters		Item		Setting					
+ URL Blocking	• Outbo	und Filter		Enable	1				
Internet Access Control	200	Allow all to pass e							
Miscellaneous	(Deny all to pass e	except those n	natch the foll	owing rules.				-
Block List						~			
	ID Source IP			Destination IP : Ports	Enable Schedule Ru		le Rule#	1	
	1				:21		1	1	
	2						0		
	3						0		
	4				-		0		
	5				-		0		
	6						0	i i	
	7				-		0		
	8				-		0		
			Save	Undo]	Inbound Filter	4			



3.3.4.7 QoS Rule

BASIC SETTI	ng 🤣	FORWARDING RULES		AD AD	VANCED SETTING	100LBOX	Ĩ
System Time	D Qo	'S Rule					
System Log		Item			Setting		
Dynamic DNS	► QoS	Gontrol	Enable				
QoS Rule		S	Well known service Schedule rule (00)Alway				
SNMP			Schedule rule 000 Alwa		ש טו נ <u>אי אי</u> אי ד		
Routing Schedule Rule	ID	Local IP	Remote IP : F	Ports	QoS Priority	Enable	Schedule Rule#
	1	192.168.1.161	168.96.2.3	21	High 😽		1
	2				Normal 💌		0
	3				Normal 😽		0
	4			-	Normal 💌		0
	5				Normal 💌		0
	6				Normal 💌		0
	7				Normal 💌		0
	- C:						

Local IP:

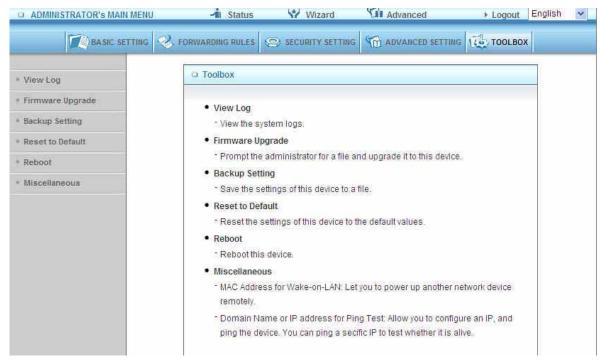
Please input Client IP,ex192.168.1.161.

Remote Priority:

Please input Global IP and port,ex:168.96.2.3 and port 21



3.3.5 Toolbox



3.3.5.1 View Log

ADMINISTRATOR'S MAI		W Wizard 🖸 Advan				
BASIC S	ETTING S FORWARDING RULES	SECONITY SETTING ADVAN	CED SETTING 120, TOOLBOX			
View Log	🗅 System Log					
Firmware Upgrade	Item		Info			
Backup Setting	WAN Type	Static IP Address (R0.29g0)				
	Display time	Fri Dec 17 17:44:29 2010				
 Reset to Default 	Time		Log			
Reboot	Friday, December 17, 2010 2:38:3	PM Blocked access attempt fro	m 192.168.0.10:2300 to UDP port 19287			
Miscellaneous	Friday, December 17, 2010 2:40:3	PM Admin from 192.168.1.160	login successfully			
	Friday, December 17, 2010 2:48:31 PM Admin from 192.168.1.161 login successfully					
	Friday, December 17, 2010 2:50:06 PM Restarted by 192:168.1.161					
	Friday, December 17, 2010 2:50:50 PM User from 192:168.123.161 login failed					
	Friday, December 17, 2010 2:50:54 PM Admin from 192.168.123.161 login successfully					
	Friday, December 17, 2010 2:51:22 PM Associated: 00-12-0E-9A-B2-15 st=0					
	Friday, December 17, 2010 2:55:42 PM Disassociated: 00-12-0E-9A-B2-15 wcid=1					
	Friday, December 17, 2010 2:56:12 PM Admin from 192.168.123.161 logged out					
	Friday, December 17, 2010 2:57:41 PM User from 192.168.123.161 login failed					
	Friday, December 17, 2010 2:57:45 PM Admin from 192.168.123.161 login successfully					
	Friday, December 17, 2010 3:14:23 PM Restarted by 192:168.123.161					
	Friday, December 17, 2010 3:14:2	PM_DOD:192.168.123.161 que	ry DNS for messenger hotmail.com			
	Friday, December 17, 2010 3:14:2	PM_DHCP:discover(My Host)				
	Friday, December 17, 2010 3:14:2	PM DHCP:offer(192.168.1.234))			

You can View system log by clicking the View Log button

AirLive GW-300R User's Manual



3.3.5.2 Firmware Upgrade

ADMINISTRATOR'S MAIN	uenu 🦂 Status 👌	Wizard	Cit Advanced	⊁ Logout	English	2
BASIC SPT	THE C FORWARDING BULKS	EGURITY SETTING	TI ADVANCED SETTING	TOOLBOX	c I	
View Log	니 Firmware Upgrade					1
Firmware Upgrade		Firmware	e Filename			
Backup Setting			Bruwse			
Reset to Default	Current firmware version	is R0.29g0. The u	ipgrade procedure takes a	bout 20 seconds.	ŝ	
Retuont						
Miscellaneous	The second se		nit when it is being upgrad			
	When the upgrade is	done successfull	y, the unit will be restarted	automatically.		
		Upgrade	Cancel			

You can upgrade firmware by clicking Firmware Upgrade button.

3.3.5.3 Backup Setting



You can backup your settings by clicking the Backup Setting button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

3.3.5.4 Reset to default

t Explorer 🔣
etting to default?
Cancel

You can also reset this product to factory default by clicking the Reset to default button.



3.3.5.5 Reboot



You can also reboot this product by clicking the Reboot button.

3.3.5.6 Miscellaneous Items

ADMINISTRATOR'S MAIN M	ENU - Status	Wizard	Cil Advanced	► Logout	English	~
122	ING 🥺 FORWARDING RULES	SECURITY SETTING	TI ADVANCED SETTING	100LBOX		
* View Log	Miscellaneous Items		i.		[HELP]	
 Firmware Upgrade 	Item		S	etting		
Backup Setting	MAC Address for Wake-on-L	AN		Wake up		
* Reset to Default	Domain Name or IP address	for Ping Test		Pin	J	
• Reboot		Save	Undo			
* Miscellaneous	in the second se					.7(4)

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 enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

Domain Name or IP Address for Test

Allow you to configure an IP, and ping the device. You can ping a secific IP to test whether it is alive.



Appendices and Index

802.1x Setting

1 Equipment Details

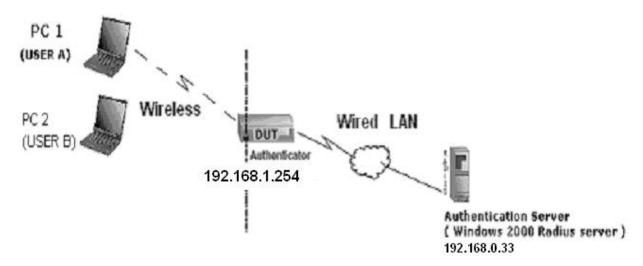


Figure 1: Testing Environment (Use Windows 2000 Radius Server) PC1:

Microsoft Windows XP Professional without Service Pack 1.

AirLive WN-200USB

Driver version:

PC2:

Microsoft Windows XP Professional with Service Pack 1a or latter.

AirLive WN-200USB

Driver version: 1.7.29.0 (Driver date: 10.20.2001)

Authentication Server: Windows 2000 RADIUS server with Service Pack 3 and HotFix Q313664.

Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and

HotFix Q313664 (You can get more information from

HHhttp://support.microsoft.com/default.aspx?scid=kb; en-us;313664UHH)



2 DUT Configuration: Enable DHCP server. WAN setting: static IP address. LAN IP address: 192.168.1.254/24. Set RADIUS server IP. Set RADIUS server shared key. Configure WEP key and 802.1X setting.

The following test will use the inbuilt 802.1X authentication method such as ,EAP_TLS, PEAP_CHAPv2(Windows XP with SP1 only), and PEAP_TLS(Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

3. DUT and Windows 2000 Radius Server Setup

Setup Windows 2000 RADIUS Server

We have to change authentication method to MD5_Challenge or using smart

card or other certificate on RADIUS server according to the test condition.

Setup DUT

Enable the 802.1X (check the "Enable checkbox").

Enter the RADIUS server IP.

Enter the shared key. (The key shared by the RADIUS server and DUT).

We will change 802.1X encryption key length to fit the variable test

condition.

Setup Network adapter on PC

1.Choose the IEEE802.1X as the authentication method. (Fig 2)

Note.

Figure 2 is a setting picture of Windows XP without service pack 1. If users upgrade to service pack 1, then they can't see MD5-Challenge from EAP type list any more, but they will get a new Protected EAP (PEAP) option.

Choose MD5-Challenge or Smart Card or other Certificate as the EAP type.

3.If choosing use smart card or the certificate as the EAP type, we select to use a certificate on this computer. (Fig 3)



4. We will change EAP type to fit the variable test condition.

🕂 Wireless Network Connection Properties 🛛 🔹 🔀						
General Wireless Networks Authentication Advanced						
Select this option to provide authenticated network access for wired and wireless Ethernet networks.						
Enable network access control using IEEE 802.1X						
EAP type: Smart Card or other Certificate MD5-Challenge						
Smart Card or other Certificate						
Authenticate as <u>computer</u> when computer information is available						
Authenticate as guest when user or computer information is unavailable						
OK Cancel						

Figure 2: Enable IEEE 802.1X access control

Figure 3: Smart card or certificate properties

4. Windows 2000 RADIUS server Authentication testing:

<u>4.1</u> DUT authenticate PC1 using certificate. (PC2 follows the same test procedures.)

Download and install the certificate on PC1. (Fig 4)

PC1 choose the SSID of DUT as the Access Point.

Set authentication type of wireless client and RADIUS server both to EAP_TLS.

Disable the wireless connection and enable again.

The DUT will send the user's certificate to the RADIUS server, and then

send the message of authentication result to PC1. (Fig 5)

Windows XP will prompt that the authentication process is success or fail

and end the authentication procedure. (Fig 6)



Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.

Certificates			? 🔀
Intended purpose:	<all></all>		~
Personal Other Peo	ple 🛛 Intermediate Certificatio	on Authorities Trusted I	Root Certification
Issued To	Issued By		endly Name
fae1	WirelessCA	2/6/2004 <no< td=""><td>one></td></no<>	one>
Import	port <u>R</u> emove		<u>A</u> dvanced
Certificate intended p	urposes		
			∐iew
			⊆lose

Figure 4: Certificate information on PC1

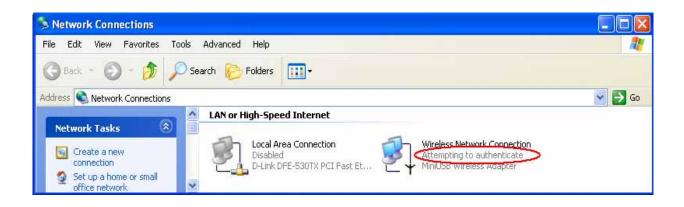




Figure 5: Authenticating

Network Connections		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u>	ools Adva <u>n</u> ced <u>H</u> elp	.
🕝 Back - 🕥 - 🏂 🎾	🔾 Search 🎼 Folders 🛄 🗸	
ddress 💊 Network Connections		💌 🛃 Go
Network Tasks	LAN or High-Speed Internet	
Create a new connection Set up a home or small office network	Local Area Connection Disabled D-Link DFE-530TX PCI Fast Et	

Figure 6: Authentication success

4.2 DUT authenticate PC2 using PEAP-TLS.

PC2 choose the SSID of DUT as the Access Point.

Set authentication type of wireless client and RADIUS server both to PEAP_TLS.

Disable the wireless connection and enable again.

The DUT will send the user's certificate to the RADIUS server, and then

send the message of authentication result to PC2.

Windows XP will prompt that the authentication process is success or fail and end the authentication procedure.

Terminate the test steps when PC2 get dynamic IP and PING remote host successfully.

Support Type: The router supports the types of 802.1x Authentication:

PEAP-CHAPv2 and PEAP-TLS.

Note.

PC1 is on Windows XP platform without Service Pack 1.

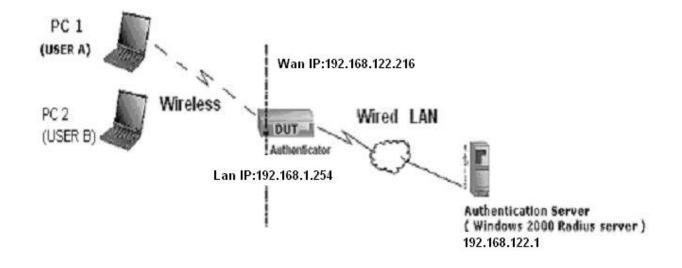
PC2 is on Windows XP platform with Service Pack 1a.

PEAP is supported on Windows XP with Service Pack 1 only.

Windows XP with Service Pack 1 allows 802.1x authentication only when data encryption function is enable.

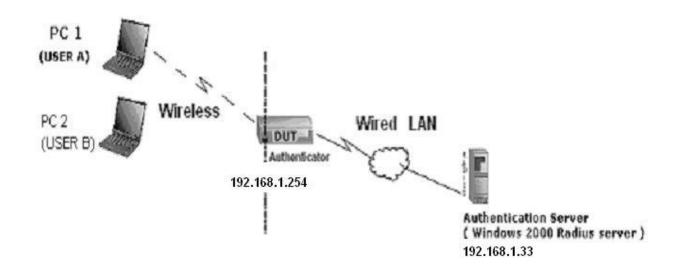


WPA Settings



Wireless Router: LAN IP: 192.168.1.254 WAN IP: 192.168.122.216 Radius Server: 192.168.122.1 UserA : XP Wireless Card:Ti-11g Tool: Odyssey Client Manager Refer to: HH<u>Uwww.funk.comU</u>HH Download: HHUhttp://www.funk.com/News&Events/ody_c_wpa_preview_pn.aspU

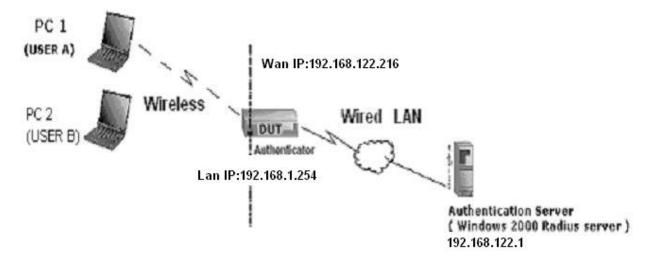
Or Another Configuration:





WPA:

For this function, we need the server to authenticate. This function is like 802.1x.



The above is our environment:

```
Method 1:
```

1. The UserA or UserB have to get certificate from Radius, first. HH<u>Uhttp://192.168.122.1/certsrvU</u>

account : fae1

passwd : fae1



- 2. Then, Install this certificate and finish.
- 3. Go to the Web manager of Wireless Router to configure, like below:



Network ID(SSID)	123kk	
Channel	8 💙	
Security		
802.1X Settings		
802.1X Settings RADIUS Server IP	192.168.122.1	
e e construction de la construction	192.168.122.1 1812	

4. Go to Odyssey Client Manager, choose "Profiles" and Setup Profile name as "1"

Add Profile 🛛 🔀
Profile name: 1
User Info Authentication I TLS Settings PEAP Settings
Login name: fae1
Password
✓ Permit login using password
 use Windows password prompt for password use the following password:
fae1
⊽ U <u>n</u> mask
Certificate
fae1
<u>V</u> iew <u>B</u> rowse
OK Cancel



Login name and passwd are fae1 and fae1. Remember that you get certificate from Radius in Step1.

5. Then Choose "certificate" like above.

ersonal Certificates		
Issued To	Issued By	
fae1	WirelessCA	
		 0
<		
<		⊻iew



6. Then go to Authentication and first Remove EAP/ TLS and Add EAP/TLS again.

		TLS Settings <u>P</u> B	
EAP / TLS	3		<u>∧</u> <u>A</u> dd <u>R</u> emove
1.1			
✓ Validate	server certificate		
☑ Validate	e server certificate		
☑ <u>V</u> alidate	e server certificate		



7. Go "Network" and Select "1" and ok

Network Properties		
- Network		
Network name (SSID):	123kk	
Connect to any ava		Scan
Description (optional):		
Network <u>type</u> :	Access point (infrastructure mode)	
C <u>h</u> annel.	default channel	
Association mode:	WPA	
Encryption method:	TKIP	-
✓ Authenticate using ✓ Keys will be genera Pre-shared key (WPA)	ted automatically for data privacy	
Passphrase:	NERRENER	
Г <u>U</u> nmask	,	
	OK Cancel	



8. Back to Connection and Select "123kk.

If successfully, the wireless client has to authenticate with Radius Server, like below:

twork Properties		<u>(0)</u>			© Odymey Client
Network Network name (SSID):	123kk				You are about to authenticate to an untrusted served
Econect to any avail	lable network	Scen			To terminate communication, press [No]
Description (optional) Network (ppe:	Claney Climit Ma Printer Conseille 1				To temposely tout this server, press [Yes] To permanently hout this server, check "add this trusted server to the detabase" and press [Yes]
Epicent Association mode Encryption method	Connection Profiles Networks	Connection Adapte: TNETTI: Adapter type: weekess Connect to network:	30 WLAN Adapter	¥ 	Centificate cham WrelessCA win2000adv intes com tw
Authenticate using (Engl will be general Pre-shared key (WPA) Engl trans Tourist	Auto-Scan Lists	Connection information Status Elapsed time Network (SSID) Access paint Packets in/out	authenticating 12343. 00:50:10:00:0F:F8		Vew
		Reconnect	Resuthenticate	400	Proceed to authenticate with this server?

9.Result:

Colyssey Client Ma			🛛		192.168.122.219: 192.168.122.219:			
ettings Commends W	eb <u>H</u> elp			Reply from	192.168.122.219:	bytes=32	tine=1ns	IIL-
C	Connection			Reply from	192.168.122.219:	bytes=32	time=1ms	TTL=
Connection		A 1.4 A 14		Reply from	192.168.122.219:	bytes=32	tine=1ns	TIL-
<u> </u>	Adapter: TNET11	00 WLAN Adapter	-	Reply from	192.168.122.219:	bytes=32	time=1ms	TTL-
€ Profiles	Adapter type: wireless			Reply from	192.168.122.219:	bytes=32	tine=1ns	IIL-
-		Lat. come		Reply from	192.168.122.219:	bytes=32	tine=1ns	III.
Networks	Connect to network:	++ <123kk>	-	Reply from	192.168.122.219:	bytes=32	tine=1ns	TTL
			Scap		192.168.122.219:			
Auto-Scan Lists				Reply from	192.168.122.219:	bytes=32	tine=1ns	TIL
-	Connection information			Reply from	192.168.122.219:	bytes=32	tine=2ns	III.
Trusted Servers	Statur:	open and authenticated		Reply from	192.168.122.219:	bytes=32	time=1ms	IIL.
100	Elapoed time:	02.03.59			192.168.122.219:			
Adapters	Network (SSID)	123kk			192.168.122.219:			
~	Access point	00-50-18-00-0F-F8			192.168.122.219:			
					192.168.122.219:			
	Packets in/out	12679 / 13605			192.168.122.219:			
					192.168.122.219:			
	Beconnect	Reauthenticate	(R4)		192.168.122.219:			
				Reply from	192.168.122.219:	bytes=32	tine=1ns	TTL-



Method 2:

1. The UserA or UserB have to get certificate from Radius,first. HHUhttp://192.168.122.1/certsrvU

account:fae1

passwd:fae1

Connect to 19	2.168.122.1	? 🛛
		LA K
Connecting to 19	2.168.122.1	
User name:	2 1	✓
Password:		
	Remember my pa	assword
	ОК	Cancel

- 2. Then Install this certificate and finish.
- 3. Setting on the router and client:

Router:

Network ID(SSID)	123kk	
Channel	8 💌	
Security	WPA 💌	
202 4V Catting		
802.1X Settings		
RADIUS Server IP	192.168.122.1	
en e	192.168.122.1 1812	



Client:

Go to "Network Connection" and select wireless adapter.

Choose "View available Wireless Networks" like below:

Advanced→ choose "123kk"

Select "WirelessCA and Enable" in Trusted root certificate authority:

L Wireless Network Connection 4 Properties ? X	Smart Card or other Certificate Properties
Select this option to provide authenticated network access for wired and wireless Ethernet networks. Properties Frable network access control using IEEE 802.1X EXP type: Smart Card or other Certificate Properties Authenticate as computer when computer information is available Authenticate as guest when user or computer information is unavailable	When connecting: Use my smart card Use a gertificate on this computer ✓ Validate server certificate Connect only if server name ends with: Trusted root certificate authority: ✓ Use a different user name for the connection OK
OK Cancel	

Use Windows to configure my wireless	network settings	Network name (SSID):	123kk
To connect to an available network, clic	k Configure.	This network requires a l	reu for the following
L dale L amit01 L JOYCE	Configure Refresh	Network Authentication: Data encryption:	
Preferred networks: Automatically connect to available netwo below:	orks in the order listed	Network Key: Confirm network Key:	
Add., Remove Pro	Move up Move down	Key index (advanced):	1 0
Learn about setting up wireless network configuration.	Advanced	This is a computer-to-co access points are not u	omputer (ad hoc) network, wireless ised

Then, if the wireless client wants to associate, it has to request to authenticate.

AirLive GW-300R User's Manual

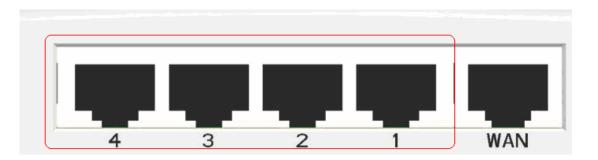


FAQ and Troubleshooting

What can I do when I have some trouble at the first time?

1. Why can I not configure the router even if the cable is plugged in the ports of Router and the led is also light?

A: First, make sure that which port is plugged. If the cable is in the Wan port, please change to plug in Lan port 1 or Lan port 4:



Then, please check if the Pc gets ip address from Router. Use command mode as below:

C:\Docum	ents a	nd Se	tti	ng	s \a	ir	liv	ve-	-հլ	on)	b):	ip	coi	nfig
Windows	IP Con	figur	ati	on										
Ethernet	adapt	er Lo	cal	A	rea	C	oni	neo	:ti	ior	1:			
	Connec	tion-	spe	ci	fic	DI	NS	Sı	ıff	i	¢			
	IP Add	ress.											-	192.168.1.199
	Subnet	Mask											-	255.255.255.0
	Defaul	t Gat	ewa	y		-	-	-			-	-	-	192.168.1.254



If yes, please execute Browser, like Mozilla and key 192.168.1.254 in address. If not, please ipconfig /release, then ipconfig /renew.

C:∖>ipco	ıfig ∕release			
Windows (IP Configuration			
Ethernet	adapter Local Area	Connection:		
	Connection-specific IP Address Subnet Mask Default Gateway		11	0.0.0
C:∖≻ipco	nfig ∕renew			
Windows 3	IP Configuration			
Ethernet	adapter Local Area	Connection:		
	Connection-specific IP Address Subnet Mask Default Gateway		- :	255.255.255.0

Whatever I setup, the pc can not get ip. Please check Status Led and refer to the Q2:

2.Why can I not connect the router even if the cable is plugged in Lan port and the led is light?

A: First, please check Status Led. If the device is normal, the led will blink per second. If not, please check How blinking Status led shows.

There are many abnormal symptoms as below:

Status Led is bright or dark in work: The system hanged up .Suggest powering off and on the router. But this symptom often occurs, please reset to default or upgrade latest fw to try again.

Status led flashes irregularly: Maybe the root cause is Flash rom and please press reset Button to reset to default or try to use Recovery mode.(Refer to Q3 and Q4)

Status flashes very fast while powering on: Maybe the router is the recovery mode and please refer to Q4.

- 3.How to reset to factory default?
- A: Press Wireless on /off and WPS button simultaneously about 5 sec Status will start flashing about 5 times, remove the finger. The RESTORE process is completed.



4.Why can I not connect Internet even though the cables are plugged in Wan port and Lan port and the leds are blink. In addition, Status led is also normal and I can configure web management?

A: Make sure that the network cable from DSL or Cable modem is plugged in Wan port of Router and

that the network cable from Lan port of router is plugged in Ethernet adapter. Then, please check which wan type you use. If you are not sure, please call the isp. Then please go to this page to input the

information isp is assigned.

• C	hoose WAN Type	
	Туре	Usage
0	Static IP Address	ISP assigns you a static IP address.
۲	Dynamic IP Address	Obtain an IP address from ISP automatically.
\bigcirc	Dynamic IP Address with	Road Runner Session Management.(e.g. Telstra BigPond)
\circ	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.

5.When I use Static IP Address to roam Internet, I can access or ping global IP 202.93.91.218, But I can not access the site that inputs domain name, for example HHUhttp://espn.comUHH ?

A: Please check the dns configuration of Static IP Address. Please refer to the information of ISP and assign one or two in dns item.



How do I connect router by using wireless?

1.How to start to use wireless?

A: First, make sure that you already installed wireless client device in your computer. Then check the Configuration of wireless router. The default is as below:

Wireless Setting	[HELP]						
Item	Setting						
▶ Wireless	◯ Enable ⊙ Disable						
Network ID(SSID)	default						
 Wireless Mode 	O 11 b/g/n Mixed O 11n only						
SSID Broadcast	⊙Enable ○Disable						
Channel	11 💌						
▶ Security	None						
	Save Undo WDS Setting						
MAC Ac	Idress Control Wireless Client List						

About wireless client, you will see wireless icon:

« _Y B

Then click and will see the ap list that wireless client can be accessed:

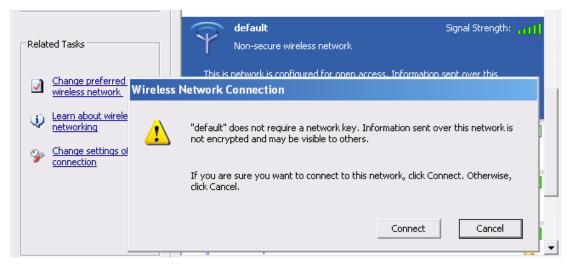


If the client can not access your wireless router, please refresh network list again. However, I still can not fine the device which ssid is "default", please refer to Q3.



Network Tasks	Choose a wireless network	network in range or to get more			
	information. default Non-secure wireless network	Signal Strength: BILLE			

Choose the one that you will want to connect and Connect:



If successfully, the computer will show



and get ip from router:

thernet adapter l	Loca	1 A	rea	C	oni	nea	:t:	io	n 5:
Connection-spec: IP Address	ific	DN	s s	ufi	Fix	¢		-	102 168 1 165
IP Hadress									172.100.1.103
Subnet Mask	terte								255.255.255.0
Default Gateway									192.108.1.254



2.When I use AES encryption of WPA-PSK to connect even if I input the correct pre-share key?

A: First, you must check if the driver of wireless client supports AES encryption. Please refer to the below:



If SSID is default and click "Properties" to check if the driver of wireless client supports AES encryption.

default properties	?	×							
Association Authentication Connection									
Network name (SSID): default	-								
Wireless network key									
This network requires a key for the following:									
Network Authentication:									
Data encryption:									
Network key:									
Confirm network key:									
Key inde <u>x</u> (advanced): 1 = The key is provided for me automatically This is a computer-to-computer (ad hoc) network; wireless access points are not used									
OK Cance	el –								



3. When I use wireless to connect the router, but I find the signal is very low even if I am close to the router?

A: Please check if the wireless client is normal, first. If yes, please send the unit to the seller and verify what the problem is.