



Step 3: Setup the LAN IP and WAN Type.



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

Example:

Air Live	T and	GW-300R Wreles	212/ 200Mbps Grps /
COMPACTNATION'S MANY INCOM	-4 3000	A HERE AN AND CH	+ Logist _ Grave
Setup Woord - 1948 Settings - PVP	down ((Mercost)		
STRANGER	1497.000.0	54.0	
· Loss P Address	104 100.1	204	
· Postern			
· Passana			
A Descention Cliffs			
· Destanting Lines		l Instantio	
A ANTINA A B Address	0.02.0	Instatut	
· Angent · Auren		(approval)	
aller 1 inter		· Manual · Longerous · Derive I	(Nette
• Batt	Passenti • MAR	 We possed at linearizing a finitian () 	Tiet -
-fux (Torr	Passent • 1144	 Weisser + Knownerg + Treiser () 	Tied >
Air Live	- Farrent - 1244	• Manual + Konsey + Tairer (GW-300R wireles	Text+
Air Live Air Live	4 June	• Witports + Konnerg + Tonier () GW-JOOR - winning W What	Connection a 272/F Society of + Logan (Digit
Air Live Air Live martilatore dan arm	4 June	• Binners + Konners + Tonier (GW-JOOR workes W Water - 50 Advanced	Corrections a 27228 ScoMbgar Grant + Legent Repla
Alis Live Alis Live Dimetrikatory Ham (Ham)	A Succession of a succession o	• Birports + Konstary + Florini () GW-300R wheeles W Water - Vill Advanced	Green and a 2722H Scottbare Gays F + Lagour Englis
Air Live Air Live Date Ward Weites seting	4. tota	* Missons + Gammary + Fasier (GW-300R winder W Waard VB Advanced	Committee 27201 Scottleas Days A + Logost Englis
File (1000	4. Hote Opatie	 Missons - Gammary - Tanier () Gitt-JOOR - wireless Without - VB Advanced O Doalite 	Committee 27201 Scottleas Days 7 + Logost English
Affer Liture: Affer Liture: Anter Waard - Wrotess settings Wrotess function Network Excellen	A line	 Missons - Gammary - Tanini (GW-300R wireles W Waard VB Atlanced W Waard VB Atlanced Obsails 	Committee 27227 Scottege Days 7 + Logost English
	 Pressonal * BAR Bartes O Enable Stratt Stratt Stratt 	 Missons - Gammary - Florini () GW-300R - Worker W - Whare W - Whare O Dealthe 	Communities 2772/F Jock/Hoger Diggs / + Logont Engla
	+ Francescol + 1944 - 4 Hotse - 9 Endis Internal - 11 M	• Physics - Gammary - Fanish (GW-300R wireles W Waard VB Athanced	Texts
	A Bate Contract Contract The M	• Winner • Gammer • Tanier I GW-JOOR wireles W Ware OB Advanced	Text -
	A Hote Code Stat	• Winner + Gammer + Tonier () GW-JOOR winner W Ware - OR Advanced	Lingent Bruth
	Contraction of the second seco	• Physics + Gammary + Timin" (GW-JOOR - wireles W Water - Vill Advanced	Constantion 2772/F 2004/Door Gray F + Legent Parts
	A Hote Contra State	• Physics + Gammary + Timin" (GW-JOOR - winning W What - Vill Advanced	Constantion 2772/F Jocombian Graph + Lagrant English
	A Hate Contra State	Hitport + Gammary + Tonisir () GW-JOOR whether W What Vill Advanced O Deally	Constantion 2772/F 300/Https://Englishing.com/ * Logon/ Englishing
	A Note Contra State	Obatte	Constantion 2772/F Scontose Guys / * Lagont Englis
	A Note Contra State	Obatte	Constantion 2772/F Scontose Guys / * Lagont Englis

Step 5: Set up your Wireless.



Set up your Authentication and Encryption.

Air Live GW-300R Minutese 2129 30 -di Status W Wilson Accession TRATING's MARK METRIC 6-12 Setup Hitzard - Witness Security (1001) 107 10 · Desuity @iann Orbinh + WEP . 4 681 1 0 1002 0 + Hay 3. 0 1 101-1 en 20 for 1286ts or 10 for 64 lats heisebecated (0, 1, 2., 8, 8, A, B., F). Plants. + 8343 | htart + Personal + Tible + Mireless + Summary + Treated) Tied >

W. Wittent

GIV-JOOR Wireless 2728 3

Step 6:

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

U Setar Vitand - Summary (DAT) Please confirm the information below (WAN Setting | WMN Type Dynamic IF Address Mint Name WAT'S MAC Address 10-52-10-21-04-57 (Westens Satting) Vibrations Trans 110 nout 11 Charged Security trone Cy you want to proceed the network testing? 1843 1 Mart + Passance + Water Welson's + Buttmary + Polatel 1 Apply Sattings

- 4 that

Step 7: Click Finish to complete it.





3.2 System Status

Air Live		GW-3	OOR Wireless 212	R 300Mbps G	e alrilve c liga Rot	om) Iter
ADMINISTRATOR'S MAIN MENU	-in Status	Wizard	Cill Advanced	+ Logout	English	v
BASIC SETTING 🥺	FORWARDING BULES	(C) SECURITY SETTING	C ADVANCED SETTING	100LBOX	1	
+ Primary Setup	O Basic Setting					
* DNCP Server	Primary Set	00				
+ Wireless	* Configure L	AN IP, and select WAN t	pe.			
Change Password	 DHCP Server The setting configuration Wireless Wireless set Change Pase Allow you to 	r is include Host IP, Subne ans. ettings allow you to confij sword a change system passwo	t Mask, Galeway, DNS; and gure the wireless configura ind	tivitNS		

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		GW-3	OOR Wireless 212	R 300Mbps (e alrilve o Siga Rot	om) iter
ADMINESTRATOR'S MAIN MENU	-ii Status	Wizard	Cill Advanced	+ Logout	English	
BASIC SETTING	C. FORWARDING RULES	(C) SECURITY SETTING	The Advanced Setting	TOOLBOX	1	
+ Primary Setup	O Basic Setting					
* DHCP Server	Primary Set	tup.				
+ Wireless	* Configure	LAN IP, and select WAN to	pe.			
Change Password	 DHCP Serve The setting configuration Wireless Wireless Change Pase Allow you to 	er gs include Host IP, Subne Ions. settings allow you to config asword to change system passwo	t Wask, Gateway, DNIS, and pure the wireless configura rd.	t WINS		



3.3.1.1 Primary Setup – WAN Type, Virtual Computers

Press "Change"

Air Live	di Status	GW-3	OOR Wireless 21	(www.airtive.com 2R 300Mbps Giga Route Lecout English
BASIC SETTING	C FORWARDING RULES			G TE TOOLBOX
Primary Setup	Primary Setup			[HELP]
DHCP Server	Item		Settin	0
Wireless	+ LAN IP Address	192.168.1	.254	
Change Password	 WAN Type 	Dynamic I	P Address Change]
	HostName	1	(000	(tenc
	WAN's MAC Address	00-50-18	21-04-57 Clone MA	C
	Renew IP Forever	Enabi	e (Auto-reconnect)	
	+ IGMP	Enabl	0	
	[Saved	we Undo Virtual	Computers	eot] booted.

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]
R 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.

D ADMINISTRATOR'S MAIN MENU	i -ii Status	W Wirard	CII Advanced	+ Logout English
BASIC SETTING		(2) месянту леттика		S TOOLBOX
· Primary Setup	O Primary Setup			[HELP]
DHCP Server	item		Setting	1
· Wireless	. LAN IP Address	192.168.1	1.254	
Change Password	WAN Type	Static IP /	Iddress Change	
	WAN IP Address	0.0.0.0		
	WAN Subnet Mask	255 255 3	265.0	
	WAN Gateway	0.0.0.0		
	Primary DNS	0.0.0.0		
	 Secondary DNS 	0.0.0		
	+ IGMP	Enabl	e	
	Saved	ave Undo Virtual The change doesn't tak	Computers	ot] pooted.

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.

BASIC SETTING		SECURITY SETTING		
Primary Setup	Primary Setup			[HELP]
DHCP Server	item		Settin	ng
· Wireless	+ LAN IP Address	192.168.1	.254	
Change Password	 WAN Type 	Oynamic I	P Address Change	
	HostName		(005	ional)
	+ WAN'S MAC Address	00-50-18-	21-D4-57 Clone MA	AC
	Renew IP Forever	Enabl	e (Auto-reconnect)	
	▶ IGMP	Enabl	D	
	Save Saved! The	Undo Virtual O	Computers Reb e effect until router is re	ebooted.



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.

BASIC SETTI	NG S FORWARDING BULES S	SECURITY SETTING TO ADVANCED SETTING
Primary Setup	O Primary Sebap	[HELP]
DHCP Server	Item	Setting
Wireless	+ LAN IP Address	192 168 1.254
Change Pasaword	• WAN Type	PPP over Ethernet Change
	PPPoE Account	
	PPPoE Password	
	Primary DNS	0.0.0
	In Secondary DNS	0.0.0.0
	Maximum Idle Time	300 seconds
	Connection Control	Connect-on-demand
	PPPoE Service Name	(optional)
	Assigned IP Address	0.0.0 (optional)
	+ MTU	1492
	► IGMP	Enable
	Saved! The cl	Save Undo Reboot hange doesn't take effect until router is rebooted.

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.

24



mont error	Theor.		
item	Setting		
LAN IP Address	192.168.1.254		
 WAN Type 	pppp 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@Jame			
PPTP Account			
PPTP Password			
Connection ID	(optional)		
Maximum Idle Time	300 seconds		
Connection Control	Connect-on-demand		
• MTU	1450		
+ IGMP	Enable		
	Item LAN IP Address WAN Type IP Mode IP Mode My IP Address My Subnet Mask Gateway IP Server IP Address/Name PPTP Account PPTP Password Connection ID Maximum Idle Time Connection Control MTU		

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.

· 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



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

MASIC SETTIN	IG 🤣 FORMA	ADING RULES AT SECURITY SET	TING	TOOLBOX
Primary Setup	Virtual Co	mputers	10.2	[HELP]
DHCP Server	255	DHCP dients 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	з		192.168.1	
one mapping of	4		192,168,1	
transfere Brough to.		1	102 168 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	O 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 (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:

BASIC SE	TTING C FORWARDING RULES	(=) весонату хеттина 🌾	ADVANCED SETTING	CBOX
Primary Setup	O DHCP Clients List		w.	[HELP]
DHCP Server	IP Address	Host Name	MAC Address	Select
Wireless	192.168 1.199	airlive-WayneNB	00-16-D4-EB-06-FC	
Change Password		Wake up Delete	Back Refresh	

3.3.1.3 Wireless

	denu -1 Status	Wizard VII Advanced + Logout English				
BASIC SET	TING 🙁 FORWARDING RULES 🙄	SECURITY SETTING				
Primary Setup	U Wireless Setting	[HELP]				
DHCP Server	Ibern	Setting				
Wireless	Wireless OEnable ODisable					
Change Password	Turn off Wireless depend as Schedule Rule	(00)A8ways 💌 🔿 Enable 💿 Disable Schedule Setting				
	Network ID(SSID)	default				
	Wireless Mode	Mixed mode 11g only 11b only 11n only				
	SSID Broadcast	Enable O Disable				
	+ Channel	11 👻				
	+ WDS	Enter				
	• WPS	Enter				
	+ Security	None				

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 SETTING	C. FORWARDING RULES	🖘 BECURITY SETTING 🌾 ADVANCED SETTING					
* Primarysetup	WI-Fi Protected Setup						
* DIICP Server	Rem	Setting					
* Wireless	+ WPS	Enable Disable					
+ Change Pasaword	• Setup	Current AP PIN Configure Wireless Station					
	Current PIN of the device	36842830 Generate New PIN					
	WPS state	Idle					
	WPS status Configured Release						
	Saved	Save Thoper 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.



O ADMINISTRATOR'S MAIN MEN	J 🕯 Status	W Witzard	Advanced	+ Logout English		
	C. FORWARDING RULES	SECURITY SETTING	The Advanced Setting	TOOLBOX		
Primary Setup	III WD5 Setting					
DHCP Server	Item		Setting			
Wireless	+ AP Mode:	AP Only 💌				
Change Password	Remote AP MAC MAC 1		i i i i i i i i i i i i i i i i i i i			
	MAC 2					
It is a system that	MAC 3					
interconnection of access points	MAC 4					
wireleasly.	Scaned AP's MAC Select	one Remote AP	MAC	Copy to		
	SSID	Cha	nnet	IAC Address		
	CL-WLAN		1 00-1	A-1E-C6-5C-90		
	CL-GUEST	11	1 00-1	A-1E-C6-5C-91		
	wmu6500		1 00-4	12-67-03-20-29		
	Air3G_Sam		1 00-4	IP-62-2A-06-4C		
	CL-WLAN		1 00-1	A-1E-0B-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



PrimarySetup	Wheless Setting	[HELP]					
DHCP Server	ltem	Setting					
Wireless	Wireless						
Change Password	Turn off Wireless depend as Schedule Rule	(00)4Ways 🔄 🔿 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 tx and RADIUS					
	Encryption Key Length						
	+ 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

Primary Setup	 Wireless Setting 	(HELP)				
+ DRCP Server	Item	Setting				
Wireless	Wreless	Enable O Disable				
Change Passworth	Turn off Wireless depend as Schedule Rule	(00)Always 💌 🔿 Enable 💿 Disable 🔄 Schedule Setting				
	+ Network ID(SSID)	default				
	 Wireless Mode 	⊗ liked mode ○ 11g only ○ 11b only ○ 11n only				
	SSID Broadcast	Enable O Disable				
	Channel	31 🐱				
	+ W05	Enter				
	• WPS	Enter				
	+ Security	WPA-PSK 👻				
	+ Encryption	© TKIP O AES				
	Preshare Key Mode	ASCI 💌				
	+ 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

Pringbey Setup	o wineress setting	[HEL			
DHCP.Server	Bern	Setting			
Westean	+ Wireless	Enable O 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 ○ 116 only ○ 11n only			
	+ 99/D Broadcast	@ Enable O Disable			
	+ Channel	11 💌			
	+ WD0	Enter			
	+ WPS	Enter			
	Security	WPA-PSK/WPA2-PSK			
	 Encryption 	TRJP + AES			
	Preshare Key Mode	ASCH 🛩			
	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

O ADMIN	INSTRATOR'S MAIN MENU	-fz Status	W Witzard	Advanced	+ Logout English	1
R	BASIC SETTING		(C) SECURITY SETTING		TOOLBOX	
+ Primary	Setup	> Windess Client List.				1
+ DHCP Se	trver.	Connecter	1 Time1	MAC A	lddress	
+ Wireles			Back:	Retrest		
+ Change	Pasaword					

3.3.1.4 Change Password

O ADDINISTRATOR'S MAIN NEW	U 👍 Status	W vitzard	Cit Advanced	+ Logout Eng	lish 🕑
ASIC SETTING	PORNARDING BULES			G TE TOOLAOK	
Primery Setup	O Change Password	112			
+ DRCP Server	item		Setting		
+ Writes	Old Password	1			
+ Change Password	+ New Password				
	+ Reconfirm				
		Save	Unde		

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



3.3.2 Forwarding Rules

Marcharter Serries	Conversion and a second
Virtual Server	P Forwarding Rules
Special AP	Virtual Server
• Miscellaneous	 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 devices/softwares.

3.3.2.1 Virtual Server

RASIC SETTING	3 H	DRWARDING RULES	SECURITY SETTING) ADVANCED SETT	ms lie	TOOLBOX
Virtual Server	o Virtu	al Server				[HELP]
Special AP Miscellaneous		Well know Schedu	n services – select one de rule (00)40ways 💌	Copy to ID	2	
	10	Server IP	Service Ports	Protocol	Enable	Schedule Rule#
	1	192,168.1		Both 💌		0
	2	192.168.1		Both 🛩		0
	3	192.168.1		Bôth 💌		0
	4	192.168.1		Both 🛩		0
	5	192.168.1		Both 💙		0
	5	192.168.1		Both 💌		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



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

RASIC SETTING	C FORM	ARDING RULES	SECONTY ACTING	ADVANCED SETTING	TOOLBOX
Virtual Server	O Special	Applications			(HELP)
Special AP		Popular appli	cations - Select on	e - 👻 Copyto ID -	
thecetlaneous	10	Trigger		Incoming Ports	Enable
	(T)				
	2				
	3				
	4				
	5				
	.6				
	7				
		1	E		

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

O ADMINISTRATOR'S MA	IN MENU -i Status	Wizard 🔨	II Advanced	+ Logout	English	
BANC 1	ATTING C. FORWARDING RULES C	ECURITY SETTING	D ADVANCED SETTING	TOOLBOX		
Virtual Server	O Miscellaneous Items					
Special AP	item		Setting		Enable	
Miscellaneous	IP Address of DMZ Host	I 192,168,1	9 192 168 1			
	Super DMZ(IP Passthrough)	0				
	Non-standard FTP port					
	UPnP setting	+ UPnP setting				
	Xbox Support	+ Xbox Support				
		Save Un	do	25		

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

O ADMINISTRATOR'S MAIN MENU	- Status	Witerd	GI Advanced	+ Logout English 🔗
	CHINARDING RULES	SECURITY SETTING		100LBOX
+ Packet Filters	 Security Setting 	li internetti		
+ Domain Filters	• Packet Filler			
+ URL Blocking	- Allows you t	, o control access to a n	etwork by analyzing the inco	ming and
* Internet Access Control	outgoing pa	ckets and letting them	pass or halling them base	t on the IP
* Miscellaneous	Domain Filter	ne source and desona	eon.	
	- Let you prev	ent users under this of	wice from accessing specif	fcURLs.
	URL Blocking			10.22
	- URL Blockin	ig will block LAN comp	uters to connect to pre-defi	ned websites.
	 Internet Addr 	ess Control		
	The device o the device o internet NA Control dep	crovides "Administrator r Internet without restri C Control by host, Grou end as user-defined to	MAC Control for specific li clion. It also provides 3 feat up MAC Control and interfac the Schedule.	IAC to access ures to access e Access
	fliscellaneou	9		
	 Remote Adr built-in web perform adr 	ninistrator Host in gen pages to perform adm ninistration task from r	eral, only Infranet user can inistration task. This feature emote host.	browse the e enables you to
	 Administrati automatical 	r Time-out The amou ly close the Administra	nt of time of inactivity before tor session. Set this to zero	the device will to disable it.
	* Discard PIN WAN cannol	G from WAN side: Whe ping the Device.	in this feature is enabled, h	osts on the



3.3.3.1 Packet Filters

C Province and the second		Street and a street of the street	Charles Shree	Contract of the state of the state		10000000		
Packet Fitters	u out	ound Packet Filter	2.5	[HELP				
Iomain Filtera	Rem			Setting				
IRL Blocking	Outbound Filter		Enable	Enable				
ternet Access Control	0	Allow all to pasis except th Cleav all to pasis except th	ose match the folloge match the folloge	fowing rules. Iowing rules.				
Wecellaneoux		Schedu	Block List - s le rule (00)46way	selections - 💌 s 🛩 Copyto ID	*			
	ID Source IP		Dest	tnation IP : Ports	Enable	Schedule Ru	le#	
	1					à	-	
	2		[1		0		
	3					0		
	(4.1		[0		
	5			3(0		
	6					0		
	7		1			0		
			1	1		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:

Q MAN AND	16 3 1	DOWNARDING ANLES NOT SEC	URITY SETTING 10 ADV	ANCER SETT	110	100,804	
Packet Filters	U-Out	ound Packet Filter			[HELP		
Somain Emers		Rem		Setting			
RL Blacking	Outbound Filter		E Enable	Enable			
etantet Access Control	0	Allow all to pass except the Denv all to pass except the	on match the following rules an inatch the following rules	alch the following rules.			
Musellaneoux		Schedule	Bisck List - select one - rule (00)4Ways - Cop	- a av	v		
	ID Source IP		Destination IP :	Parts	Enable	Schedule Rule#	
		123100-123140		25-100		0	
	2	12310-12320			B	0	
	3	1		-		0	
	4					0	
	\$					D	
						a	
	7					0	
		1	10		0	0	

(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:

Packet Filmex	Outbound Packet Filter						HELP
Dormain filters		item		Se	ting		
sRL Backing	Outbound Filter		E Enable				
Internet Access Control	0	Allow all to pass except thos Deny all to pass except thos	e match the following match the following	ng isules. Ng isules			
		Schedule	Block List - selec rule (50)44ways 🛩	Copyta ID	- M		
	- ID	Source IP	Destinat	ion IP : Ports	Enable	Schedule	Rule#
		123.100-123.109		21	2	0	1
	2	123100-123199		199		0	
	3			10		0	
	- 4	[]	E.			0	
	5			10		0	
	6			10		Ó	
	7	C		-10		a	
		22	1		1	1.	-

(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

A BASIC SETT	narg 😪 P	DemAdding Putts (C) SI	CURITY SETTING	(m) ADVANCED SET	TING Lee	TOOLBOX		
Packet Filters	Out	ound Packet Filter				(HE		
Dortun Filters	Hern			Setting				
VRL Blocking	Outbound Filter		🗹 Enable	Enable				
Internet Access Control		Allow all to pass except th Denv all to pass except the	ose match the follose match the follo	match the following rules.				
Miscellaneous		Schedul	Block List - 1 e rule (00)43ways	electione - 💌	v			
	ID	ID Source IP		ination IP : Ports	Enable	Schedule Rule		
	1	100-192.158.12.149		21-100	2	0		
	2	2.10-192.188.12.20			2	0		
	3			14		0		
	4			le l		Q		
	5					0		
	6			1		0		
	7			-		0		
	8					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

To BASIC	аттио 😒 р	DRIVANDING RULES	ECURITY SETTING		ma Tè	1000,004	1
acket Filters	U Out	O Outbound Packet Filter					[HELP]
oonan Filters		Rem	10	Setting			
HL Blocking	Outpo	Outbound Filter		Enable			
dernet Access Control		Allow all to pass except those		natch the following rules.			
facellaneous.		Deny all to pass except the	losie match the follo	owing rules.			
		Schedu	Block List - 5 le rule 100;Always	Copy to ID	- 9		
	10	10 Source IP Dester		nation IP : Ports	Enable	Schedu	le Rule#
		1002 568 12 100	1	1.24	1 121	0	
	1	19a.100.1a.100		2	1 121	1.0	
	Ĩ	192 168 12 199		119	N N	0	
	2	192 168 12 199		119		0	
	1 2 3 4	192 168 12 199		(= (119 (0	
	1 2 1 4 5	192.168.12.199		 119 		0	
	1 2 3 4 5 0			4** 119 4 4 4		0 0 0 0 0 0	
	1 2 3 4 5 0 7			(** (119 [[[[[[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

- Papier Citera	La Dare	an filter				10021	
· Springer Fillers	Ren			fatting			
101 Dankey	+ Domain Filter		E Cruste				
Research Assessed Description	+ Log Dhiti Guery		E linine				
* Bazatarena	+ Phillip	lege IP Addresses Range From T		To 10			
	8	Domain Suttix		Action	Enites	Schedule Rules	
	1			Done Dire	R	0	
	2			Danie Duig		0	
	3			Done Dura		0	
	4			Done Dire		0	
	¥.			Drep Duty		0	
	. 4			Done Dire		. 0	
	. 1			Dow Dug	13	6	
	8			Done Duis		0.0	
	3			Day Duy		4	
	10	10 *tab officers)		Dow Duty	100	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:

PacketFilters	o Dom	ain Filter		EHELP			
Domain Filters	llem			Setting			
URL Blocking	+ Doma	+ Domain Filter		Enable			
Internet Access Control	+ Log DNS Query		🗹 Enable				
• Miscellaneous	· Privile	ge IP Addresses Range	From 100	To 199			
	10	Domain Suffix		Action	Enable	Schedule Rulei	
	1	www.msn.com		Drop DLog		0	
	2	www.sina.com		Drop 2Log	2	0	
	3	www.baidu.com			9	0	
	4					0	
	5			Drop Log		0	
	6					0	
	7			Crop Log		0	
	8					0	
	8					0	
	10	10 * (all others)			-	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.99 can access Internet without restriction.



3.3.3.3 URL Blocking

A BASE MIT		A STATEMENT AND A STATEMENT AN	A RECORD ALTING	(II) service (II) II (II)	1to.		
Packet Filters	O URL	D URL Blocking			Date		
Domain Piltera		Bern		Settin	0		
IRL Disching	+ URL B	liscking	🗆 Enabi				
Internet Access Control	ID URL			Enable	Schedule R	ulet	
Muzefianeoua	. 1					0	
	2					0	1
	з					0	
	:4					0	1
	5					0	1
	0					0	1
	2					0	
						0	
	9					0	
	10					0	Г

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.



R MARC SETT	ni (3 10	manendi mitata (C) secure	TY SETTING	TADVANCED METTING	165-100	KINGH
Packet fillers	ia URL I	u URL Blocking				[HELP]
Doman Filters		Item		Setting		
19L Backing	+ URL B	oching	Enable			
Internet Access Control	10	1	181.		Enable	Schedule Raled
Miscallaneoux	1	man				0
	2	sina			2	.0
	3					0
	4			19		0
	5	1				0
	8			1		0
	7					0
						0
						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.

D ADDINESTRATOR'S BAIN US	inu 👍 Status	Wittant Of Advanced	+ Logout English 9
ASC STT		THE ADVANCED BETTING	NG TOOLSON
Packet Films	D Administrator MAC Cont	ed.	[HELP]
Soman Filters	DHCP clients 00-15	-O4-E8-05-FC 192 158 123 151 (artive-na) 👻	Copy to to 1 👻
URL Blocking	ID	MAC Address	Enable
Internet Access Control		00-15-D4-EB-06-FC	
Allacettaneous :	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.

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

MAC control

ADMINISTRATOR'S MAIN I		-it Status	Wizard	CII Advanced	يە. مەتقىرا سى	Logo	ut English
The second	THUS CON	ONVARIANG RULES	Seconity setting	(I) VDAVRCED TELL	- 16 0 .	TOOL	BOX
Packet Filters	O MA	G MAC Address Control [HELP]					
Somain Filtera		Bem		Setting			
URL Blocking	MAC Address Control		Enable				
Internet Access Control	Flow	and the second set	Wireless and wired o	lients with C checked c	an connect	to thi	s device; and
Miscellaneous	Licon	nection control	allow 💌 unspecifie	d MAC addresses to co	innect.		
		ociation control	Wireless clients with deny unspecifie Note: Association co	A checked can associa d MAC addresses to an introl has no effect on	ate to the wi ssociate, wired clien	ireles its.	is LAN; and
		DHCP clients - Select one V Schedule rule (00)Always V Copy to ID - V					
	1D	MAC Address	N. AN	IP Address	с	A	Schedule Rule
	4			192.168.1			0
	2			192.168.1			0
	3			192.168.1			0
	4			102 108 1	E		0

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

ID	MAC Address	IP Address	c	A	Schedule Rule#
1		192.168.1			0
2	×?	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.

		_		1		
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:

MANC SET	ing 😵		SECURITY SETTING		16	100	LBOX
Packet Filters	ia-MA	C Address Control				_	[HELP]
Domain Filters		Item		Setting			
URL Blocking	 MA 	C Address Control	Enable .				
Internet Access Control	Rea	apartion control	Wireless and wired o	lients with C checked c	an connect	to th	is device; and
Miscellaneous	ElCo	mecoon conner	allow 💌 unspecifie	d MAC addresses to co	nnect.		
	[€] Ass	octation control	Wreless clients with deny v unspecifie Note: Association co	A checked can associa d MAC addresses to as ntrol has no effect on t	te to the wi isociate. wired clien	irele its.	ss LAN; and
		DHCP clients Sch	Select one edule rule (00)Always	Copy to ID -	*	+	
	ID	MAC Address		IP Address	c	A	Schedule Rule
		00-12-34-56-78-90	11) I - A	192.168.1 100			0
	1					-	
	2			192.168.1	2	2	0
	2	00-98-78-54-32-10		192.168.1	2		0

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	J -11 Status	W Wirard	Advanced	+ Logout	English
R RASIC SETTING		C SECURITY SETTING	T ADVANCED SETTING	120 100180	2
PacketFilters	O Group MAC Access Cor	strol			[HELP]
Domain Filtera	Item		Setting		
URL Blocking	Group MAC Access Contr	ol 🔲 Enable			
Internet Access Control	Save Undo				
Miscellaneous	G Add Member to Group L	ist			
	Add MAC Address to Grou	up 1 and apply sched	opy Select one ule rule (00)Always V (EB-06-FC to Group 1!	Add]	•
	Group List 1 - Always a	cūve.			2
	MAC Address	Host	Name IP	Address	Action
	00-15-D4-EB-05-FC	W-avinic	ayneNB 193	2 168 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.

ADC MIT	mi 🧹 rommanis mita (2) SECURITY SETTING (C) ADVANCED SETTING	1 Cal TOOLBOR
Packet filters	 Interface Access Control 		[HELP]
Domen Filters	item	Setting	
ML Bickey	+ Interface Access Control	Enable	
Internet Assess Control	Interface	Schedule Role	Deny
Mecelaneoux	Port 1	(00048ways 😾	Ø
	Port2	(00)Always M	Ð
	Port 3	(00)44e3(3 M	Ð
	Purt 4	(00)4/mays	2
	Witeless	(00)46ays 🛩	2





3.3.3.5 Miscellaneous Items

BASIC SETTI	NG CORWARDING RULES (C) SECUR	RITY SETTING	TOOLBOX
PackotFillers	 Miscellaneous items 	100	[HELP]
Domain Filters	Item	Setting	Enable
· URL Blocking	+ Remote Administrator Host / Port	0.0.0.0	
Internet Access Control	Administrator Time-out [600] seconds (0 to disable)		
Miscellaneous	Discard PING from WAN side		
	+ SPI mode		
	DoS Attack Detection		
	+ VEN PPTP Pass-Through		
	VPN IPSec Pass-Through	2	

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

O ADMINISTRATOR'S MAIN MENU	-1 Status	W Witsard	Cil Advanced	+ Logout English	2
BASIC SETTING	TOMINARDING RULES		ADVANCED SETTING	TOOLEOX	
* System Time	O Advanced Settin	o.			
+ System Log	• Custom Time				
+ Dynamic DHS	* Allow you to	set device time manua	illy or consult network time tro	om NTP	
+ QoS Rule	server,			N 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
* 3030P	System Log Send system	n loo to a dedicated ho	st or email to specific receipt		
+ Bouting	Dynamic DNS	i i i i i i i i i i i i i i i i i i i			
* Schiedule Bulle	- To hest your domain nam	server on a changing ne service (DDNS).	IP address, you have to use o	dynamic	
	GoS Rule Cuality of Se or guarantee	invice can provide diffe e a certain level of perf	ent priority to different users o simance.	or data flows,	
	 Shitp Gives a use and setting 	r the capability to remo terminal values and m	tely manage a computer network events	vork by polling	
	Routing				
	 If you have in routing table subnets to o 	nore than one routers : to allow packets to fin communicate with each	and subnets, you may want to d proper routing path and allo 1 other.	ertable ow different	
	 Schedule Rul - Apply sched 	e Iule rules to Packet Filt	ers and Virtual Server.		

3.3.4.1 System Time

HASIC M		S C SECURITY SETTING
	O System Time	[HELP]
iyatem time	lbern	Setting
system Log	System Time	Friday, December 17, 2010 5:28:18 PM
oynamic Dirs	. Get Date and Time	by NTP Protocol Sync Now!
CRATE	Time Server	time.nist.gov 💌
Rooting	Time Zone	(GMT-08:00) Pacific Time (US & Canada)
Schedule Rule	• O Set Date and Time	using PC's Date and Time
	PC Date and Time	Friday, December 17, 2010 5/28:19 PM
	+ O Set Date and Time	manually
	Date	Year 2009 V Month Jun V Day: 01 V
	Time	Hour: 0 (0-23) Minute 0 (0-59) Second: 0 (0-59)
	Daylight Saving	O Enable O Disable
	Start	Month: Jan V Day: 01 V Hour: 00 V
	End	Month Jan V Day: 01 V Hear 00 V

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

System Time	 System Log 		[HELP]	
System Log	ttern	Setting	Enable	
Dynamic DRS	IP Address of Syslog Server	192.168.1		
QoS Rule	• E-mail Alert	Send Mail Now		
SHAP	SMTP Server IP/Port			
Routing	• E-mail addresses	8		
 Schedule Rule 		8		
	E-mail Subject			
	User name			
	Password			
	+ Log Type	System Activity Solution Attacks Topped Packets Topped Pa		

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

STERG STONAL STONAL STREET	C BICHNEY METTING THE ADVANCED METTING	
Dynamic DNS	[40	LP)
Bern	Setting	
+ 00148	@Disable O'Enable	
Prouder	DynDf2S srgiDynamici 🗑 Provider website	
+ Hostilaria		
+ Usamama / E-mail		
+ Fassword/Kay		
	Providence autors Providence Provider HostName HostName HostName HostName HostName HostName HostName HostName	Demonstration Description Setting Imm Setting

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

CI ADN	INISTRATOR'S MAIN MENU	-in Status	W Witard	Cil Advanced	+ Logout	English	2
3	BASIC SETTING	C FORWARDING RULES	C: SECURITY SETTING	C ADVANCED SETTING	TOOLBOX		
- Syster	m Time	O SNMP Setting				[HELP]	1
· Syster	mLog	Item		Setting			
" Дупал	nic DHS	Enable ShillP	ELocal Remote	ē.]
· QoSR	ule	 Get Community 	public				
* SHMP		Set Community	private				1
- Routin	10	▶ (P 1				- P	1
+ School	fule Rule	• UP 2					1
		F IF 3					1
		• IP 4					1
		SPAMP Version	© V1 @ V2¢				1
			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

ADMINISTRATOR'S MAIN ME	NU .	A Status	Witard	Advanced	Logout €	English
ANC BUT	6	CHNARONG RULES	(С) меняти аттик	ADVANCED SETTIN	IG TOOLION	
System Time	I Ros	uting Table				[HELP]
System Log		item		Setting		
Dynamic DILS	• Dyn	mic Routing	Disable O RIP	V1 O.RIPV2		
Qu'S Rule	 Stati 	c Routing	Disable O End	itie		
SHUP	iD	Destination	Subnet Mask	Gateway	Нор	Enable
Bouting	1	1		18 8		
Schedule Rule	2					
2022-2041-55	3					
	4					
	.6					
	.6	[
	7					
	8		1			
	-		Save	Undo		

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	•
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

O ADMINISTRATOR's MA	IN MENU	status	W Witard	Cit Advanced	+ Logout	English	1
R MASIC S	ETTING S FORWARD	ING RULES	CO SECURITY SETTING		NG TOOLION		
* System Time	G Schedule Ru	łė	15			THELPI	1
* System Log		item		Settin	ig		
* Dynamic DHS	+ Schedule		E Email	ble			1
+ OoS Rule	Rule#		Rule Name		Action		1
+ SHMP			Save Ad	d New Rule			1
* Routing	1.1.1						1
+ 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

R ADMINISTRATOR'S MAIN MEN	C FORMARDING RULES	C MCONTY SETTING	Advanced	ETTING	
System Time	G Schedule Rule Setting			[HELJ	1
System Log	Bem		Set	ting	
Dynamic DRS	tame of Rule 1				
Go S Rule	 System Time 	Friday, Decemb	er 17, 2010 5 38 50	S PM	
Smap	Week Day	Start Tim	e (hhumm)	End Time (hfumm)	
Routing	Sunday		-		٦
Schodule Rule	Monday				1
0.0000000000000000000000000000000000000	Tuesday				٦
	Wednesday				٦
	Thursday				1
	Friday		+		٦
	Saturday				٦
	Every Day				1
		Save Un	ido 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 N	IENU	A Status	W Wizard	Cit Advanced		Logout English
BASIC SET	111G 🛞 P	DRWARDING RULES	C SECURITY SETTING	() ADVANCED SET	nna tie	TOOLBOX
Virtual Server	III Virts	al Server				[HELP]
Special AP Miscelianeous		Wel	known services Selec Schedule rule (00)Always	t one I 🛩 Copy to ID	2	
	ID	Server IP	Service P	orts Protocol	Enable	Schedule Rule#
	1	192.168.1	21	Both 🛩		1
	2	192,168,1		Both 🛩		ō
	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 🛩		D
	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 ME	NU	-it Status	Wizard	Ci Advanced		Logout E	nglish
BASIC SETTIN	6 3 R	DRWARDING RULES	SECURITY SETTING	C ADVANCED SET	ting 😥	TOOLBOX	
Packet Filters	a Out	ound Packet Filter					[HELP]
Domain Filters		Item		Set	tting		
RL Blocking	Outpo	und Filter	Enable				
nternet Access Control	(Allow all to pass ex	cept those match the foll	lowing rules.			
discellaneous	(O Deny all to pass exc	ept those match the foll	owing rules.			
	Block List select one Schedule rule (00)Always Copy to ID						
	ID	Source IP	Dest	Destination IP : Ports		Enable Schedule Rule#	
	1			21		1	
	2					0	
	3			1		0	
	4					0	
	5			1		0	
	6					0	
				11		0	
	7.						



3.3.4.7 QoS Rule

BASIC SET	TING 😵	FORWARDING RULES	S SECURITY SET	ning (C) A	OVANCED SETTING	TOOLBO	IX .
atem Time	10 Qo	S Rule					
stem Log		Item			Setting		
mamic DNS	+ Q65	i Control	Enable				
oS Rule		Sc	Well known ser hedule rule (00)A	vices - sele Iways • C	opy to ID - 💌		
Routing Schedule Bule	ю	Local IP	Remote I	P : Ports	QoS Priority	Enable	Schedule Rule#
	1	192.168.1.161	168.96.2.3	21	High 💌	9	1
	2		1	-	Normal 🛩		0
	3			1	Normal 😪		0
	4].[Normal 🛩		0
	5			2	Normal 🛩		0
	6			-	Normal 💌		0
	7		E	-	Normai 🛩		0
	8			1	Normal 🐱		0

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